TARNVEER SINGH

DIGITAL RESILIENCE, CYBERSECURITY AND SUPPLY CHAINS

BUSINESS AND DIGITAL TRANSFORMATION

ROUTLEDGE

DIGITAL RESILIENCE, CYBERSECURITY AND SUPPLY CHAINS

In the digital era, the pace of technological advancement is unprecedented, and the interconnectivity of systems and processes has reached levels never seen before. While this interconnectivity has brought about numerous benefits, it has also introduced new risks and vulnerabilities that can potentially disrupt operations, compromise data integrity, and threaten business continuity. In today's rapidly evolving digital landscape, organisations must prioritise resilience to thrive. Digital resilience encompasses the ability to adapt, recover, and maintain operations in the face of cyber threats, operational disruptions, and supply chain challenges. As we navigate the complexities of the digital age, cultivating resilience is paramount to safeguarding our digital assets, ensuring business continuity, and fostering long-term success. *Digital Resilience, Cybersecurity and Supply Chains* considers the intricacies of digital resilience and its various facets, including cyber resilience, operational resilience, and supply chain resilience. Executives and business students need to understand the key challenges organisations face in building resilience and provide actionable strategies, tools, and technologies to enhance our digital resilience capabilities. This book examines real-world case studies of organisations that have successfully navigated the complexities of the digital age, providing inspiration for readers' own resilience journeys.

Tarnveer Singh is an experienced CISO and Security Director at Cyber Wisdom Ltd.

BUSINESS AND DIGITAL TRANSFORMATION

Digital technologies are transforming societies across the globe, the effects of which are yet to be fully understood. In the business world, technological disruption brings an array of challenges and opportunities for organizations, management and the workplace.

This series of textbooks provides a student-centred library to analyse, explore and critique the evolutionary effects of technology on the business world. Each book in the series takes the perspective of a key business discipline and examines the transformational potential of digital technology, aided by real world cases and examples.

With contributions from expert scholars across the globe, the books in this series enable critical thinking students to excel in their studies of the new digital business environment.

Demand-Driven Business Strategy
Digital Transformation and Business Model Innovation
Cor Molenaar

Navigating Digital Transformation in Management
Richard Busulwa

Smart Business and Digital Transformation
An Industry 4.0 Perspective
Sándor Gyula Nagy and Tamás Stukovszky

Data Analytics and Digital Transformation
Erik Beulen and Marla A. Dans

Consumer Behaviour and Digital Transformation
Ayantunji Gbadamosi

Digital Infrastructures for Business Innovation
Magda David Hercheui and Tony Cornford

Digital Resilience, Cybersecurity and Supply Chains
Tarnveer Singh

For more information about this series, please visit www.routledge.com/Routledge-New-Directions-in-Public-Relations–Communication-Research/book-series/BAD

DIGITAL RESILIENCE, CYBERSECURITY AND SUPPLY CHAINS

Tarnveer Singh

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Designed cover image: Getty Images

First published 2025
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 9781032995878 (hbk)
ISBN: 9781032995670 (pbk)
ISBN: 9781003604969 (ebk)

DOI: 10.4324/9781003604969

Typeset in Times New Roman
by Taylor & Francis Books

CONTENTS

TABLES

1

DIGITAL RESILIENCE

The Case For Digital Resilience

In today's rapidly evolving digital landscape, organisations must prioritise resilience to thrive. Digital resilience encompasses the ability to adapt, recover, and maintain operations in the face of cyber threats, operational disruptions, and supply chain challenges. As we navigate the complexities of the digital age, cultivating resilience is paramount to safeguarding our digital assets, ensuring business continuity, and fostering long-term success.

Boh et al. (2023) argue digital resilience must be an utmost concern for businesses to build the capabilities to absorb major shocks, adapt to disruptions caused by the shocks, and transform to a new stable state, where entities are more prepared to deal with major shocks.[1]

Resilience is not a one-time endeavour; it is an ongoing journey that requires continuous vigilance, proactive measures, and a deep understanding of the ever-changing risks and vulnerabilities.[2] By embracing digital resilience, we equip ourselves with the tools and strategies necessary to anticipate, mitigate, and respond effectively to potential threats and disruptions, ultimately fortifying our organisations for the future.[3]

He et al. (2023) emphasise that strategic technology investment helps organisations to develop systematic control and sustain operations in crises. Transformation management intensity equips an organisation with transformative vision, governance and culture, and such transformative built-in leadership enables the organisation to embrace employees with innovativeness and help employees grow their capabilities when facing crises.[4]

We must consider the intricacies of digital resilience, its various facets, including cyber resilience, operational resilience, and supply chain resilience. Executives must understand the key challenges organisations face in building

DOI: 10.4324/9781003604969-1

resilience and provide actionable strategies, tools, and technologies to enhance our digital resilience capabilities. We will examine real-world case studies of organisations that have successfully navigated the complexities of the digital age, serving as inspiration for our own resilience journeys.

Kashem et al. (2024) contend as organisations are under pressure to go through digital transformation, digital resilience is increasingly the best approach to improving resilience within organisations.[5]

In the digital era, the pace of technological advancement is unprecedented, and the interconnectivity of systems and processes has reached unprecedented levels. While this interconnectivity has brought about numerous benefits, it has also introduced new risks and vulnerabilities that can potentially disrupt operations, compromise data integrity, and threaten business continuity.

Lee et al. (2024) insist digital resilience can effectively mitigate the effects of pandemics, including their health, economic, and societal impacts. However, digital resilience is often narrowly approached, overemphasising quick actions without a deep understanding of how to develop digital resilience practices at a societal level. They provide guidelines to maintain digital resilience.[6]

The consequences of failing to build digital resilience can be severe, ranging from financial losses and reputational damage to regulatory non-compliance and loss of customer trust. Cyber attacks, system failures, natural disasters, and supply chain disruptions can all have devastating impacts on an organisation's ability to operate effectively and maintain competitive advantage.

Digital Resilience = Operational Resilience + Cyber Resilience

Operational resilience is the ability of an institution to deliver critical operations through disruption to operate within their impact tolerances (ensuring risk identification and management, adaptive governance, business continuity plan, IT resilience, crisis management and response.)

Cyber resilience is focused on protecting the digital assets: the ability of an organisation to prepare, identify, respond, and recover from an information security incident. This is underpinned by risk-focus assessments and acknowledging an incident will happen.

Cyber and operational resilience are both core components of *Digital resilience*. This is where employees and individuals are in strategic alignment with the company. Digital resilience is vital to maintain your ability to operate in a disruption and evolve to take advantage of new conditions and technology advancements. It is vital that organisations can respond to all kinds of crises to accelerate and innovate.. Building cross-functional crisis management, business continuity plan (BCP), and continuous monitoring, to break down siloed digital environments in and across often complex

sophisticated technology teams. Adapting to an all-hazards disruption event ranging from cyber threats such as ransomware, insider threat, data leakage, business continuity, and non-cyber events such as natural disasters.

Incident response and crisis management teach how to manage a crisis from the Board level down to technical and operational teams.[7] Expertise in this field indelibly embeds both technical and soft skill expertise, to input to a variety of internal and external stakeholders. This includes supporting the strategy in different jurisdictions, where self-reporting early on to regulators is mandatory. Incorporating the resiliency standards such as *ISO 22301:2019 (BCMP)* with good practice guidelines such as *ISO 22361:2022 (Crisis Management)*, which emphasises an all-hazards approach (and not just a cyber-related crisis), can help organisations steer the resiliency programme[8] and these standards are referred to in later sections.

Governance is critical for cybersecurity by integration into the business operations to reduce the potential impact and sharpness felt following interruption due to a root cause cyber-related threat and the impact that follows. National Institute of Standards and Technology (NIST) released their Cybersecurity Framework (CSF) with version 2.0[9] and this is referred to in later sections.

Incident Response (IR) capabilities support digital resilience as they require you to have a plan, practice and learn the plan, implement the plan, and carry out lessons learned activities and after-action reviews. IR skillsets can be used proactively, to address and mitigate risk before an operational or cyber crisis occurs. Arguably, they are essential skills with supporting the Board and regulatory response in a crisis, but equally so in building trust at normal times.

The aim is to complement cybersecurity needs and activities that support the business strategic goals. This often means honest and upfront discussions to debate, ensuring self-challenge and independence (also from a different vendor perspective so no marking your own homework).

UK, US, and EU legislation is a key driver in the push for resiliency. The requirements for financial services firms in particular reference the need to prevent disruption, set impact tolerance, perform mapping and testing, identify vulnerabilities, exercise regularly, and perform lessons learned activities.[10]

By embracing digital resilience, we can protect critical assets. This enables us to safeguard our digital assets, including data, systems, and infrastructure, from cyber threats, unauthorised access, and malicious activities. Digital resilience ensures business continuity. Thus, we can maintain operations and minimise downtime in the face of disruptions, enabling us to continue delivering products and services to our customers without interruption. Through resilience we can mitigate risks. Identify, assess, and proactively address potential risks and vulnerabilities before they escalate into major incidents, reducing the likelihood and impact of disruptions. Greater resilience fosters

agility and adaptability. We develop the ability to quickly adapt to changing circumstances, pivot strategies, and implement contingency plans, ensuring our organisations remain resilient and competitive in the face of evolving challenges. We can build trust and confidence. Thereby we can demonstrate to stakeholders, including customers, partners, and regulatory bodies, that our organisations prioritise resilience, thereby enhancing our reputation and fostering trust in our ability to operate securely and reliably.

By investing in digital resilience, we not only protect our organisations from potential threats and disruptions but also position ourselves for long-term success in the ever-changing digital landscape. In the digital age, cyber threats have become increasingly sophisticated and pervasive, posing significant risks to organisations of all sizes and industries.

Cyber, Operational, and Supply Chain Resilience

Cyber resilience is the ability to prepare for, respond to, and recover from cyber attacks and incidents, ensuring the confidentiality, integrity, and availability of our digital assets. Achieving cyber resilience requires a multi-layered approach that encompasses people, processes, and technology.

Implement robust cybersecurity measures to drive down risk. Deploy advanced security solutions, such as firewalls, antivirus software, intrusion detection and prevention systems, and encryption technologies, to protect our systems and data from cyber threats.

Foster a culture of cybersecurity awareness. Educate and train employees on cybersecurity best practices, including identifying and responding to potential threats, practising safe online behaviour, and adhering to security policies and procedures.

Develop incident response and recovery plans. Establish comprehensive incident response and recovery plans that outline clear protocols and procedures for detecting, containing, and mitigating cyber incidents, as well as restoring systems and data to operational status.

Regularly assess and test defences to find any awareness gaps. Conduct periodic risk assessments, vulnerability scans, and penetration testing to identify and address potential weaknesses in our cybersecurity posture, ensuring our defences remain effective against evolving threats.

Collaborate and share threat intelligence to learn and improve. Participate in industry-wide information-sharing initiatives and threat intelligence platforms to stay informed about emerging cyber threats and best practices for mitigating risks.

By prioritising cyber resilience, we can better protect our digital assets, safeguard sensitive information, maintain business continuity, and build trust with our stakeholders, ultimately positioning our organisations for long-term success in the digital age. In today's interconnected world, organisations rely heavily on complex systems, processes, and technologies to conduct their operations.

However, even the slightest disruption can have rippling effects, potentially leading to operational failures, financial losses, and reputational damage.

Operational resilience is the ability to anticipate, withstand, and recover from operational disruptions, ensuring the continuity of critical business functions and services.

Achieving operational resilience requires a holistic approach that encompasses people, processes, technology, and infrastructure. Identify and assess critical operations. Conduct a comprehensive risk assessment to identify and prioritise our critical operations, systems, and processes, enabling us to focus our resilience efforts on the areas that are most vital to our organisation's success. Develop and implement comprehensive business continuity and disaster recovery plans that outline strategies and procedures for maintaining essential operations and services in the event of disruptions, such as natural disasters, power outages, or system failures. Implement redundancy and failover mechanisms. Establish redundant systems, backup facilities, and failover mechanisms to ensure that critical operations can be quickly resumed or redirected in the event of a disruption, minimising downtime and service interruptions. Foster a culture of resilience to win hearts and minds. Cultivate a culture of resilience within our organisations by promoting awareness, training employees on emergency response procedures, and encouraging a mindset of continuous improvement and adaptation. Regularly test and update resilience plans. Conduct periodic testing and simulations of our business continuity and disaster recovery plans to identify and address any gaps or weaknesses, ensuring our plans remain effective and aligned with evolving operational requirements.

By embracing operational resilience, we can mitigate the impact of disruptions, maintain the continuity of critical operations, and protect our organisations from potential financial losses, legal liabilities, and reputational damage, ultimately fostering trust and confidence among our stakeholders.

In the globalised economy, supply chains have become increasingly complex and interconnected, spanning multiple countries and involving numerous suppliers, manufacturers, and logistics providers. However, this intricate network also introduces vulnerabilities and potential points of failure that can disrupt the flow of goods and services, impacting our ability to meet customer demands and maintain business continuity.

Supply chain resilience is the ability to anticipate, adapt to, and recover from disruptions within the supply chain, ensuring the continuous and efficient flow of materials, products, and services. Building supply chain resilience requires a proactive and holistic approach. Visibility and transparency must be considered. Implement robust supply chain management systems and technologies that provide end-to-end visibility and transparency across the entire supply chain, enabling us to monitor and track the movement of goods, identify potential bottlenecks or disruptions, and make informed decisions.

Risk assessment and mitigation must be continuous. Conduct comprehensive risk assessments to identify potential vulnerabilities and points of failure within our supply chains, such as natural disasters, political instability, or supplier issues. Develop contingency plans and mitigation strategies to address these risks proactively.

Diversification and redundancy can reduce risk. Diversify our supplier base and establish redundant sources of supply to reduce our reliance on single suppliers or geographic regions, mitigating the impact of localised disruptions and ensuring continuity of supply.

Collaboration and information sharing can build trust. Foster strong collaborative relationships with suppliers, logistics providers, and other stakeholders within the supply chain. Establish effective communication channels and information-sharing platforms to facilitate timely decision-making and coordinated responses to disruptions.

Agility and flexibility are necessary for adaptation. Cultivate agility and flexibility within our supply chain operations, enabling us to quickly adapt to changing market conditions, customer demands, or disruptions by rapidly shifting production, adjusting transportation routes, or implementing alternative sourcing strategies.

By prioritising supply chain resilience, we can minimise the impact of disruptions, ensure the continuous flow of goods and services, maintain customer satisfaction, and protect our organisations from financial losses and reputational damage, ultimately gaining a competitive advantage in the global marketplace.

Challenges and Strategies

While the benefits of digital resilience are clear, organisations often face several challenges in their efforts to build and maintain resilience across cyber, operational, and supply chain domains. Understanding these challenges is crucial for developing effective strategies and overcoming potential obstacles.

Complexity and interconnectivity of systems, processes, and supply chains are only increasing and these make it difficult to identify and mitigate potential vulnerabilities and points of failure, requiring a holistic and comprehensive approach to resilience.

The evolving threat landscape means that cyber threats, operational risks, and supply chain disruptions are constantly evolving, necessitating continuous monitoring, adaptation, and investment in resilience measures to stay ahead of emerging challenges.

Siloed organisational structures are challenging. Many organisations operate in siloed structures, with different departments or functions responsible for cyber security, operational continuity, and supply chain management. Bridging these silos and fostering cross-functional collaboration is essential for building a cohesive and integrated approach to digital resilience.

Resource constraints hamper risk reduction. Implementing robust resilience measures often requires significant financial investment, skilled personnel, and dedicated resources, which can be challenging for organisations with limited budgets or resource constraints.

Cultural resistance can hinder improvement. Fostering a culture of resilience requires a mindset shift and buy-in from all levels of the organisation, including leadership, employees, and stakeholders. Overcoming cultural resistance and promoting a resilience-focused mindset can be a significant challenge.

Regulatory and compliance requirements must be considered. Organisations must navigate a complex landscape of regulatory and compliance requirements related to data protection, cybersecurity, operational continuity, and supply chain management, which can add complexity and additional challenges to building digital resilience.

Vendor and third-party dependencies can be highly complex. Many organisations rely on third-party vendors, suppliers, and service providers, introducing potential vulnerabilities and risks that must be carefully managed and mitigated as part of the overall resilience strategy.

By understanding and addressing these challenges proactively, organisations can develop comprehensive and effective strategies for building and maintaining digital resilience, ensuring they are well-prepared to navigate the complexities of the digital age.

Strategies for developing digital resilience must be considered. Building digital resilience is a multifaceted endeavour that requires a strategic and holistic approach. By implementing strategies, organisations can enhance their resilience across cyber, operational, and supply chain domains.

Establishing a resilience-focused culture is vital so we must win hearts and minds. Foster a culture of resilience throughout the organisation by promoting awareness, training, and continuous improvement. Encourage open communication, collaboration, and a shared responsibility for resilience among all employees and stakeholders.

Develop a comprehensive resilience framework in order to reduce blindspots in a systematic way. Create a comprehensive resilience framework that encompasses cyber security, operational continuity, and supply chain resilience. This framework should outline policies, procedures, and guidelines for identifying, assessing, and mitigating risks, as well as responding to and recovering from incidents or disruptions.

Implement robust risk management practices to ensure risks are properly recorded and managed, and decisions can be audited. Conduct regular risk assessments to identify potential vulnerabilities and threats across cyber, operational, and supply chain domains. Develop and implement risk mitigation strategies, including contingency plans, redundancy measures, and incident response protocols.

Leverage advanced technologies to improve decision-making. Invest in and adopt advanced technologies that can enhance resilience, such as cloud

computing, automation, artificial intelligence, and blockchain. These technologies can provide scalability, redundancy, and improved visibility and transparency across systems and supply chains.

Foster collaboration and information sharing. Establish strong partnerships and collaborations with industry peers, government agencies, and other stakeholders. Participate in information-sharing initiatives and threat intelligence platforms to stay informed about emerging risks and best practices for building resilience.

Conduct regular testing and simulations to better understand weaknesses. Regularly test and simulate potential cyber incidents, operational disruptions, and supply chain challenges to validate the effectiveness of resilience measures and identify areas for improvement. Use these insights to refine and enhance resilience strategies continuously.

Invest in employee training and awareness as people are important assets. Provide ongoing training and awareness programmes to educate employees on cyber security best practices, operational continuity procedures, and supply chain resilience measures. Empower employees to be proactive in identifying and mitigating potential risks.

Embrace agility and adaptability. Cultivate a mindset of agility and adaptability within the organisation, enabling rapid response and adaptation to changing circumstances, evolving threats, and emerging disruptions. Encourage continuous improvement and innovation in resilience strategies.

By implementing these strategies, organisations can develop a comprehensive and robust approach to digital resilience, ensuring they are well-prepared to navigate the complexities of the digital age and maintain business continuity in the face of cyber, operational, and supply chain challenges.

Tools and technologies for enhancing digital resilience play a vital role. In the pursuit of digital resilience, organisations can leverage a range of tools and technologies to enhance their capabilities across cyber, operational, and supply chain domains. These tools and technologies can provide advanced protection, improved visibility, and streamlined processes, enabling organisations to proactively identify and mitigate risks, respond effectively to incidents, and recover quickly from disruptions.

Cybersecurity solutions are crucial in improving resilience. These solutions include firewalls and intrusion prevention systems (IPS), antivirus and anti-malware software, encryption technologies (data at rest and in transit), security information and event management (SIEM) tools and vulnerability scanning and penetration testing tools.

Business continuity and disaster recovery tools are vital in getting business operations back up and running so the business can recover quickly and ensure any disruption is minimised. These solutions include backup and recovery solutions, virtualisation and cloud-based technologies, failover and redundancy systems, incident response and crisis management platforms and emergency notification and communication tools.

Supply chain management solutions are an essential ingredient to ensuring the effective management of the supply chain. These include enterprise resource planning (ERP) systems, supplier relationship management (SRM) platforms, supply chain visibility and tracking tools, predictive analytics and risk modelling software, and blockchain-based supply chain solutions.

Automation and artificial intelligence are vital tools in ensuring businesses have agility in processing vast amounts of information and making decisions quickly. These include robotic process automation (RPA), machine learning and predictive analytics, chatbots and virtual assistants, and automated incident response and remediation.

Cloud computing and infrastructure is necessary to ensure systems can be joined up and prevent silos. These solutions include cloud-based storage and backup, cloud-based disaster recovery and business continuity services, cloud-based security and monitoring tools, and scalable and redundant cloud infrastructure.

Collaboration and information-sharing platforms are necessary to help in the identification and mitigation of risks as well as sharing best practice and learning. These include secure communication and collaboration tools, threat intelligence-sharing platforms, industry-specific information-sharing communities, and incident response and crisis management portals.

By leveraging these tools and technologies, organisations can enhance their visibility, automate processes, streamline incident response, and improve overall resilience across cyber, operational, and supply chain domains. However, it is crucial to carefully evaluate and select the appropriate solutions that align with the organisation's specific needs, requirements, and existing infrastructure.

Case Studies

Case studies can be helpful in providing practical examples of organisations that have developed strong digital resilience. To illustrate the importance and impact of digital resilience, let's explore real-world examples of organisations that have successfully navigated cyber, operational, and supply chain challenges through their resilience strategies.

Cyber Resilience: Maersk

In 2017, the global shipping giant Maersk was hit by the NotPetya ransomware attack, which crippled its IT systems and caused widespread disruptions across its global operations. However, Maersk's robust cyber resilience measures, including incident response plans, backup systems, and a culture of cyber awareness, enabled the company to recover quickly and minimise the impact of the attack.

Maersk's cyber resilience strategy included implementing advanced cybersecurity solutions and monitoring tools, conducting regular risk assessments,

and penetration testing. This strengthened the identification of cyber risks. They then established more effective incident response and recovery protocols and invested in employee training and awareness programmes. This improved response times to security incidents and reduced the level of human risk. They then leveraged cloud-based infrastructure and redundancy measures, improving technical controls.

Despite the initial disruption, Maersk's resilience efforts allowed the company to restore its systems and operations within 10 days, avoiding catastrophic financial losses and maintaining customer trust.

Operational Resilience: Southwest Airlines

In December 2022, Southwest Airlines faced a major operational disruption due to a winter storm that caused widespread flight cancellations and delays. However, the airline's robust operational resilience measures, including contingency planning and effective communication, enabled it to navigate the crisis and minimise the impact on customers.

Southwest Airlines' operational resilience strategy included developing comprehensive business continuity and disaster recovery plans, and implementing redundant systems and failover mechanisms. It was vital that the airline began fostering a culture of resilience and continuous improvement. They also began leveraging advanced technologies for real-time tracking and decision-making, and established effective communication channels with customers and stakeholders.

Through these resilience efforts, Southwest Airlines was able to quickly mobilise resources, adjust flight schedules, and provide timely updates to customers, minimising the overall impact of the disruption and maintaining customer loyalty.

Supply Chain Resilience: Toyota

Toyota, the world-renowned automotive manufacturer, has long been recognised for its resilient supply chain practices. In the aftermath of the 2011 Tohoku earthquake and tsunami in Japan, Toyota's supply chain resilience strategies enabled the company to recover and resume operations relatively quickly compared to its competitors.

Toyota's supply chain resilience approach included implementing end-to-end supply chain visibility and tracking systems. This improved understanding and visibility. They began diversifying their supplier base and establishing redundant sources. Most important was the culture change through fostering better, collaborative relationships with suppliers and logistics providers. They leveraged advanced analytics and risk modelling tools. They cultivated agility and flexibility throughout supply chain operations.

By prioritising supply chain resilience, Toyota was able to mitigate the impact of the natural disaster, maintain production levels, and meet customer demand, demonstrating the competitive advantage of a resilient supply chain.

These case studies highlight the tangible benefits of investing in digital resilience and serve as inspiration for organisations seeking to navigate the complexities of the digital age successfully.

International Standards

International standards are created by a group of stakeholders through a consensus process, adhering to strict rules for development, commenting, balloting, and approval. These standards are designed to be globally applicable, without any country- or region-specific requirements or language.

Standards from international standards groups will be referenced. They include:

- *ISO* – International Organization for Standardization (ISO) is an independent, non-governmental international body with 167 national standards organisations as members.[11] Technical committees and subcommittees bring together experts to share knowledge and create voluntary, consensus-based, market-relevant international standards that foster innovation and offer solutions to global challenges.
- *IEC* – International Electrotechnical Commission (IEC) was founded in 1906, and is the world's leading organisation for the preparation and publication of international standards for all electrical, electronic, and related technologies.[12] The IEC is one of three global sister organisations (IEC, ISO, ITU) that develop international standards for the world. When appropriate, IEC cooperates with ISO or ITU to ensure that international standards fit together seamlessly and complement each other.
- *NIST* – National Institute for Standards and Technology (NIST) publishes cybersecurity recommendations primarily for the US federal government and its contract organisations.[13] They are generally mandatory for US federal agencies and are often adopted by private industry. The NIST SP 800 (Special Publication 800) series documents include the NIST Risk Management Framework and Cyber Security recommendations. The NIST SP 800 series covers a variety of security tasks, including risk management, incident response, security controls, and recommended practices.[14]

ISO 22300

The ISO 22300 series is part of the Societal Security family of standards, focusing on business continuity.

ISO 22301

ISO 22301 outlines a general framework that organisations can use to establish a business continuity management system. At a high level, business continuity management involves identifying an organisation's key products or services and the activities needed to deliver them. Therefore they must understand restoration priorities and necessary resources. In order to improve business continuity they must also recognise the threats to business activities, the dependencies between them and other organisations, and the impacts of not resuming them. They must test arrangements (processes, agreements, etc.) to resume activities after an incident. It is then they can review and update the arrangements to ensure they will be effective when needed.

The standard outlines seven areas to consider when developing a business continuity plan:

Context – formally document and understand the organisation's functions; identify the organisation's risk appetite; understand legal and regulatory requirements and constraints; and determine the scope of required business continuity.

Leadership – secure and understand management's commitment to business continuity; develop a business continuity policy; and assign organisational roles and responsibilities.

Planning – address risk and opportunities; define business continuity objectives; and develop plans to achieve the objectives.

Support – determine resources required to execute the business continuity plan; assure that personnel performing business continuity tasks are trained and competent; assure that employees are aware of the business continuity policy and plans, and understand their roles; develop communication plans, including what will be communicated and with whom to communicate; and develop and maintain formal documentation for the business continuity plan, including actions taken when executing the plan.

Operation – plan, implement, and control processes to carry out business continuity requirements; perform a business impact analysis and a risk assessment; prioritise business functions for recovery activities; select a strategy to achieve business continuity objectives; establish resource requirements; establish and implement procedures, including incident response structures, warning and communication, business continuity, and recovery; and exercise and test the business continuity plan on a periodic basis.

Performance evaluation – monitor, measure, analyse, and evaluate the business continuity processes and plans; perform internal audits to assess the business continuity plan; and perform management reviews to ensure the business continuity plan remains adequate and effective.

Improvement – update the business continuity plan in response to issues identified during periodic testing, auditing, or management review.

It follows the "plan–do–check–act" framework to categorise the process. The "plan" component is composed of the context, leadership, planning, and support areas; the "do" component is the operation area; the "check" component is the evaluation area; and the "act" component is the improvement area.

ISO 22313

ISO 22313 provides guidance on how to implement the framework described in ISO 22301 by offering recommendations and suggestions for each area of the framework.

ISO 22316

ISO 22316 provides guidance on assessing an organisation's resilience. It offers specific guidance in three major areas:

Principles – including general principles and a coordinated approach.

Attributes for organisational resilience – including general attributes; shared vision and clarity of purpose; understanding and influencing context; effective and empowered leadership; a culture supportive of organisational resilience; shared information and knowledge; availability of resources; development and coordination of management disciplines; supporting continual improvement; and the ability to anticipate and manage change.

Evaluating the factors that contribute to resilience – including general factors; organisational requirements; monitoring and assessment; and reporting.

ISO 22317

ISO/TS 22317 provides guidance on establishing, implementing, and maintaining a business impact analysis process that can be used in support of the operation component of ISO 22301.

It sets out a series of prerequisite tasks and resources, and offers guidance on conducting the analysis.

Prerequisite tasks and resources encompass *defining the context and scope* for business continuity and thereon *establishing business continuity programme roles*, including roles and responsibilities; roles and competencies; programme commitment, and programme resources.

The analysis process involves project planning and management. Prioritising products and services is the next important step. Prioritising processes is crucial for effective management. The next step is prioritising activities. Analysis and consolidation of these is crucial. Securing top management endorsement of results is important for maintaining support. Thereafter the

business continuity strategy can be selected and agreed with senior stakeholders.

The standard also advises that the business impact analysis process be monitored and reviewed periodically (typically annually) or following an organisational change.

Other ISO/IEC 22300 Family Standards

The ISO 22300 family includes several standards which can be considered in terms of relevance to the project. These standards provide guidance in areas such as export interoperability for video surveillance, examination of existing available technologies, planning mass evacuations, and supply chain continuity. Other standards that could be considered include planning for the involvement of spontaneous volunteers, incident response, public warning, colour-coded alerts, and capability assessment. There are some other standards which may be pertinent such as monitoring facilities with identified hazards, human aspects of business continuity, message structure for information exchange, establishing partnering arrangements, and conducting exercises.

ISO 27001 and ISO 27002

The core components of the family are standards ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC 27001 provides a high-level overview of the seven elements of an information security management programme. It then offers a high-level description of the security requirements, grouped as 14 security control objectives containing 35 major categories, and 114 high-level control areas (as of 2018).

ISO/IEC 27002 offers further implementation guidance for each of the 114 high-level control statements outlined in ISO/IEC 27001, with some areas presenting multiple implementation options.

There are seven elements of an information security management system described in ISO/IEC 27001. *Context of the organisation* includes understanding the organisation and its context; understanding the needs and expectations of interested parties; determining the scope of the information security management system; and information security management system. *Leadership* includes leadership and commitment; policy; and organisational roles, responsibilities, and authorities. *Planning* includes actions to address risks and opportunities (general; information security risk assessment; information security risk treatment); and information security objectives and planning to achieve them. *Support* includes resources; competence; awareness; communication; and documented information. *Operation* includes operational planning and control; information security risk assessment; and information security risk treatment. *Performance evaluation* includes

monitoring, measurement, analysis, and evaluation; internal audit; and management review. *Improvement* including nonconformity and corrective action; and continual improvement.

There are 14 control objectives from ISO/IEC 27001 and IEC/ISO 27002. *Information security policies* include management direction for information security. *Organisation of information security* includes internal organisation, mobile devices, and teleworking. *Human resource security* includes security prior to employment, during employment, and after termination and change of employment. *Asset management* includes responsibility for assets, information classification, and media handling. *Access control* includes business requirements of access control, user access management, user responsibilities, and system and application access control. *Cryptography* is crucial and this includes cryptographic controls. *Physical and environmental security* is vital, including secure areas and equipment. *Operations security* is important, including operational procedures and responsibilities; protection from malware; backup; logging and monitoring; control of operational software; technical vulnerability management; and information systems audit considerations. *Communications security* includes network security management, and information transfer. *System acquisition, development, and maintenance* is an important area, including security requirements of information systems; security in development and support processes; and test data. *Supplier relationships* are increasingly important, including information security in supplier relationships; and supplier service delivery management. *Information security incident management* includes management of information security incidents and improvements. *Information security aspects of business continuity management* must be considered and include information security continuity and redundancies. *Compliance* is a crucial area, including compliance with legal and contractual requirements, and information security reviews.

NIST SP 800–34

NIST SP 800–34, last updated in 2010, provides guidance for contingency planning for information systems. It focuses on contingency planning activities to recover from disruption of client/server systems, telecommunications systems, and mainframe systems. The guide supports the "contingency planning control" components of NIST SP 800–53, offering advice.

Digital resilience is crucial in today's rapidly evolving digital landscape. Advice is shared in this book based on best practice and international standards to help you build and maintain resilience across cyber, operational, and supply chain domains.

Don't wait until it's too late. Take proactive steps to safeguard your digital assets, ensure business continuity, and foster long-term success. In the digital age, resilience is not just a luxury; it is an essential prerequisite for survival and

success. By embracing the principles of digital resilience, we can navigate the complexities of cyber threats, operational disruptions, and supply chain challenges with confidence and agility. Through a proactive and holistic approach, leveraging advanced tools and technologies, and fostering a culture of resilience, we can fortify our organisations against potential risks and position ourselves for long-term growth and prosperity.

Remember, resilience is an ongoing journey, and complacency is our greatest enemy. By continuously adapting, learning, and improving our resilience strategies, we can stay ahead of emerging threats and maintain a competitive edge in the ever-changing digital landscape.

Notes

1 Boh, W., Constantinides, P., Padmanabhan, B., and Viswanathan, S., 2023. Building Digital Resilience against Major Shocks. *Mis Quarterly*, 47(1), pp.343–360.
2 Abidi, N., El Herradi, M., and Sakha, S., 2022. Digitalisation and Resilience: Firm-level Evidence during the COVID-19 Pandemic. International Monetary Fund.
3 Florkowski, M., Hayashi, H., Matsuda, S., Moribe, H., Moriwaki, N., Jones, D., and Pauska, J., 2024. Digitally Boosted Resilience: Digitalization to Enhance Resilience of Electric Power System. *IEEE Power and Energy Magazine*, 22(2), pp.100–109.
4 He, Z., Huang, H., Choi, H., and Bilgihan, A., 2023. Building Organisational Resilience with Digital Transformation. *Journal of Service Management*, 34(1), pp.147–171.
5 Kashem, M.A., Shamsuddoha, M., and Nasir, T., 2024. Digital-Era Resilience: Navigating Logistics and Supply Chain Operations after COVID-19. *Businesses*, 4 (1), pp.1–17.
6 Lee, J.Y.H., Chou, C.Y., Chang, H.L., and Hsu, C., 2024. Building Digital Resilience Against Crises: The Case of Taiwan's COVID-19 Pandemic Management. *Information Systems Journal*, 34(1), pp.39–79.
7 https://www.iso.org/standard/50267.html.
8 https://www.iso.org/standard/75106.html.
9 https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework.
10 www.fca.org.uk/firms/operational-resilience.
11 https://www.iso.org/home.html.
12 https://www.iec.ch/homepage.
13 https://www.nist.gov.
14 https://csrc.nist.gov/publications/sp800.

2

OPERATIONAL RESILIENCE AND BUSINESS CONTINUITY PLANNING

Operational Resilience

Operational resilience is a key imperative that comes to the fore at this juncture. Operational resilience refers to an organisation's ability to anticipate, withstand, and recover from disruptions while continuing to deliver its products or services at an acceptable level.

Cui et al. (2023) argue that building operational resilience in businesses is vital to avoid being extremely vulnerable to disruption and that digital technologies are highly effective at building resilience within the firm and its supply chain. Without this, information complexities will leave an organisation caught adrift in a highly disruptive event.[1]

Organisations face a myriad of challenges that can disrupt their operations and threaten their continuity. From natural disasters and cyber attacks to supply chain disruptions and regulatory changes, the risks are numerous and varied. As such, building operational resilience has become a crucial imperative for businesses of all sizes and across all industries.

Xi et al. (2024) argue operational resilience can be further improved by incorporating greater digital technologies such as AI to improve business intelligence and to automate key aspects of resilience improvements. They research intelligent manufacturing and its use of digital technologies, which they conclude has significantly improved operational resilience overall.[2]

Boh et al. (2023) contend that digital resilience initiatives do require entities to consider and embrace important trade-offs regarding short- vs long-term planning horizons, efficiency vs flexibility, and independence vs interdependence.[3]

Operational resilience is a proactive approach that involves identifying potential risks, developing contingency plans, and implementing strategies to mitigate the impact of disruptive events.

He et al. (2023) contend transformation leadership enables the organisation to embrace employees with innovativeness and help employees grow

DOI: 10.4324/9781003604969-2

their capabilities when facing crises. The dimensions of operational resilience have clear influences on the organisation and employees.[4]

By fostering operational resilience, businesses can not only survive challenging times but also emerge stronger and better prepared to navigate future uncertainties. We must explore the key components of operational resilience, its importance in ensuring business continuity, and practical strategies for implementing and maintaining a robust resilience framework.

Atadoga et al. (2024) argue emerging technologies such as Internet of Things (IoT), AI, and blockchain can help improve intelligence, data gathering, secure data sharing, and continuous risk assessment, which can improve operational and supply chain resilience.[5]

Shahzad et al. (2024) insist blockchain can be highly effective in improving both operational resilience and supply chain resilience and improving the security of information sharing.[6]

Business Continuity

Business continuity is a critical aspect of operational resilience, as it focuses on maintaining essential business functions and processes during and after a disruptive event. A comprehensive business continuity plan outlines the strategies, procedures, and resources necessary to ensure the continuity of critical operations and the recovery of disrupted systems and processes.

Steen et al. (2024) emphasise business continuity fits into the framework of operational resilience and that this combined approach allows for a shift in thinking from control to flexibility and from accountability to adaptability, thereby enhancing the capacity for "anticipated improvisation" during crises.[7]

Onazi (2024) argues effective business continuity planning involves identifying critical business functions, assessing potential risks and their impact, developing recovery strategies, and establishing communication protocols. It also includes provisions for data backup and recovery, alternative work arrangements, and the allocation of necessary resources to support continuity efforts.[8]

By having a well-designed business continuity plan in place, organisations can minimise downtime, reduce financial losses, maintain customer confidence, and protect their reputation in the face of disruptions.

In today's volatile and unpredictable business environment, the importance of operational resilience cannot be overstated. Challenging times, such as economic downturns, pandemics, natural disasters, or cyber threats, can have far-reaching consequences for businesses, potentially leading to operational disruptions, financial losses, and reputational damage.

Operational resilience enables organisations to adapt and respond effectively to these challenges, ensuring that critical functions and services remain available to customers, stakeholders, and employees. By proactively

identifying and mitigating risks, implementing robust contingency plans, and fostering a culture of resilience, businesses can navigate through turbulent periods with minimal disruption and maintain their competitive edge.

Moreover, operational resilience contributes to long-term sustainability and growth by enhancing an organisation's ability to recover quickly from setbacks, seize new opportunities, and adapt to changing market conditions. It also instils confidence in stakeholders, customers, and regulatory bodies, demonstrating the organisation's commitment to risk management and business continuity.

Building operational resilience involves several key components that work together to create a comprehensive and effective framework. These components include risk assessment and management, business impact analysis (BIA), incident response and crisis management, business continuity (BC) and disaster recovery (DR) planning, supply chain resilience, cyber resilience, workforce resilience, and crucially, governance and oversight.

Each of these components plays a crucial role in identifying potential risks, developing mitigation strategies, and ensuring the continuity of critical operations during and after disruptive events.

Effective risk assessment and management are foundational elements of operational resilience. This process involves identifying potential risks that could disrupt business operations, analysing their likelihood and impact, and developing strategies to mitigate or manage those risks.

Risk assessment should be a collaborative effort involving stakeholders from various departments and functions within the organisation. It should consider a wide range of risks, including natural disasters, cyber threats, supply chain disruptions, regulatory changes, and geopolitical events.

Once risks have been identified and assessed, organisations can develop and implement risk management strategies tailored to their specific needs. These strategies may include implementing robust cybersecurity measures, diversifying supply chains, and establishing alternative suppliers. Risk management will also involve developing contingency plans for critical business functions and investing in disaster recovery infrastructure. Implementing business continuity plans (BCPs) will be crucial to reduce risk and provide effective planning for risk events. Providing employee training and awareness programmes is very important for employees to understand their roles and responsibilities in the event a business continuity plan needs to be evoked.

Regular risk assessments and updates to risk management strategies are essential to ensure that organisations remain agile and responsive to emerging threats and changing business environments.

Lincke (2024) argues developing a comprehensive BCP is a cornerstone of operational resilience. It outlines the strategies, procedures, and resources necessary to maintain critical business functions and processes during and after a disruptive event.[9]

Developing an effective BCP involves several key steps. *Conducting a business impact analysis (BIA)* is a vital first step. The BIA identifies critical

business functions, their dependencies, and the potential impact of disruptions on those functions. *Identifying recovery strategies* is crucial. Based on the BIA, organisations can develop recovery strategies for critical functions, such as data backup and recovery, alternative work arrangements, and the allocation of necessary resources. *Establishing communication protocols* is important for effectiveness. Effective communication protocols ensure that stakeholders, employees, and customers are kept informed during and after a disruptive event. *Defining roles and responsibilities* is essential for clarity. Clear roles and responsibilities should be assigned to individuals or teams responsible for executing the BCP. *Testing and updating the plan* is important to maintain control. Regular testing and updating of the BCP are essential to ensure its effectiveness and relevance in the face of changing business environments and emerging risks.

By developing and implementing a comprehensive BCP, organisations can minimise downtime, reduce financial losses, and maintain customer confidence during disruptive events.

Implementing business continuity strategies effectively is essential. Once a business continuity plan has been developed, it is essential to implement the strategies outlined in the plan effectively. *Allocating resources* is important, ensuring that the necessary resources, such as personnel, equipment, and facilities, are available to support business continuity efforts. *Establishing alternative work arrangements* helps in implementing remote work capabilities, identifying alternative work locations, and ensuring that employees have the necessary tools and resources to continue operations during disruptions. *Data backup and recovery* help businesses reduce risk as through the implementation of robust data backup and recovery solutions we can better protect critical data and ensure its availability during and after disruptive events. *Supply chain resilience* is important in diversifying supply chains, establishing alternative suppliers, and implementing strategies to mitigate supply chain disruptions. *Cyber resilience* means that by implementing robust cybersecurity measures, including incident response and recovery plans, we can better protect against cyber threats and ensure the continuity of critical systems and data. *Employee training and awareness* is vital as by providing regular training and awareness programmes we can ensure that employees understand their roles and responsibilities in supporting business continuity efforts. Effective implementation of business continuity strategies requires a collaborative effort across the organisation, involving stakeholders from various departments and functions.

Regular testing and reviewing of the BCP are essential to ensure its effectiveness and relevance in the face of changing business environments and emerging risks. Testing the BCP helps to identify potential gaps or weaknesses, validate assumptions, and ensure that the plan can be executed effectively in the event of a disruption. There are several approaches to testing a BCP. *Tabletop exercises* are very useful as these simulated scenarios allow

stakeholders to discuss and walk through the BCP, identifying potential issues and refining the plan. *Functional testing* is highly effective as this involves testing specific components or functions of the BCP, such as data backup and recovery procedures or alternative work arrangements. *Full-scale testing* is irreplaceable as a comprehensive test of the entire BCP: simulating a real-life disruptive event is highly effective to evaluate the organisation's readiness and response capabilities.

In addition to testing, it is essential to review and update the BCP regularly to ensure that it remains aligned with the organisation's current operations, risks, and business environment. This may involve incorporating lessons learned from testing or actual disruptive events. Businesses must update recovery strategies and procedures based on changes in technology or business processes. It is important to regularly review and update risk assessments and business impact analyses. Contact information and resource allocations must be kept up to date.

By regularly testing and reviewing the BCP, organisations can maintain a high level of operational resilience and be better prepared to respond effectively to disruptive events.

Case Studies

Case studies of successful operational resilience can be helpful here. Numerous organisations have demonstrated the value of operational resilience in navigating through challenging times and ensuring business continuity.

HSBC as a financial institution demonstrated resilience during the COVID-19 pandemic. As a bank they quickly adapted to remote work arrangements and implemented robust cybersecurity measures to maintain critical operations during the COVID-19 pandemic. Their business continuity plans and investments in technology enabled them to continue serving customers and maintaining regulatory compliance.

Volkswagen demonstrated the importance of good supply chain resilience in the automotive industry. They have implemented strategies to diversify their supply chains and establish alternative suppliers in response to disruptions caused by natural disasters, trade disputes, and other events. This has helped them mitigate the impact of supply chain disruptions and maintain production levels.

GSK plc have evidenced improvements in their cyber resilience. Health organisations have faced an increasing number of cyber threats, such as ransomware attacks and data breaches. GSK have moved in an agile way to implement robust cyber resilience strategies, including incident response plans and data backup and recovery solutions, which have ensured they are better equipped to protect data and maintain critical services.

Walmart has improved its disaster recovery capabilities. Major retailers like Walmart have invested in disaster recovery solutions, including data

centres in multiple geographic locations, to ensure the continuity of their e-commerce platforms and customer-facing systems during natural disasters or other disruptive events.

These case studies highlight the importance of operational resilience and the tangible benefits it can provide to organisations across various industries in the face of challenging circumstances.

Driving Culture Change

Building a *culture of operational resilience* is crucial. While implementing robust operational resilience strategies and plans is essential, fostering a culture of resilience within the organisation is equally important. Leadership commitment is essential. Senior leadership must champion operational resilience initiatives, allocate necessary resources, and communicate the importance of resilience to the entire organisation. Employee engagement and awareness is important to ensure everyone understands the role they play. Employees at all levels should be trained and made aware of their roles and responsibilities in supporting operational resilience efforts. This can be achieved through regular training, communication, and involvement in testing and exercises. Continuous improvement is vital as without this any plans are just pieces of paper. Organisations should continuously assess and improve their operational resilience strategies based on lessons learned, changes in the business environment, and emerging risks. Cross-functional collaboration is essential in order to bring key stakeholders on board. Operational resilience requires collaboration and coordination across various departments and functions, such as IT, finance, operations, and risk management. Developing a risk-aware mindset is important. Cultivating a risk-aware mindset among employees, where potential risks are identified and addressed proactively, can contribute to a more resilient organisation.

By fostering a culture of operational resilience, organisations can embed resilience into their DNA, ensuring that it becomes an integral part of their decision-making processes, operations, and overall business strategy. Operational resilience is no longer an option but a necessity for organisations seeking to ensure business continuity and long-term success. By proactively identifying and mitigating risks, developing robust business continuity plans, and implementing effective strategies, businesses can navigate through challenging times with minimal disruption and maintain their competitive edge.

Building operational resilience requires a comprehensive approach that involves risk assessment, business impact analysis, incident response planning, supply chain resilience, cyber resilience, and workforce resilience. It also necessitates regular testing and reviewing of business continuity plans to ensure their effectiveness and relevance.

Moreover, fostering a culture of operational resilience within the organisation is crucial. This involves leadership commitment, employee engagement

and awareness, continuous improvement, cross-functional collaboration, and a risk-aware mindset.

Ensuring uninterrupted operations is paramount to maintaining a competitive edge. Business continuity planning is a proactive approach that organisations adopt to mitigate potential disruptions and safeguard their operations from unexpected events. It involves creating a comprehensive strategy that outlines the necessary steps to maintain critical business functions and minimise the impact of disruptions on customers, employees, and stakeholders.

BCP is a crucial aspect of risk management, as it enables organisations to identify potential threats, assess their impact, and develop contingency plans to address them effectively. By implementing a well-crafted BCP, companies can enhance their resilience, protect their reputation, and ensure the continuity of essential services during times of crisis.

The Role of Suppliers

Understanding the importance of business continuity planning is necessary for suppliers. As a *supplier*, your role in the supply chain is critical, and any disruption to your operations can have far-reaching consequences for your customers and their businesses. Implementing a robust business continuity plan is essential to mitigate the risks associated with potential disruptions and ensure the uninterrupted delivery of goods or services to your clients.

Without a comprehensive BCP, suppliers may face significant challenges. Operational disruptions can have a significant impact on businesses and their profitability. Reputational damage can erode relationships with customers, suppliers, partners, and regulators. Financial losses can hamper cashflow and set back investment in growth opportunities. Contractual breaches can be the cause of legal disputes with suppliers and partners. Loss of customer trust is the natural byproduct of all of this. Customers vote with their feet and will walk away from organisations that have security breaches or business continuity problems.

By proactively addressing these risks through a well-designed BCP, suppliers can enhance their resilience, maintain their competitive advantage, and solidify their position as reliable partners in the supply chain.

The risks and challenges faced by suppliers without a BCP are huge. Suppliers without a robust BCP are vulnerable to a wide range of risks and challenges that can severely impact their operations and jeopardise their relationships with customers. These risks can stem from various sources, including natural disasters, cyber attacks, supply chain disruptions, and other unforeseen events.

Significant risks and challenges are faced by suppliers without a BCP. Operational disruptions are damaging. Without a contingency plan in place, suppliers may experience prolonged downtime, leading to delays in

production and delivery, which can have severe consequences for their customers' operations. Financial losses are the effect of disruptions which can result in lost revenue, increased costs, and potential contractual penalties, putting a strain on the supplier's financial stability. Reputational damage is caused by the failure to deliver goods or services on time. This can tarnish a supplier's reputation, making it challenging to retain existing customers and attract new ones. Supply chain disruptions are highly impactful. Suppliers are part of a larger supply chain ecosystem, and disruptions at their end can have ripple effects throughout the entire network, causing widespread disruptions and delays. Regulatory compliance issues can have a severe impact. Depending on the industry, suppliers may be subject to various regulatory requirements, and a lack of a BCP can lead to non-compliance and potential legal consequences.

By recognising these risks and challenges, suppliers can appreciate the critical importance of implementing a comprehensive BCP to safeguard their operations and maintain their position as reliable partners in the supply chain.

An effective BCP is a comprehensive and well-structured document that outlines the strategies, procedures, and resources necessary to ensure the continuity of critical operations during and after a disruptive event. Risk assessment helps to identify potential threats and analyse their impact on operations, supply chain, and customer relationships. BIA is important to determine the critical business functions, processes, and resources that must be prioritised and protected during a disruption. Recovery strategies are vital as we must develop strategies to restore and maintain critical operations, such as alternative suppliers, backup facilities, or outsourcing arrangements. Communication plans are vital to establish clear communication protocols to keep stakeholders, employees, and customers informed during a crisis. Incident response plans help to define procedures for responding to and managing various types of incidents, including roles and responsibilities. Testing is important so regularly test and update the BCP to ensure its effectiveness and relevance in the face of changing circumstances.

By incorporating these key components, suppliers can create a robust and adaptable business continuity plan that addresses their unique operational requirements and risk profile, ensuring their ability to maintain essential functions and minimise disruptions.

Conducting a comprehensive risk assessment is a crucial first step in developing an effective BCP for suppliers. This process involves identifying potential threats and analysing their impact on operations, supply chain, and customer relationships. By understanding the risks, suppliers can prioritise their mitigation efforts and allocate resources effectively.

The risk assessment process involves a sequence of activities. Identifying potential threats helps with the analysis. Compile a list of potential threats that could disrupt operations, such as natural disasters, cyber attacks, supply chain disruptions, or geopolitical events. Analyse likelihood and impact.

Assess the likelihood of each threat occurring and its potential impact on operations, finances, reputation, and customer relationships. Prioritise risks as not all risks can be dealt with at once. Rank the identified risks based on their likelihood and potential impact, allowing suppliers to focus their efforts on the most critical areas. Develop mitigation strategies based on prioritisation. For each prioritised risk, develop mitigation strategies to reduce the likelihood of occurrence or minimise the impact if the risk materialises. Continuous monitoring and review are crucial. Regularly monitor and review the risk assessment to ensure it remains relevant and up to date as circumstances change.

By conducting a thorough risk assessment, suppliers can gain a comprehensive understanding of the threats they face and develop targeted strategies to mitigate those risks, enhancing their overall resilience and ability to maintain operations during disruptive events.

Developing a business continuity strategy is pivotal. After conducting a comprehensive risk assessment, the next step in the business continuity planning process is to develop a robust strategy that outlines the specific actions and procedures to be taken in the event of a disruption. This strategy should be tailored to the unique needs and requirements of the supplier's operations, supply chain, and customer relationships.

The business continuity strategy for suppliers must focus on improving recovery. Critical business functions are those that are essential for core operations. Identify the essential business functions and processes that must be maintained or restored quickly to minimise disruptions and meet customer obligations. Recovery time objectives (RTOs) must be set. Establish realistic timeframes for restoring critical functions, taking into account the potential impact on customers and stakeholders. Recovery point objectives (RPOs) must be identified. Determine the acceptable amount of data loss or operational disruption that can be tolerated before significant consequences occur. Resource requirements should be considered. Assess the necessary resources, such as personnel, equipment, facilities, and technology, required to execute the business continuity strategy effectively. Alternative suppliers and contingency plans must be considered. Identify alternative suppliers or contingency plans for obtaining critical materials, components, or services in the event of a disruption in the primary supply chain. Communication protocols should be put in place. Establish clear communication protocols for disseminating information to employees, customers, and stakeholders during a crisis, ensuring transparency and effective coordination.

By developing a comprehensive business continuity strategy, suppliers can proactively address potential disruptions and minimise their impact on operations, customers, and stakeholders, ultimately enhancing their resilience and competitiveness in the market.

Implementing and testing the BCP is the next step. Once the BCP has been developed, it is crucial to implement and regularly test it to ensure its

effectiveness in the event of an actual disruption. Implementing the plan relies on key measures being taken. Training and awareness is an essential component. Conduct training sessions for all employees to ensure they understand their roles and responsibilities in executing the BCP. Raise awareness about the importance of the BCP and its potential impact on the organisation. Resource allocation must be assessed. Allocate the necessary resources, such as personnel, equipment, facilities, and technology, to support the implementation and ongoing maintenance of the BCP. Documentation and communication must provide clarity. Document the BCP in a clear and accessible format, and ensure it is communicated to all relevant stakeholders, including employees, customers, and partners. Testing and validation are crucial in providing assurance. Regularly conduct simulations, tabletop exercises, and live tests to validate the effectiveness of the BCP and identify areas for improvement. Testing should cover various scenarios, including IT system failures, supply chain disruptions, and natural disasters. Continuous improvement offers the opportunity of review and embedding learning. Based on the results of testing and feedback from stakeholders, continuously review and update the BCP to ensure it remains relevant and effective in addressing evolving risks and challenges.

By implementing and testing the BCP, suppliers can ensure that their strategies and procedures are well understood, properly executed, and capable of minimising the impact of disruptions on their operations and customer relationships.

To maximise the effectiveness of their business continuity planning efforts, suppliers should adopt best practices. Engage key stakeholders, including employees, customers, and partners, in the development and testing of the BCP to ensure their perspectives and requirements are considered. Align with industry standards and regulations related to business continuity planning, such as ISO 22301 or industry-specific guidelines. Leverage technology solutions, such as cloud-based services, remote work capabilities, and advanced data backup and recovery systems, to enhance the resilience and flexibility of operations. Foster collaboration and information sharing with partners, suppliers, and customers to ensure a coordinated and effective response to disruptions across the supply chain. Identify and prioritise the most critical business functions and processes, allocating resources accordingly to ensure their continuity during a disruption. Treat the BCP as a living document: regularly review and update it to reflect changes in the business environment, risks, and operational requirements. Cultivate a culture of resilience within the organisation, encouraging employee awareness, participation, and continuous improvement in business continuity planning efforts.

By adopting these best practices, suppliers can enhance the effectiveness of their business continuity planning efforts, ensuring they are well prepared to navigate disruptions and maintain uninterrupted operations, ultimately strengthening their position as reliable partners in the supply chain.

To support their business continuity planning efforts, suppliers can leverage a variety of tools and resources. Business continuity planning software is very useful. Specialised software solutions are designed to streamline the business continuity planning process, including risk assessment, plan development, testing, and maintenance. Numerous online resources offer templates, guides, and best practices for developing and implementing effective business continuity plans. Professional associations and regulatory bodies often provide guidance, standards, and resources specific to the supplier's industry or sector. Consulting services are widely available. Experienced consultants and firms specialising in business continuity planning can provide valuable expertise and support throughout the process. Various organisations offer training and certification programmes to equip suppliers with the knowledge and skills necessary for effective business continuity planning. Participating in peer networks and communities can facilitate knowledge sharing, collaboration, and best practice exchange among suppliers facing similar challenges.

By leveraging these tools and resources, suppliers can gain access to valuable insights, expertise, and support, enabling them to develop and implement robust BCPs tailored to their unique operational requirements and risk profiles.

In today's dynamic and interconnected business environment, ensuring uninterrupted operations is a critical imperative for suppliers. By implementing a comprehensive BCP, suppliers can proactively address potential disruptions, mitigate risks, and maintain their ability to deliver goods and services to customers without interruption.

Business continuity planning is not a one-time exercise but rather an ongoing process that requires regular review, testing, and updating to adapt to changing circumstances. By embracing best practices, leveraging available tools and resources, and fostering a culture of resilience, suppliers can enhance their preparedness and strengthen their position as reliable partners in the supply chain.

Remember, a well-executed BCP not only safeguards operations but also protects the supplier's reputation, customer relationships, and long-term competitiveness in the market. Invest in business continuity planning today to ensure your organisation is equipped to navigate disruptions and maintain uninterrupted operations, delivering value to your customers and stakeholders.

Notes

1 Cui, L., Wu, H., Wu, L., Kumar, A., and Tan, K.H., 2023. Investigating the Relationship between Digital Technologies, Supply Chain Integration and Firm Resilience in the Context of COVID-19. *Annals of Operations Research*, 327(2), pp.825–853.

2 Xi, M., Liu, Y., Fang, W., and Feng, T., 2024. Intelligent Manufacturing for Strengthening Operational Resilience during the COVID-19 Pandemic: A Dynamic

Capability Theory Perspective. *International Journal of Production Economics*, 267, p.109078.
3 Boh, W., Constantinides, P., Padmanabhan, B., and Viswanathan, S., 2023. Building Digital Resilience against Major Shocks. *Mis Quarterly*, 47(1), pp.343–360.
4 He, Z., Huang, H., Choi, H., and Bilgihan, A., 2023. Building Organisational Resilience with Digital Transformation. *Journal of Service Management*, 34(1), pp.147–171.
5 Atadoga, A., Osasona, F., Amoo, O.O., Farayola, O.A., Ayinla, B.S., and Abrahams, T.O., 2024. The Role of IT in Enhancing Supply Chain Resilience: A Global Review. *International Journal of Management & Entrepreneurship Research*, 6(2), pp.336–351.
6 Shahzad, K., Helo, P., Ranta, M., and Nousiainen, E., 2024. Blockchain Technology for Operational Excellence and Supply Chain Resilience: A Framework based on Use Cases and an Architecture Demonstration. *Technology Analysis & Strategic Management*, pp.1–18.
7 Steen, R., Haug, O.J., and Patriarca, R., 2024. Business Continuity and Resilience Management: A Conceptual Framework. *Journal of Contingencies and Crisis Management*, 32(1), p.e.12501.
8 Onazi, L., 2024. Business Impact Analysis (Bia)/Business Continuity Planning (Bcp). *Business Continuity Planning (Bcp)* (May 8).
9 Lincke, S., 2024. Addressing Business Impact Analysis and Business Continuity. In *Information Security Planning: A Practical Approach* (pp. 91–109). Cham: Springer International Publishing.

3

BUILDING SUPPLY CHAIN RESILIENCE

Supply Chain Management

Supply chain management (SCM) has emerged as a critical component for businesses across industries, playing a pivotal role in ensuring operational efficiency, cost optimisation, and customer satisfaction. As professionals in the field, we understand the intricate web of interconnected activities that span from raw material sourcing to final product delivery. Effective supply chain management is the backbone of any successful enterprise, enabling seamless coordination between various stakeholders, including suppliers, manufacturers, distributors, and customers.

Iftikhar et al. (2024) contend that strengthening supply chain resilience particularly through use of cyber resilience and emerging technologies can help in protecting supply chains from extremely disruptive shocks.[1]

In today's globalised and highly competitive business landscape, the ability to manage supply chains effectively can be a game-changer. Companies that excel in this area can gain a significant competitive advantage, reducing operational costs, minimising waste, and delivering products and services to customers promptly.[2] Conversely, organisations that fail to prioritise SCM often face challenges such as inventory imbalances, production delays, and customer dissatisfaction, ultimately hampering their growth and profitability.

Wang et al. (2022) purport it is vital that firms use digital technologies to monitor and control their supply chains and help build resilience.[3]

Alvarenga et al. (2023) argue building supply chain resilience and robustness is vital and the solution is using SCM in combination with building resilience through effective use of technology.[4]

As experienced CISO and Finance leaders, we recognise the importance of continuously improving and adapting to the ever-changing market dynamics.

DOI: 10.4324/9781003604969-3

By leveraging cutting-edge technologies, embracing sustainable practices, and fostering collaborations with key partners, businesses can unlock new opportunities for growth and innovation within their supply chains.[5]

Effective SCM is crucial for businesses to thrive in today's competitive landscape. It encompasses a wide range of activities, from procurement and logistics to inventory management and customer service. By optimising these processes, organisations can achieve significant benefits that directly impact their bottom line and customer satisfaction levels. Cost optimisation is important. Streamlining supply chain operations can lead to substantial cost savings through reduced inventory levels, minimised waste, and improved operational efficiencies. Effective supply chain management helps identify and eliminate bottlenecks, enabling businesses to operate more cost-effectively. Enhanced customer satisfaction can be valuable. By ensuring timely delivery of products and services, SCM plays a pivotal role in meeting customer expectations. Efficient supply chains enable businesses to respond quickly to changing market demands, adapt to fluctuations in consumer preferences, and provide superior customer service. In today's fast-paced business environment, agility and responsiveness are essential for success. Effective SCM allows organisations to rapidly adapt to changing market conditions, respond to disruptions, and capitalise on emerging opportunities, giving them a competitive edge over their rivals. Risk mitigation is a major benefit. Supply chains are vulnerable to various risks, including natural disasters, geopolitical tensions, and supplier disruptions. Robust SCM strategies help identify potential risks and implement contingency plans to mitigate their impact, ensuring business continuity and minimising financial losses.

By recognising the importance of effective SCM, businesses can unlock significant value, drive growth, and foster long-term sustainability within their operations.

SCM encompasses a multitude of interconnected components that work in harmony to ensure the efficient flow of goods, services, and information from the point of origin to the final consumer. As a supply chain professional, I understand the significance of each component and its role in contributing to the overall success of the supply chain. Procurement and sourcing is vital. This component involves identifying and selecting reliable suppliers, negotiating favourable terms, and ensuring the timely and cost-effective acquisition of raw materials, components, and services. Effective procurement strategies can significantly impact the overall supply chain performance. Production and manufacturing focuses on the transformation of raw materials into finished goods through various manufacturing processes. It involves capacity planning, quality control, and the implementation of lean manufacturing principles to optimise production efficiency and minimise waste. Inventory management is essential as maintaining optimal inventory levels is crucial for ensuring smooth operations and meeting customer demand. This component involves forecasting demand, managing stock levels, and

implementing inventory control strategies such as just-in-time (JIT) or vendor-managed inventory (VMI) systems. Logistics and transportation as a process encompasses the physical movement of goods from suppliers to manufacturing facilities, distribution centres, and ultimately to the end customers. It involves selecting appropriate transportation modes, optimising routes, and managing warehousing and distribution operations. Information and technology is vital as SCM heavily relies on the effective flow of information and data across all components. This component involves implementing robust information systems, integrating technology solutions, and leveraging data analytics to drive informed decision-making and continuous improvement. Effective SCM requires close collaboration and integration among all stakeholders, including suppliers, manufacturers, logistics providers, and customers. This component involves fostering strong partnerships, sharing information, and aligning processes to achieve common goals.

By understanding and effectively managing these key components, businesses can streamline their supply chain operations, enhance efficiency, and ultimately drive profitability and customer satisfaction.

Implementing effective SCM practices can yield numerous benefits for businesses, positively impacting various aspects of their operations. As a supply chain professional, I have witnessed firsthand the transformative power of well-executed supply chain strategies. Benefits are considerable. Operational efficiency can be achieved. By optimising processes, reducing waste, and eliminating redundancies, SCM enhances overall operational efficiency. This results in faster turnaround times, increased productivity, and better resource utilisation, ultimately leading to cost savings and improved profitability. Customer satisfaction can be enhanced. Efficient SCM ensures timely delivery of products and services, meeting or exceeding customer expectations. It also enables businesses to respond quickly to changing customer demands, fostering stronger relationships and brand loyalty. Competitiveness can be increased as companies with robust SCM practices can gain a competitive edge by offering shorter lead times, better product availability, and superior customer service. This can translate into increased market share and a stronger position in the industry. Inventory costs can be reduced. Effective inventory management strategies, such as JIT or VMI, help minimise excess inventory levels, freeing up working capital and reducing associated costs like storage, handling, and obsolescence. Risk management can be improved. SCM involves identifying and mitigating potential risks, such as supplier disruptions, transportation delays, or natural disasters. By implementing contingency plans and diversifying supply sources, businesses can enhance their resilience and ensure business continuity. Visibility and transparency can be enhanced. Advanced SCM systems and technologies provide real-time visibility into the flow of goods, materials, and information across the entire supply chain. This transparency enables better decision-making, proactive problem-solving, and continuous improvement. Modern SCM

practices emphasise sustainability and ethical sourcing, enabling businesses to minimise their environmental impact, promote social responsibility, and enhance their reputation among conscious consumers.

By embracing SCM best practices, businesses can unlock significant value, drive growth, and achieve a competitive advantage in their respective markets.

Within procurement, consideration of SCM principles as part of the procurement process can help assess and mitigate supply chain-related project risks, which is particularly important since challenges related to the supply chain are not expected to ease in the short term. Overall, SCM can help achieve business objectives. SCM makes the supply chain more resilient (e.g., creating a supply chain that can withstand shocks and disruptions). It helps with responding to supply chain disruptions (e.g., caused by COVID-19, natural catastrophes, delays at customs) and market distortions (e.g., a constrained global supply). SCM helps with addressing transportation challenges and delays (e.g., posed by more complex logistics arrangements and higher costs). It assists with managing increased delivery lead times (e.g., due to supply shortages or capacity limitations). SCM promotes environmental and social sustainability through the supply chain (e.g., by emphasising adequate labour standards, including employment terms and conditions, and occupational health and safety, and the importance of managing environmental impacts). It helps with monitoring project performance and completion according to specifications (e.g., on-time and on-budget performance, which can also be determined by the supply chain).

While the benefits of effective SCM are numerous, implementing and maintaining efficient supply chain practices can present various challenges. As a supply chain professional, I have encountered and navigated through challenges to ensure seamless operations. Globalisation and complexity are among the business challenges. As businesses expand their operations globally, supply chains become increasingly complex, involving multiple suppliers, manufacturers, and distribution channels across different countries and regions. Managing these intricate networks and ensuring compliance with diverse regulations and cultural norms can be a daunting task. Companies often depend on a global supply base. An overseas supplier or contractor might be cheaper, produce better quality, or simply be the only source for the needed input or service. However, an overseas supplier or contractor can also heighten the risk associated with the required input due to the physical distance, making it harder to control and monitor the supplier and the associated supply chain. Organisations should therefore aim to identify critical inputs and scrutinise the supplier's supply chain, particularly the geographic location of higher-tier suppliers or subcontractors and any risks that may be associated with, for instance, different legal systems in other countries, challenges related to border crossings, or reliable infrastructure and transportation. One factor driving globalisation and enabling it to be better managed is

information technology (IT). Coordination and interaction across multi-country supply chains can be facilitated with IT systems, enhancing visibility and transparency.

Supply and demand volatility is a serious challenge. Fluctuations in customer demand, market trends, and economic conditions can create imbalances in supply and demand, leading to excess inventory or stock shortages. Accurately forecasting demand and adapting supply chains to these fluctuations are constant challenges. Supply shortages can cause catastrophic failures. If a product or component does not arrive when needed, this may delay or even prevent the completion of an entire project. Supply shortages are often the reason for this delay, which can be triggered by challenges experienced by higher-tier suppliers or contractors or by unexpectedly high demand. For example, the COVID-19 pandemic led to many supply shortages. Increasingly longer and more complex supply chains, coupled with companies' attempts to be "lean" and efficient (i.e., carrying as little inventory as possible), have been increasing the risk of supply shortages. Organisations should therefore assess the supplier's supply chain to look for choke points that may lead to supply shortages, as well as the availability of inventory buffers to alleviate any shortages.

Technology integration and data management pose serious problems. Supply chain management relies heavily on technology and data integration across various systems and stakeholders. Ensuring seamless integration, data accuracy, and real-time visibility can be challenging, especially when dealing with legacy systems or disparate data sources.

Risk mitigation and disruption management in the supply chain are complex and difficult to resolve. Supply chains are vulnerable to various risks, such as natural disasters, geopolitical tensions, cyber threats, and supplier disruptions. Identifying and mitigating these risks, as well as developing contingency plans for business continuity, requires constant vigilance and proactive planning. Geopolitical events and other disruptions can be very damaging. Dispersed, worldwide supply chains are vulnerable to disruptions caused by geopolitical tensions and other events. Examples include trade sanctions, conflict, and the COVID-19 pandemic. Deliberate management of the supply chain is important to identify, mitigate, and manage such potential vulnerabilities.

Talent and skill gaps exist across the supply chain. As SCM evolves and becomes more complex, there is a growing need for skilled professionals with specialised knowledge and expertise. Attracting, retaining, and developing talent in this field can be a significant challenge for many organisations.

Sustainability and environmental concerns can clash with SCM. Businesses are under increasing pressure to adopt sustainable practices and minimise their environmental impact throughout the supply chain. Balancing sustainability goals with operational efficiency and cost considerations can be a delicate balance.

Supply Chain Risks

Third-party risk management can be a daunting task. Supply chains often involve multiple third-party partners, such as suppliers, logistics providers, and distributors. Managing and mitigating risks associated with these external partners, including compliance, quality, and security concerns, is a critical challenge.

To overcome these challenges, supply chain professionals must continuously adapt, innovate, and leverage best practices, technologies, and collaborative partnerships. By addressing these challenges head-on, businesses can build resilient and efficient supply chains that drive long-term success.

Dubey et al. (2023) argue government must do more to drive organisations to improve their supply chain resilience by enhancing digital adaptability and digital agility.[6]

Strategies for mitigating third-party risks in supply chain management must be given proper consideration. In today's interconnected business landscape, supply chains often involve numerous third-party partners, such as suppliers, logistics providers, and distributors. While these partnerships can bring significant benefits, they also introduce potential risks that need to be carefully managed. As a supply chain professional, I understand the importance of implementing effective strategies to mitigate third-party risks and ensure the integrity and resilience of the supply chain.

Comprehensive due diligence and vetting processes are essential. Before onboarding any third-party partner, it is crucial to conduct thorough due diligence assessments. This includes evaluating their financial stability, operational capabilities, compliance with regulations, and adherence to ethical and sustainability standards. A rigorous vetting process can help identify potential risks and ensure alignment with your organisation's values and requirements.

Robust contracts and service level agreements (SLAs) provide clarity. Clear and comprehensive contracts and SLAs are essential for defining expectations, responsibilities, and accountability with third-party partners. These agreements should outline performance metrics, quality standards, data security measures, and contingency plans for potential disruptions or non-compliance.

Continuous monitoring and performance evaluation are necessary to provide assurance. Regularly monitoring and evaluating the performance of third-party partners is crucial for identifying potential issues or risks before they escalate. This can involve conducting audits, reviewing performance metrics, and maintaining open communication channels to address concerns promptly.

Diversification and contingency planning improve preparedness. Overreliance on a single third-party partner can increase supply chain vulnerability. Diversifying your supplier base, logistics providers, and distribution channels can help mitigate risks and ensure business continuity in case of

disruptions. Additionally, developing contingency plans and alternative sourcing strategies can provide a safety net in case of unforeseen events.

Cybersecurity and data protection are important considerations. Supply chains involve the exchange of sensitive information and data with third-party partners. Implementing robust cybersecurity measures, such as encryption, access controls, and regular security audits, is essential to protect against data breaches, cyber threats, and intellectual property theft.

Collaborative partnerships and transparency are necessary in building healthy relationships. Building strong, collaborative partnerships with third-party partners based on trust and transparency can help mitigate risks. Open communication, information sharing, and joint problem-solving can foster a culture of accountability and enable proactive risk management.

Continuous improvement and adaptation are necessary to embed lessons learned. Supply chain risks are dynamic and ever-evolving. Regularly reviewing and updating risk mitigation strategies, incorporating lessons learned, and adapting to changing market conditions and emerging threats are crucial for maintaining supply chain resilience.

By implementing these strategies, businesses can effectively manage third-party risks, build resilient supply chains, and safeguard their operations, reputation, and long-term success.

Best practices for successful SCM provide a litmus test. Achieving success in SCM requires a combination of strategic planning, operational excellence, and continuous improvement. As a supply chain professional, I have witnessed firsthand the transformative impact of implementing best practices and tailoring these to the unique needs of each organisation.

Aligning supply chain strategy with business objectives is necessary to focus business efforts. Effective SCM starts with aligning the supply chain strategy with the overall business objectives and goals. This ensures that supply chain initiatives and investments are aligned with the company's strategic direction, enabling better resource allocation and decision-making.

Embracing collaboration and partnership helps address mutual problems and provide mutual support. Supply chains involve multiple stakeholders, including suppliers, manufacturers, logistics providers, and customers. Fostering collaborative partnerships based on trust, transparency, and shared goals can lead to improved efficiency, innovation, and risk mitigation.

By leveraging technology and data analytics, decision-making can be enhanced. Implementing advanced technologies, such as enterprise resource planning (ERP) systems, supply chain management software, and data analytics tools, can provide real-time visibility, optimise processes, and drive data-driven decision-making throughout the supply chain.

Adopt lean and agile principles to improve efficiency. Lean and agile methodologies, such as JIT production, continuous improvement (Kaizen), and value stream mapping, can help eliminate waste, reduce lead times, and increase responsiveness to changing customer demands.

Implement sustainable and ethical practices to enhance your brand. Incorporating sustainability and ethical practices into supply chain operations is not only beneficial for the environment and society but can also enhance brand reputation, attract conscious consumers, and drive long-term value creation.

Invest in talent development and training. SCM requires a skilled and knowledgeable workforce. Investing in talent development, training programmes, and continuous learning opportunities can help build a strong and capable supply chain team.

Measure and continuously improve through learning. Establishing key performance indicators (KPIs) and regularly measuring supply chain performance are crucial for identifying areas for improvement. Continuous improvement initiatives, such as process optimisation, risk management, and supplier performance evaluation, can drive ongoing efficiency and effectiveness.

Fostering supply chain resilience is vital. Building resilient supply chains involves identifying potential risks, developing contingency plans, and implementing strategies for risk mitigation and business continuity. This can include diversifying supplier bases, maintaining safety stocks, and investing in supply chain visibility and agility.

By embracing these best practices, organisations can optimise their supply chain operations, enhance competitiveness, and drive long-term success in an ever-changing business landscape.

Technologies and Tools

Technologies and tools for optimising SCM must be considered. In the modern era of globalisation and digital transformation, SCM has evolved to leverage cutting-edge technologies and tools to optimise operations, enhance visibility, and drive efficiency. As a resilience professional, I recognise the importance of embracing these technological advancements to stay ahead of the curve and gain a competitive edge.

ERP systems help with integration. ERP systems provide a centralised platform for managing and integrating various business processes, including supply chain management. These systems offer real-time visibility into inventory levels, order tracking, and financial data, enabling informed decision-making and streamlined operations.

SCM software assists with optimisation. Specialised SCM software solutions are designed to optimise supply chain processes, from procurement and logistics to inventory management and demand forecasting. These tools leverage advanced algorithms, analytics, and data integration to drive operational efficiency and cost savings.

Internet of Things (IoT) and sensor technology ensure data is constantly being gathered around the clock. IoT and sensor technology enable real-time

tracking and monitoring of assets, products, and shipments throughout the supply chain. By capturing data on location, temperature, humidity, and other environmental conditions, businesses can optimise logistics, prevent spoilage, and improve product quality.

Blockchain and distributed ledger technology can improve security. They offer enhanced transparency, traceability, and security in supply chain operations. By creating an immutable and decentralised record of transactions, these technologies can streamline processes, reduce fraud, and improve trust among supply chain partners.

Artificial intelligence (AI) and machine learning (ML) are vital emerging technologies. AI and ML algorithms can analyse vast amounts of supply chain data to uncover patterns, predict demand, optimise routes, and automate decision-making processes. These technologies can enhance forecasting accuracy, inventory management, and resource allocation, leading to improved efficiency and cost savings.

Robotics and automation offer huge potential to reduce labour costs and error. Robotic systems and automation technologies are transforming warehousing and distribution operations. Automated storage and retrieval systems (AS/RS), autonomous mobile robots (AMRs), and automated guided vehicles (AGVs) can increase productivity, reduce labour costs, and improve safety in supply chain operations.

Cloud computing and Software-as-a-Service (SaaS) allow us to break away from silo systems. Cloud-based solutions and SaaS platforms offer scalable and cost-effective ways to access SCM tools and services. These solutions enable real-time data sharing, collaboration, and accessibility from anywhere, promoting agility and responsiveness.

Big data and analytics allow us to identify hidden patterns. Supply chains generate vast amounts of data from various sources, such as sensors, ERP systems, and customer interactions. Big data analytics tools can process and analyse this data to uncover insights, identify trends, and optimise supply chain performance.

Groenewald et al. (2024) argue emerging technologies such as AI-powered supplier risk assessment could help organisations to improve speed and effectiveness in mitigating risks and ensure supply chain resilience. By leveraging these technologies and tools such as AI, supply chain professionals can unlock new levels of efficiency, visibility, and agility, enabling their organisations to stay ahead in an increasingly competitive and complex business landscape.[7]

Case Studies

SCM is hard to get right. To illustrate the transformative power of effective SCM, let's explore two case studies of companies that have excelled in this domain, driving significant business success and competitive advantage.

Case Study 1: Amazon's Logistics and Supply Chain Management

Amazon, the e-commerce giant, has long been recognised for its innovative and efficient SCM strategies. At the core of Amazon's success lies its relentless focus on customer satisfaction and operational excellence. By investing heavily in advanced technologies, automation, and data-driven decision-making, Amazon has revolutionised the way goods are sourced, stored, and delivered to customers.

One of Amazon's key strengths is its vast and highly automated fulfilment centre network. These state-of-the-art facilities leverage robotics, automated storage and retrieval systems, and advanced software to streamline order processing, inventory management, and shipping operations. This automation has enabled Amazon to handle millions of orders per day with remarkable speed and accuracy.

Additionally, Amazon's proprietary logistics and transportation network, which includes a fleet of planes, trucks, and delivery vans, has allowed the company to gain greater control over the last-mile delivery process. This vertical integration has significantly reduced reliance on third-party carriers, resulting in faster delivery times and improved customer experiences.

Another critical aspect of Amazon's supply chain success is its data-driven approach. The company leverages advanced analytics and ML algorithms to optimise inventory levels, forecast demand, and identify potential supply chain bottlenecks. This data-driven decision-making has enabled Amazon to maintain lean inventory levels while ensuring product availability, reducing costs, and minimising waste.

Furthermore, Amazon's commitment to sustainability and environmental responsibility has been a driving force behind its supply chain initiatives. The company has implemented various eco-friendly practices, such as optimising transportation routes, utilising renewable energy sources, and reducing packaging waste, all while maintaining operational efficiency.

By continuously innovating and investing in cutting-edge technologies, Amazon has set new standards for supply chain excellence, raising the bar for competitors and demonstrating the transformative power of effective SCM.

Case Study 2: Zara's Agile and Responsive Supply Chain

Zara, the Spanish fashion retailer, has gained global recognition for its ability to rapidly respond to changing fashion trends and consumer demands. At the heart of Zara's success lies its agile and responsive SCM strategy, which has allowed the company to bring new designs from concept to store in a matter of weeks.

One of Zara's key advantages is its vertically integrated supply chain, which encompasses design, production, and distribution. By maintaining

control over these critical processes, Zara can quickly adapt to market trends and minimise lead times. The company's design teams closely monitor consumer preferences and incorporate feedback into new product lines, enabling rapid design iterations and reduced time-to-market.

Zara's production facilities, located primarily in Spain and Portugal, are strategically positioned to support its agile supply chain model. By keeping a significant portion of its manufacturing operations close to its headquarters, Zara can respond swiftly to changing demands and minimise transportation times.

Additionally, Zara's inventory management strategy is driven by a "pull" system, where products are replenished based on real-time sales data from its retail stores. This demand-driven approach helps minimise excess inventory and reduces the risk of overstocking or understocking.

Zara's supply chain success is further bolstered by its use of advanced technologies and data analytics. The company leverages real-time sales data, forecasting algorithms, and integrated supply chain systems to optimise production planning, inventory levels, and distribution strategies.

By embracing agility, responsiveness, and data-driven decision-making, Zara has disrupted the traditional fashion industry supply chain model, enabling the company to consistently deliver fresh and on-trend products to its customers worldwide.

These case studies demonstrate the transformative power of effective supply chain management and the competitive advantages it can provide. By embracing innovation, leveraging advanced technologies, and fostering agility and responsiveness, businesses can optimise their supply chain operations, drive efficiencies, and ultimately enhance customer satisfaction and profitability.

To stay ahead in today's fast-paced and competitive business landscape, it is essential to prioritise supply chain excellence. Comprehensive SCM is vital in meeting business needs. Experienced supply chain professionals, backed by cutting-edge technologies and industry best practices, are crucial to streamline operations, mitigate risks, and unlock new levels of efficiency and profitability.

Supply Chain Vulnerabilities

Supply chain vulnerabilities can manifest in myriad forms, from natural disasters and geopolitical instabilities to cyber threats and regulatory shifts. These vulnerabilities can strike at any point along the supply chain, rippling through the entire ecosystem and potentially immobilising operations. Recognising and addressing these risks is not merely a matter of business continuity; it is a strategic imperative that can spell the difference between success and failure in an increasingly competitive and uncertain world.

Dubey et al. (2023) argue government must do more to drive organisations to improve their supply chain resilience by enhancing digital adaptability and digital agility.[8]

Hägele et al. (2023) emphasise the important of supply chain resilience and identifying vulnerabilities because in the intricate tapestry of modern business operations, supply chains form the backbone, weaving together a complex network of interdependencies. However, with complexity comes vulnerability, and the potential for disruptions lurks within the intricate web of processes and relationships that define SCM.[9]

Alvarenga et al. (2023) argue building supply chain resilience and robustness is vital.[10] As we navigate the ever-evolving landscape of global commerce, it becomes paramount to unearth these hidden vulnerabilities, empowering organisations to fortify their resilience and safeguard their operational integrity.

We will delve into the depths of supply chain vulnerabilities, shedding light on their impact, identifying common types, and equipping you with the tools and strategies necessary to assess and mitigate these risks. Through real-life case studies and expert insights, I aim to empower you with the knowledge and foresight to navigate the complexities of SCM, ensuring optimal resilience and long-term success.

Supply chain vulnerabilities can have far-reaching consequences that extend beyond the confines of a single organisation. When supply chains falter, the ripple effects can disrupt operations, erode customer confidence, and ultimately undermine profitability and market position. The impact of these vulnerabilities on businesses can manifest in various ways.

Operational disruptions are costly. Supply chain disruptions can grind production lines to a halt, leading to costly delays, missed deadlines, and unfulfilled customer orders. This can result in lost revenue, strained relationships with clients, and reputational damage.

Financial implications can be severe. Supply chain vulnerabilities can impose significant financial burdens on businesses. From increased costs associated with expedited shipping, alternative sourcing, and inventory management to potential penalties for late deliveries, the financial toll can be substantial.

Reputational harm can damage trust. In today's interconnected world, supply chain disruptions can quickly become public knowledge, potentially tarnishing a company's reputation and eroding consumer trust. This can have long-lasting effects on brand equity and market positioning.

Regulatory compliance risks must be taken into consideration. Supply chain vulnerabilities can expose businesses to regulatory non-compliance, potentially leading to hefty fines, legal disputes, and even temporary shutdowns in severe cases.

Competitive disadvantage should also be factored in. While some businesses proactively address supply chain vulnerabilities, those that fail to do so may find themselves at a competitive disadvantage, losing market share to more resilient competitors.

Recognising the far-reaching implications of supply chain vulnerabilities is the first step toward building a robust and resilient ecosystem capable of

withstanding the inevitable challenges that arise in the dynamic world of global commerce.[11]

Supply chain vulnerabilities can manifest in various forms, each presenting unique challenges and requiring tailored mitigation strategies. Understanding the common types of vulnerabilities is crucial for developing a comprehensive risk management approach.

Natural disasters are damaging. Extreme weather events, earthquakes, and other natural calamities can disrupt supply chains by damaging infrastructure, impeding transportation routes, and disrupting production facilities.

Geopolitical instabilities can have far-reaching effects causing damage across the world. Political unrest, trade disputes, and economic sanctions can create barriers to cross-border trade, disrupt supply lines, and introduce regulatory complexities.

Cyber threats are highly pervasive. The increasing reliance on digital systems and interconnected networks makes supply chains vulnerable to cyber attacks, data breaches, and system failures, potentially compromising sensitive information and disrupting operations.

Supplier risks can be unpredictable and cause damage that ripples across entire industries. Overreliance on a single supplier, inadequate supplier vetting processes, or financial instability among key suppliers can create vulnerabilities that ripple through the supply chain.

Transportation and logistics disruptions can cause significant disputes and supply-side shocks. Disruption in transportation networks, port congestion, or labour disputes can delay the movement of goods, leading to stockouts and production bottlenecks.

Regulatory changes can add complexities that can impact two seemingly similar companies in the same sector in different ways. Evolving regulations, trade policies, and compliance requirements can introduce complexities and necessitate operational adjustments, potentially disrupting established supply chain processes.

Quality control issues can erode trust and reputations faster than ever before. Lapses in quality control, counterfeit products, or defective components can compromise product integrity and lead to recalls, reputational damage, and potential legal liabilities.

Supply and demand volatility can lead to stockpiles or shortages. Sudden shifts in consumer demand, market trends, or supply shortages can strain supply chain capabilities and lead to inventory imbalances or stockouts.

By understanding these common vulnerabilities, organisations can proactively develop risk mitigation strategies and build resilience into their supply chain operations.

Identifying hidden risks in the supply chain is vital. While some supply chain vulnerabilities are readily apparent, others can remain hidden, lurking beneath the surface and posing insidious threats to operational continuity.

Identifying these hidden risks requires a proactive and comprehensive approach, leveraging various techniques and tools to uncover potential weaknesses and awareness gaps. Here are some strategies for uncovering hidden supply chain risks.

Supply chain mapping is essential. Develop a comprehensive map of your supply chain, including all tiers of suppliers, transportation routes, and distribution channels. This visual representation can help identify potential bottlenecks, single points of failure, and dependencies that may not be immediately apparent.

Supplier audits and assessments allow for proper scrutiny. Conduct thorough audits and assessments of your suppliers to evaluate their financial stability, operational capabilities, risk management practices, and compliance with industry standards and regulations. This can help identify potential vulnerabilities within your supplier network.

Data analytics and predictive modelling can develop unique insights. Leverage data analytics and predictive modelling techniques to analyse historical data and identify patterns, trends, and potential risk factors. This can provide valuable insights into hidden vulnerabilities and enable proactive risk mitigation strategies.

Mayur (2024) argues *scenario planning and stress testing* are vital and can help identify weaknesses and inform contingency planning.[12] Engage in scenario planning exercises and stress test your supply chain against various potential disruptions, such as natural disasters, cyber attacks, or regulatory changes.

Collaboration and information sharing enables better outcomes for everyone. Foster collaboration and information sharing with industry peers, trade associations, and government agencies. This can provide access to valuable intelligence and insights into emerging risks and best practices for risk mitigation.

Employee feedback and whistleblower programmes are helpful. Encourage employee feedback and implement whistleblower programmes to gather insights from those on the front lines of your operations. This can help uncover potential risks or issues that may not be visible from a top-down perspective.

Continuous monitoring and risk assessments accelerate learning. Implement a continuous monitoring and risk assessment process to regularly evaluate your supply chain for emerging vulnerabilities. This proactive approach can help identify risks before they escalate into full-blown disruptions.

By employing these strategies and embracing a culture of continuous improvement, organisations can enhance their ability to identify hidden risks and fortify their supply chain resilience.

Supply Chain Mapping

Supply chain maps enable organisations to pinpoint potential weak spots, which are critical weaknesses in the supply chain that could threaten the

project. Recognising these possible supply chain vulnerabilities allows organisations to concentrate their monitoring on the most fragile parts of the supply chain, create supply risk mitigation strategies if those vulnerabilities cause a disruption, and/or address the vulnerability by reinforcing that segment of the supply chain.

Data gathered through supply chain mapping can assist organisations in identifying vulnerabilities. By considering these supply chain characteristics, organisations can gain a clearer understanding of the dependencies and potential choke points and risks.

Organisations should be aware that, in most cases, it is not feasible to obtain complete information on all aspects of the supply chain. However, even limited insights, based on the available information, are better than none.

Supply chain maps are effective in identifying points of vulnerability. Supply chain characteristics can make the supply chain more or less vulnerable to disruptions.

The number of tiers in a supply chain has a considerable impact. The vulnerability of a supply chain increases with the number of tiers, due to the practical inability to control and gain insight into such complex supply chains. While in most cases it is impossible to obtain a complete picture of complex supply chains, organisations can regularly scan newspapers and other media that may provide information on disruptions that could potentially impact the industry and/or the supply chain – for instance, a ship blocking the Suez Canal, COVID-19 lockdowns, trade sanctions, or microchip/semiconductor shortages. Advanced technologies and analytics can also be used to obtain such insights.

The criticality of each supply chain tier is crucial. Where a supplier is the only organisation (i.e., a sole supplier) or one of the few organisations that can provide the input, the vulnerability of the supply chain increases. Vulnerability can be reduced by respecifying or redesigning the required input (e.g., via value engineering or value analysis) so that more suppliers are able to provide the component, thereby reducing supply chain vulnerability. The COVID-19 pandemic, for example, disrupted almost every supply chain, demonstrating to many organisations the benefits of dual- or multi-sourcing. Vulnerabilities were also discovered in the aftermath of the 2011 earthquake and subsequent tsunami in Japan, which also highlighted the risks of single-sourcing. For example, several automotive firms were not able to deliver cars in a certain paint colour (Tuxedo Black and Royal Red), since the sole supplier of those colour pigments had been impacted by the tsunami. It is important to learn from these experiences and design the supply chain to reduce risks to avoid further disruptions. In this case, organisations started to dual-source pigments, and, more broadly, design their other supply chains with resilience in mind. Toyota, for instance, credits the lessons learned from the 2011 earthquake with the firm being able to reduce the impact of the semiconductor shortages in 2021.

Relationships with suppliers can have a considerable effect. Strong business relationships can go a long way to dealing with supply chain vulnerabilities. If a vulnerability disrupts a supplier, a solid relationship can help the organisation get special treatment. For instance, once the supplier recovers and resumes production, the organisation might be the first to get shipments. The semiconductor shortage that began in 2021 was tackled by companies enhancing their supplier relationships through better information sharing, such as synchronised capacity planning, which boosts planning reliability and transparency.

Information visibility is crucial. Vulnerabilities can be better managed with improved data. This includes tracking and tracing shipments, early warning systems, and frequent status reports. Contracts with suppliers should specify what data should be available and when, and clearly outline the organisation's right to conduct inspections or audits. Commercial software solutions that offer this visibility are also available.

Prioritising SCM on vulnerability is a crucial step. Organisations can determine the importance of each supply chain by using an evaluation matrix to assess their vulnerability. The five dimensions (number of tiers, average tier criticality, geographic location, supplier relationship, information availability) can be rated on a 1–5 point scale, with these values being totalled for a combined score. The supply chain with the highest score would be the most vulnerable and thus the most deserving of scrutiny using this simple method. Different vulnerability ratings (e.g., high, medium, low) can also be assigned. In this example, the supply chain for medical equipment needs the most immediate attention.

Note that using a 5-point scale allows organisations to make a subjective assessment, as specifying an actual value – for example, for the number of tiers – may not be possible. Organisations should use their best judgement, integrating the information they have gathered with their own experience and assessment, to decide on the appropriate score. Vulnerabilities can also be assessed with SWOT (strengths and weaknesses, and opportunities and threats) and PESTLE (political, economic, social, technological, legal, and environmental) analyses.

Please note there are other tools and techniques that can make vulnerability assessment even easier. In the quest to uncover and mitigate supply chain vulnerabilities, a variety of tools and techniques can be employed to assess and quantify risks. These tools and techniques range from qualitative assessments to sophisticated quantitative models, each offering unique insights and capabilities.

Risk assessment matrices provide a structured framework for evaluating and prioritising risks based on their likelihood of occurrence and potential impact. These matrices can be customised to reflect the specific context and priorities of an organisation.

Failure Mode and Effects Analysis (FMEA) is a systematic approach for identifying potential failure modes, their causes, and their effects on the

supply chain. This technique can help organisations prioritise and mitigate risks based on their severity and likelihood.

Monte Carlo simulations are computational techniques that use random sampling and probability distributions to model the impact of various risk scenarios on supply chain performance. These simulations can provide valuable insights into the potential consequences of disruptions and inform risk mitigation strategies.

Supply chain risk management software can streamline processes for information gathering. Specialised software solutions are available to assist in supply chain risk management. These tools often incorporate features such as risk monitoring, scenario modelling, and real-time alerts, providing a centralised platform for risk assessment and mitigation.

Business continuity planning (BCP) and disaster recovery planning (DRP) are proactive approaches that involve developing comprehensive plans and strategies to ensure the continuity of critical operations and facilitate rapid recovery in the event of disruptions.

Supply chain mapping and visualisation tools can help organisations create visual representations of their supply chain networks, enabling them to identify potential vulnerabilities, dependencies, and bottlenecks more effectively.

Supplier risk assessment tools are designed specifically to evaluate and monitor supplier risks, taking into account factors such as financial stability, operational capabilities, compliance, and reputational risks.

Cybersecurity risk assessment tools can save valuable time. As cyber threats become increasingly prevalent, specialised tools are available to assess the cybersecurity risks within supply chain operations, including vulnerability scanning, penetration testing, and threat intelligence analysis.

By leveraging these tools and techniques, organisations can gain a comprehensive understanding of their supply chain vulnerabilities, enabling them to prioritise risk mitigation efforts and allocate resources effectively.

Strategies for mitigating supply chain vulnerabilities are an important next step. Once supply chain vulnerabilities have been identified and assessed, it is crucial to implement effective mitigation strategies to fortify resilience and ensure operational continuity. These strategies should be tailored to the specific risks and vulnerabilities faced by an organisation, while also considering the broader supply chain ecosystem.

Diversification and redundancy is a proven approach. Diversifying your supplier base, transportation routes, and distribution channels can help mitigate the impact of disruptions by providing alternative sources and redundant pathways. This strategy reduces overreliance on single points of failure and enhances supply chain flexibility.

Supply chain visibility and transparency are essential. Enhancing visibility and transparency throughout the supply chain can help identify potential vulnerabilities and enable proactive risk mitigation. This can be achieved

through improved data sharing, real-time tracking, and collaborative platforms with suppliers and partners.

Supplier risk management can considerably reduce the likelihood of incidents. Implementing robust supplier risk management programmes can help mitigate risks associated with your supplier network. This may involve supplier audits, performance monitoring, and contingency planning for supplier disruptions or failures.

Inventory optimisation can help provide a buffer. Striking the right balance between lean inventory practices and maintaining sufficient safety stock can help mitigate the impact of supply chain disruptions. Advanced inventory management techniques, such as demand forecasting and dynamic safety stock calculations, can optimise inventory levels while maintaining operational resilience.

Business continuity and disaster recovery planning can help consider alternative approaches. Developing comprehensive business continuity and disaster recovery plans can help organisations respond effectively to disruptions and minimise the impact on operations. These plans should include contingency strategies, communication protocols, and recovery procedures.

Collaboration and information sharing are necessary. Fostering collaboration and information sharing with industry peers, government agencies, and other stakeholders can provide valuable insights into emerging risks and best practices for risk mitigation. This collective intelligence can enhance overall supply chain resilience.

Cybersecurity and data protection must be considered. Implementing robust cybersecurity measures and data protection protocols can help mitigate the risks associated with cyber threats and data breaches. This may involve employee training, access controls, encryption, and regular security audits.

Continuous improvement and adaptability are essential for growth and mitigation. Embracing a culture of continuous improvement and adaptability is crucial in the face of ever-evolving supply chain risks. Regular risk assessments, process reviews, and the adoption of emerging technologies can help organisations stay ahead of potential vulnerabilities.

By implementing a combination of these strategies, organisations can build a resilient supply chain that is better equipped to withstand disruptions and maintain operational continuity in the face of unforeseen challenges.

Notes

1 Iftikhar, A., Ali, I., Arslan, A., and Tarba, S., 2024. Digital Innovation, Data Analytics, and Supply Chain Resiliency: A Bibliometric-based Systematic Literature Review. *Annals of Operations Research*, 333(2), pp.825–848.

2 Belhadi, A., Kamble, S., Subramanian, N., Singh, R.K., and Venkatesh, M., 2024. Digital Capabilities to Manage Agri-food Supply Chain Uncertainties and Build

Supply Chain Resilience during Compounding Geopolitical Disruptions. *International Journal of Operations & Production Management*, 44(5), pp.624–647.
3 Li, L., Wang, Z., Ye, F., Chen, L., and Zhan, Y., 2022. Digital Technology Deployment and Firm Resilience: Evidence from the COVID-19 Pandemic. *Industrial Marketing Management*, 105, pp.190–199.
4 Alvarenga, M.Z., Oliveira, M.P.V.D., and Oliveira, T.A.G.F.D., 2023. The Impact of using Digital Technologies on Supply Chain Resilience and Robustness: The Role of Memory under the Covid-19 Outbreak. Supply Chain Management: *An International Journal*, 28(5), pp.825–842.
5 Yuan, Y., Tan, H., and Liu, L., 2024. The Effects of Digital Transformation on Supply Chain Resilience: A Moderated and Mediated Model. *Journal of Enterprise Information Management*, 37(2), pp.488–510.
6 Dubey, R., Bryde, D.J., Dwivedi, Y.K., Graham, G., Foropon, C., and Papadopoulos, T., 2023. Dynamic Digital Capabilities and Supply Chain Resilience: The Role of Government Effectiveness. *International Journal of Production Economics*, 258, p.108790.
7 Groenewald, C.A., Garg, A., and Yerasuri, S.S., 2024. Smart Supply Chain Management Optimization and Risk Mitigation with Artificial Intelligence. *Naturalista Campano*, 28(1), pp.261–270.
8 Dubey, R., Bryde, D.J., Dwivedi, Y.K., Graham, G., Foropon, C., and Papadopoulos, T., 2023. Dynamic Digital Capabilities and Supply Chain Resilience: The Role of Government Effectiveness. *International Journal of Production Economics*, 258, p.108790.
9 Hägele, S., Grosse, E.H., and Ivanov, D., 2023. Supply Chain Resilience: A Tertiary Study. *International Journal of Integrated Supply Management*, 16(1), pp.52–81.
10 Alvarenga, M.Z., Oliveira, M.P.V.D., and Oliveira, T.A.G.F.D., 2023. The Impact of using Digital Technologies on Supply Chain Resilience and Robustness: The Role of Memory under the Covid-19 Outbreak. Supply Chain Management: *An International Journal*, 28(5), pp.825–842.
11 Iftikhar, A., Ali, I., Arslan, A., and Tarba, S., 2024. Digital Innovation, Data Analytics, and Supply Chain Resiliency: A Bibliometric-based Systematic Literature Review. *Annals of Operations Research*, 333(2), pp.825–848.
12 Mayur, J., 2024. Contingency Planning: The Need, Benefits, and Implementation of Scenario Planning. *International Journal of Trend in Scientific Research and Development*, 8(3), pp.866–869.

4

SUPPLY CHAIN RISK MANAGEMENT AND FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

Supply Chain Risk Management

Effective risk management of supply chain risk is crucial. Conducting risk management is a continuous process that requires a comprehensive and proactive approach to identifying, assessing, and mitigating supply chain vulnerabilities.

Rashid et al. (2024) found that information processing capability and digital supply chain significantly affect supply chain risk management and resilience. Supply chain risk management positively mediates the relationship between information processing capability and digital supply chains.[1] So there is a very clear link. Globalisation, specialisation, outsourcing, lean operations, rapid changes, geopolitical challenges, and complex supply chains make risk management crucial in SCM. Risks include quality defects, supply shortages, legal issues, natural disasters, exchange rate fluctuations, port congestions, regulatory compliance, and terrorism. Disruptions can occur anytime and anywhere in the supply chain.

Shishehgarkhaneh et al. (2024) argue that use of artificial intelligence in supply chain risk management is highly beneficial as the process of risk management inherently relies on identifying and minimising risk, managing impacts which are central to the procurement process. Organisations should look beyond first-tier suppliers to assess risks from second-tier suppliers.[2]

While organisations can influence suppliers through direct interaction and contract management, it's harder across the entire supply chain. Regular meetings with key organisations in the supply chain can help share messages and learnings.[3]

Organisations should encourage first-tier suppliers to enforce behaviours throughout their supply chains. This can be formalised by including contract

DOI: 10.4324/9781003604969-4

requirements for first-tier suppliers to assess their suppliers with the same standards the organisation uses. This practice was used in the 2012 London Olympics.

Odimarha et al. (2024) contend that emerging technologies can be used to provide greater transparency across the supply chain. Use of IoT sensors, AI, and blockchain can enable continuous monitoring, risk assessment, and secure information sharing reducing risk to all parties through the supply chain.[4]

By adopting a structured risk management framework, organisations can enhance their resilience and ensure the continuity of their operations in the face of potential disruptions.

Risk identification is the first step in the risk management process. Identify potential risks and vulnerabilities within the supply chain. This can be achieved through various techniques, such as supply chain mapping, supplier assessments, data analysis, and scenario planning exercises. Collaborating with stakeholders and subject matter experts can also provide valuable insights into potential risks.

Risk assessment is crucial once risks have been identified. Assess their likelihood of occurrence and potential impact on the organisation. This assessment can be conducted using tools and techniques such as risk assessment matrices, Failure Mode and Effects Analysis (FMEA), or Monte Carlo simulations. Prioritising risks based on their severity and probability can help organisations allocate resources effectively.[5]

Risk mitigation planning comes after assessing the risks. Organisations should develop comprehensive mitigation plans to address the identified vulnerabilities. These plans may include strategies such as diversification of suppliers, inventory optimisation, business continuity planning, cybersecurity measures, and contingency planning for various disruption scenarios.[6]

Implementation and monitoring is the next step. Implement the risk mitigation plans and continuously monitor the supply chain for emerging risks or changes in existing vulnerabilities. This may involve deploying specialised risk management software, conducting regular audits and assessments, and fostering collaboration and information sharing with stakeholders.[7]

Continuous improvement is essential. Risk management is an iterative process that requires continuous improvement and adaptation. Organisations should regularly review and update their risk management strategies based on lessons learned, changes in the business environment, and the adoption of new technologies or best practices. Encouraging a culture of continuous improvement can help organisations stay ahead of potential supply chain vulnerabilities. Emerging technologies like AI and machine learning can help improve monitoring, ensure continuous risk assessment, and embed continuous improvement.[8]

Stakeholder engagement and communication helps to identify and mitigate risks. Effective risk management requires collaboration and communication

with internal and external stakeholders, including suppliers, partners, regulatory bodies, and industry associations. Sharing information, best practices, and risk intelligence can enhance overall supply chain resilience and foster a collaborative approach to risk mitigation.

By embracing a comprehensive risk management approach and fostering a culture of proactive risk identification and mitigation, organisations can fortify their supply chain resilience and ensure operational continuity in the face of potential disruptions.

Supply chain risk management as a process starts with identifying all possible risks, followed by prioritisation, mitigation, management, and communication to stakeholders.

A critical step is assigning responsibility to risk owners in the team or Project Implementation Unit (PIU), who are accountable for monitoring, mitigating, and managing risks. Risk owners must understand their responsibilities and the management strategy.

After mitigating or managing risks, it's important to learn from these experiences to refine approaches. The process should be a continuous cycle, with activities reinforcing each other. This circular process can be conducted alongside procurement risk analysis.

Step 1: Risk Identification

Risks are unexpected and varied, so nobody can capture every risk but aim for as many possible choke points as you can. Typical risks for identification include those below:

TABLE 4.1 Risk Taxonomy

Risk Category	*Risk Type*	*Risk Description*
Supplier performance	Financial	Risk associated with the financial health of the supplier, which could result in bankruptcy, causing supply interruptions and other losses
	Quality	Risk associated with the quality of products or services provided by a supplier
	Delivery	Risk of the supplier failing to deliver the product/service on time
	Capacity	Risk of the supplier not having sufficient capacity to satisfy demand
	Integrity	Risks associated with corrupt, fraudulent, collusive, coercive, or obstructive practices by the supplier
	Reputation	Risk associated with negative effects on the brand or reputation of the organisation caused by supplier practices or actions

Risk Category	*Risk Type*	*Risk Description*
Environmental and social	Social	Risk associated with activities in the supply chain such as engagement of workers, safe working conditions, social impacts on local communities due to labour influx, engagement with stakeholders, and impacts associated with use of land
	Environmental	Risk associated with activities in the supply chain such as hazardous waste, pollution, carbon emission, actions that cause conversion or degradation of natural or critical habitats
	Health and safety	Risk associated with suppliers not following relevant occupational health and safety requirements, including the handling of hazardous conditions and substances, ineffective safety training, incomplete records of incidents and accidents, lack of preparedness to respond to incidents, and lack of remedies for adverse impacts
Supply market	Category	Risk associated with a specific supply category, caused, for instance, by highly complex and fragmented supply chains
	Raw material	Risk associated with specific raw materials, which can include global shortages and competition from other industries
	Logistics	Risk associated with the transportation and storage of products across the supply chain
Technology	Cybersecurity	Risk associated with the theft of or damage to the organisation's or supplier's hardware, software, or information, including possible disruption to their operations
	Intellectual property	Risk involving a potential loss of intellectual property
Geopolitical	Domestic	Risk associated with changes in policy in the domestic market of organisation that can affect its ability or costs of sourcing, such as changes in tariffs, trade restrictions, and trade sanctions
	Labour	Risk associated with labour disputes that could disrupt the production and delivery of products and services
	Legal	Risk that exposes the organisation to potential legal actions or disputes in international trade

Risk Category	*Risk Type*	*Risk Description*
Macroeconomic	Currency	Risk associated with currency volatility that might negatively affect an organisation's profitability (sometimes also termed foreign exchange risk)
	Inflation/ volatility	Risk associated with inflationary pressure or swift changes in the price of raw materials and labour in source countries
Natural disasters		Risk associated with disruptions affecting the operation of suppliers or the flow of products, due to major natural catastrophes such as earthquakes, tsunamis, tornados, hurricanes, fires, and floods

Organisations should note that this is just one framework that can be adapted to suit a project's needs. The ability to address these risks depends largely on the organisation's influence over its suppliers. It's important to understand the supply market, consider how attractive the procurement is to suppliers, and assess their ability to manage identified risks.

In challenging environments, such as those affected by fragility, conflict, and violence, organisations may consider engaging specialist support or requesting hands-on expanded implementation support.

Step 2: Risk Prioritisation

Once risks are identified, they can be prioritised by their likelihood and potential severity. Likelihood assesses how probable a risk is, while severity assesses its impact. This assessment is subjective, but organisations can use prior experience and information from the procurement process.

Prioritisation can be done using a five-category scale:

1. = Very Low (VL).
2. = Low (L).
3. = Medium (M).
4. = High (H).
5. = Very High (VH).

Based on these classifications, organisations can plot each risk on a risk criticality matrix. This matrix, sometimes called a heat map, shows high overall risk in red, and lower risks in amber and green.

Step 3: Risk Mitigation and Management

Organisations can use the heat map to determine how to address these risks, using the colours to categorise risks on a scale from high to low risk. Typical actions for each category include:

- *High risk:* Address through ongoing assessments and contingency plans (e.g., alternative sources, higher inventory, inspections, and audits).
- *Substantial risk:* Address with periodic assessments, monitoring, and contingency plans.
- *Moderate risk:* Manage via routine procedures and internal reporting. Organisations may accept these low-priority risks.
- *Low risk:* Accept as part of doing business or monitor as needed.

The supply chain risk management process can lead to four main strategies:

- *Avoid:* Do not pursue the current supply chain design if risks are too severe. For example, if forced labour risk is high, find an alternative design with suppliers that have strict workforce protection policies.
- *Minimise:* Implement the design but mitigate risks through improved monitoring or process modifications. For example, require regular reporting and inspections.
- *Spread or transfer:* Implement the design but reduce risk via diversification, subcontracting, outsourcing, joint ventures, hedging, or insurance. For example, purchase scarce components and provide them to the supplier, giving more control but also greater liability.
- *Accept:* Implement the design and accept associated risks. For example, accept small quality defects if they can be corrected easily and inexpensively without harm to stakeholders.

Step 4: Risk Communication and Learning

Learning from past successes and failures is crucial. A template for recording this information is available,[9] which can be shared to refine risk management approaches and increase expertise.

Capturing the information in a risk management plan: Organisations can compile insights into a risk management plan. This plan offers a transparent way to review, compare, and prioritise risks, and develop action plans if needed. There is no right or wrong way to do this. Think about risks, classify them, and find mitigation strategies.

Case Studies

Real-life case studies of supply chain vulnerabilities help us bring to life the real and present risks that exist in our businesses. Supply chain vulnerabilities are not mere theoretical constructs; they manifest in real-world scenarios, impacting businesses across industries and geographies. Examining real-life case studies can provide valuable insights into the potential consequences of supply chain disruptions and the importance of proactive risk mitigation strategies.

The 2011 Thailand floods had huge impact. In 2011, severe flooding in Thailand disrupted the operations of numerous manufacturing facilities, including those of major automotive and electronics companies. The disruption rippled through global supply chains, causing production delays and shortages of critical components. This event highlighted the vulnerability of supply chains to natural disasters and the need for geographic diversification and contingency planning.

The Fukushima nuclear disaster was catastrophic. The 2011 earthquake and tsunami in Japan, which led to the Fukushima nuclear disaster, had far-reaching consequences for global supply chains. The disaster disrupted production of critical components used in various industries, including automotive and electronics. This event underscored the importance of supply chain resilience and the need for robust risk management strategies.

The Suez Canal blockage caused severe disruption. In March 2021, a massive container ship became wedged in the Suez Canal, blocking one of the world's most critical maritime trade routes for nearly a week. This disruption caused significant delays and backlogs in global supply chains, highlighting the vulnerability of transportation networks and the need for contingency plans and alternative routes.

The COVID-19 pandemic led to shortages the world over. The global COVID-19 pandemic has exposed vulnerabilities in supply chains across industries, from healthcare to consumer goods. Disruptions in manufacturing, transportation, and labour availability have led to shortages, delays, and increased costs. This event has underscored the need for agility, diversification, and the ability to adapt to rapidly changing circumstances.

The NotPetya cyber attack hit well -corporations hard. In 2017, the NotPetya cyber attack targeted Ukrainian organisations but quickly spread globally, impacting major corporations like Maersk, Merck, and FedEx. This attack disrupted operations, caused significant financial losses, and highlighted the vulnerability of supply chains to cyber threats and the need for robust cybersecurity measures.

These real-life examples serve as sobering reminders of the far-reaching consequences of supply chain vulnerabilities and the importance of proactive risk management strategies. By learning from these events, organisations can better prepare for and mitigate potential disruptions, enhancing their overall supply chain resilience.

Safeguarding your supply chain from hidden vulnerabilities is not just a matter of business continuity; it's a strategic imperative that can spell the difference between success and failure in today's interconnected global marketplace.

Failure Mode and Effects Analysis (FMEA)

In the ever-evolving landscape of supply chain management, proactive measures are paramount to mitigating risks and ensuring seamless operations.

One such powerful tool is *Failure Mode and Effects Analysis (FMEA)*, a systematic approach that identifies potential failures, evaluates their effects, and implements preventive actions. By employing FMEA, we can unlock a realm of opportunities to enhance supply chain efficiency, reduce costs, and maintain a competitive edge.

Marco-Ferreira et al. (2023) argue FMEA can be highly effective and in some cases more effective than alternatives to reduce risk in the supply chain and provide preventive actions. Alternatives considered include the analytic hierarchy process (AHP), analytic network process (ANP), fuzzy logic DEMATEL, and disruption analysis network (DA_NET) methods.[10]

FMEA is a structured methodology that originated in the aerospace industry but has since been adopted across various sectors, including manufacturing, healthcare, and logistics. Its core objective is to anticipate and address potential failures before they occur, thereby minimising disruptions and maximising operational excellence.

Carvalho et al. (2022) insist FMEA as an approach is effective in assessing resilience including that of critical infrastructure, providing a cost-effective way to evaluate plausible alternatives concerning the improvement of preventive measures.[11]

We must delve into the intricacies of FMEA and its invaluable role in supply chain management. From understanding its components to implementing best practices, we will explore how this powerful tool can fortify your supply chain operations and propel your business toward unprecedented success.

Ghadir et al. (2022) assert that traditional FMEA can be highly effective for supply chain risk, especially when combined with Best–Worst Method (BWM), applying appropriate risk weights. This approach can help assess the potential impact of major disruptions.[12]

The value of FMEA should not be underestimated. The modern supply chain is a complex web of interconnected processes, involving numerous stakeholders, intricate logistics, and stringent quality standards. Any disruption or failure within this intricate system can have far-reaching consequences, impacting customer satisfaction, profitability, and brand reputation.

FMEA plays a crucial role in supply chain management by identifying potential risks. By systematically analysing each process step, FMEA helps identify potential risks, bottlenecks, and vulnerabilities that could lead to failures or disruptions. Prioritising critical areas is essential. FMEA assigns risk priority numbers (RPNs) to potential failures, allowing organisations to prioritise their efforts and allocate resources effectively. Implementing preventive measures helps provide assurance. Through the development of robust control plans, FMEA enables the implementation of preventive and corrective actions, mitigating the likelihood and impact of failures.

Enhancing quality and compliance are proven methods to deal with regulation. FMEA promotes adherence to industry standards, regulatory

requirements, and quality management systems, ensuring consistent product quality and customer satisfaction. Fostering continuous improvement allows for learning. By regularly reviewing and updating FMEA analyses, organisations can continuously improve their processes, adapt to changing market conditions, and stay ahead of emerging risks.

Understanding the components of FMEA is crucial. FMEA comprises several key components that work in tandem to provide a comprehensive risk assessment and mitigation framework.

Failure modes are potential ways in which a process, product, or service could fail to meet specified requirements or customer expectations. Failure effects are the consequences or impacts of a particular failure mode on the overall system, process, or end user. Severity rating is a numerical score assigned to each failure effect, reflecting the magnitude of its potential impact. Occurrence rating is a numerical score assigned to each failure mode, indicating the likelihood of its occurrence. Detection rating is a numerical score assigned to each failure mode, representing the ability to detect the failure before it reaches the end user or customer. Risk priority number (RPN) is a calculated value derived from the product of the severity, occurrence, and detection ratings, used to prioritise and address high-risk areas. Recommended actions are preventive and corrective measures proposed to address identified failure modes and mitigate their effects.

By systematically evaluating these components, FMEA provides a structured framework for risk assessment and mitigation, enabling organisations to make informed decisions and implement proactive strategies.

Conducting an effective FMEA requires a structured approach and collaboration among cross-functional teams. Assemble a cross-functional team. Gather a diverse team of subject matter experts, including representatives from various departments (e.g., engineering, operations, quality, and supply chain). Clearly define the scope and objectives of the FMEA, whether it is focused on a specific process, product, or service. Establish the objectives and desired outcomes. Map the process flow. Create a detailed process map or diagram, outlining each step and identifying potential failure modes. For each process step, brainstorm and identify all potential failure modes that could occur. Determine failure effects by analysing the consequences or impacts of each identified failure mode on the overall system, process, or end user. Using established rating scales, assign numerical scores for severity, occurrence, and detection for each failure mode. Calculate RPNs by multiplying the severity, occurrence, and detection ratings to obtain the RPN for each failure mode. Prioritise and address high-risk areas: develop recommended actions to mitigate or eliminate these risks. Execute the recommended actions, such as process improvements, design modifications, or additional controls, to address the identified risks. Continuously monitor with regular review and update the FMEA analysis to reflect changes in processes, products, or services, and to identify new potential risks.

By following this structured approach, you can ensure a comprehensive and effective FMEA implementation, enabling proactive risk management and continuous improvement within your supply chain operations.

Benefits of implementing FMEA should be considered. Integrating FMEA into your supply chain management strategy yields numerous benefits that can significantly enhance operational efficiency, customer satisfaction, and overall business performance. By identifying and addressing potential failures, FMEA helps ensure consistent product quality, service reliability, and adherence to industry standards and regulations. Proactive risk mitigation through FMEA can reduce costs and waste as it prevents costly product recalls, rework, and downtime, ultimately reducing operational costs and minimising waste. By delivering high-quality products and services consistently, FMEA contributes to improved customer satisfaction, loyalty, and brand reputation. FMEA facilitates streamlined processes, optimised resource allocation, and effective risk management, leading to improved operational efficiency throughout the supply chain. By implementing FMEA, organisations can gain a competitive edge by delivering superior quality, reliability, and customer experience, setting themselves apart from competitors. FMEA supports compliance with industry-specific regulations, quality management systems, and safety standards, ensuring adherence to legal and regulatory requirements. The systematic approach of FMEA fosters a culture of continuous improvement, encouraging organisations to regularly review and enhance their processes, products, and services.

By leveraging the power of FMEA, organisations can proactively mitigate risks, optimise operations, and drive sustainable growth within their supply chain ecosystem.

Case Studies

Case studies are useful in providing real-life examples of FMEA in action. To illustrate the practical application and benefits of FMEA in supply chain management, let's explore two real-life case studies:

Case Study 1: Automotive Manufacturing (Ford Motor Company)[13]

Ford, a leading automotive manufacturer, implemented FMEA to enhance the quality and reliability of their supply chain operations. By conducting a comprehensive FMEA analysis, they identified potential failure modes in their production processes, such as defective components, assembly errors, and quality control issues.

Through the FMEA process, the manufacturer assigned RPNs to each identified failure mode, prioritising high-risk areas. They then developed and implemented recommended actions, including:

- Implementing stricter incoming material inspections.
- Redesigning assembly processes to minimise human error.
- Enhancing quality control procedures.
- Providing specialised training to production personnel.

As a result of their FMEA implementation, Ford experienced a significant reduction in product defects, warranty claims, and customer complaints. Additionally, they achieved cost savings through improved operational efficiency and reduced rework and waste.

Case Study 2: Biopharmaceutical Supply Chain (Talecris Biotherapeutics)[14]

Talecris Biotherapeutics, a leading biopharmaceutical company, recognised the importance of FMEA in ensuring the integrity and safety of their supply chain operations. They conducted an FMEA analysis focused on their cold chain logistics processes, which are critical for maintaining the efficacy and quality of temperature-sensitive biopharmaceutical products.

Through the FMEA process, they identified potential failure modes such as temperature excursions during transportation, equipment malfunctions, and human errors in handling and storage. The company assigned RPNs to these failure modes and developed recommended actions, including:

- Implementing real-time temperature monitoring systems.
- Upgrading refrigerated transportation vehicles.
- Enhancing staff training on proper handling and storage procedures.
- Developing contingency plans for equipment failures.

By implementing these FMEA-driven recommendations, the biopharmaceutical company significantly reduced the risk of product spoilage, maintained product quality and efficacy, and ensured compliance with stringent regulatory requirements. Additionally, they experienced improved customer satisfaction and minimised the financial impact of product losses.

These case studies demonstrate the powerful impact of FMEA in enhancing supply chain management across diverse industries, showcasing its versatility and effectiveness in mitigating risks, improving quality, and driving operational excellence.

Wong et al. (2023) argue FMEA is crucial in the pharmaceutical industry in reducing risk in supply chains.[15] The European Medicines Agency provided guidance on the effective implementation of FMEA for the pharmaceutical industry.[16]

Challenges and Best Practices with FMEA

While FMEA is a valuable tool for supply chain management, it is essential to acknowledge and address its potential challenges and limitations. By understanding these factors, organisations can effectively mitigate risks and maximise the benefits of FMEA implementation.

Conducting a comprehensive FMEA analysis can be time-consuming and resource-intensive, particularly for complex processes or products with numerous components and failure modes. The assignment of severity, occurrence, and detection ratings can be influenced by subjective judgements and biases, potentially leading to inaccurate risk assessments. Accurate and reliable data is crucial for effective FMEA analysis. Lack of historical data or incomplete information can hinder the identification and assessment of potential failure modes. Effective FMEA implementation relies on the collaboration and expertise of cross-functional teams. Challenges may arise due to communication barriers, lack of subject matter expertise, or conflicting priorities among team members. As processes, products, or technologies evolve, FMEA analyses may become outdated, requiring regular updates and revisions to maintain their relevance and effectiveness. Successful FMEA implementation often requires a cultural shift within the organisation, embracing a proactive risk management approach. Resistance to change or lack of buy-in from stakeholders can hinder the adoption and effectiveness of FMEA.

To address these challenges, organisations should allocate adequate resources and time for thorough FMEA analyses. They must implement robust training programmes to mitigate subjectivity and biases. They should establish robust data collection and management systems. It helps to foster cross-functional collaboration and leverage subject matter expertise. Regularly review and update FMEA analyses to reflect changes in processes, products, or technologies. It is important to cultivate a culture of continuous improvement and risk management.

By proactively addressing these challenges, organisations can maximise the benefits of FMEA and ensure its effective integration into their supply chain management strategies.

Best practices for successful implementation help with embedding. To ensure the successful implementation and sustained effectiveness of FMEA in supply chain management, organisations should adopt best practices.

Secure buy-in and commitment from top management to foster a culture of risk management and continuous improvement throughout the organisation. Encourage cross-functional collaboration and ensure representation from various departments and stakeholders in the FMEA team to leverage diverse perspectives and expertise. Provide comprehensive training to FMEA team members on the methodology, tools, and techniques to ensure consistent and effective implementation. Develop and implement standardised processes, rating scales, and tools for conducting FMEA analyses across the

organisation to ensure consistency and comparability. Adopt a data-driven approach by collecting and analysing relevant data from various sources, such as historical records, customer feedback, and industry benchmarks, to inform the FMEA process. Prioritise FMEA efforts based on risk levels, focusing on high-risk areas or processes that have the greatest potential impact on supply chain operations and customer satisfaction. Regularly monitor and review FMEA analyses to ensure their relevance and effectiveness, incorporating changes in processes, products, technologies, or regulatory requirements. Integrate FMEA with other quality management initiatives, such as Six Sigma, Lean Manufacturing, or Total Quality Management, to leverage synergies and drive comprehensive process improvement. Encourage knowledge sharing and the dissemination of lessons learned from FMEA implementations across the organisation to foster continuous learning and improvement. Collaborate with suppliers, vendors, and partners throughout the supply chain to align FMEA efforts, share best practices, and ensure consistent quality and risk management across the entire ecosystem.

By adhering to these best practices, organisations can maximise the benefits of FMEA, foster a culture of proactive risk management, and drive sustainable improvements in supply chain operations.

Tools and software are crucial for FMEA in supply chain management. To streamline and enhance the implementation of FMEA in supply chain management, organisations can leverage various tools and software solutions. These tools facilitate efficient data collection, analysis, and collaboration, enabling more effective risk assessment and mitigation strategies.

Dedicated FMEA software applications provide a centralised platform for conducting FMEA analyses, capturing data, calculating RPNs, and generating reports. These tools often include customisable templates, risk prioritisation features, and collaboration capabilities. Quality management systems (QMS), such as those offered by leading providers like Sparta Systems, Greenlight Guru, and MasterControl, integrate FMEA functionality, enabling seamless integration of risk management processes with other quality initiatives. While not as robust as dedicated FMEA software, spreadsheet applications like Microsoft Excel or Google Sheets can be used to create customised FMEA templates, perform calculations, and generate basic reports.

Project management platforms like Trello, Asana, or Microsoft Teams can facilitate collaboration, task assignment, and communication among FMEA team members, ensuring efficient coordination and information sharing.

Data analytics and visualisation tools: Tools like Tableau, Power BI, or Python libraries (e.g., Matplotlib, Seaborn) can be leveraged to analyse FMEA data, generate insightful visualisations, and identify patterns or trends that inform risk mitigation strategies.

Specialised risk management software solutions, such as those offered by providers like Riskturn, Palisade, or Protecht, can integrate FMEA functionality into broader enterprise risk management frameworks.

When selecting tools and software for FMEA implementation, organisations should consider factors such as user-friendliness, integration capabilities, scalability, and support for industry-specific requirements. Additionally, providing adequate training and ensuring user adoption are crucial for maximising the benefits of these tools.

Grabill et al. (2024) contend FMEA software and tooling can be improved further through AI augmentation. They suggest FMEA can be used in reliability engineering and software development by presenting a novel AI-augmented tool for d-FMEA and d-FMECA processes, offering a significant leap forward in terms of efficiency and user engagement. By integrating principles of risk assessment and reliability engineering into the software development process, we can use a more powerful graphical user interface and clearer, more insightful assessments.[17]

Maximising supply chain efficiency is made possible with FMEA. In the dynamic and complex landscape of supply chain management, proactive risk mitigation and continuous improvement are essential for achieving operational excellence and maintaining a competitive edge. FMEA is a powerful tool that empowers organisations to identify potential failures, evaluate their effects, and implement preventive actions, ultimately enhancing supply chain efficiency and customer satisfaction.

By leveraging the systematic approach of FMEA, organisations can identify and mitigate potential risks and vulnerabilities within their supply chain processes. Prioritise critical areas for improvement and allocate resources effectively. Implement robust control plans and preventive measures. Enhance product quality, reliability, and compliance. Try to foster a culture of continuous improvement and risk management.

To unlock the full potential of FMEA in supply chain management, it is crucial to adopt best practices, leverage appropriate tools and software, and foster cross-functional collaboration and commitment at all levels of the organisation.

Notes

1 Rashid, A., Rasheed, R., Ngah, A.H., Pradeepa Jayaratne, M.D.R., Rahi, S., and Tunio, M.N., 2024. Role of Information Processing and Digital Supply Chain in Supply Chain Resilience through Supply Chain Risk Management. *Journal of Global Operations and Strategic Sourcing*, 17(2), pp.429–447.
2 Shishehgarkhaneh, M.B., Moehler, R.C., Fang, Y., Aboutorab, H., and Hijazi, A. A., 2024. Construction Supply Chain Risk Management. *Automation in Construction*, 162, p.105396.
3 De Oliveira, U.R., Dias, G.C., and Fernandes, V.A., 2024. Evaluation of a Conceptual Model of Supply Chain Risk Management to Import/export Process of an Automotive Industry: An Action Research Approach. *Operations Management Research*, 17(1), pp.201–219.
4 Odimarha, A.C., Ayodeji, S.A., and Abaku, E.A., 2024. The Role of Technology in Supply Chain Risk Management: Innovations and Challenges in Logistics. *Magna Scientia Advanced Research and Reviews*, 10(2), pp.138–145.

5 Hajarath, K., and Vummadi, J., 2024. Enhancing Supply Chain Resilience: Proactive Strategies for Disruptive Events. *International Journal of Supply Chain Management*, 9(3), pp.1–11.
6 Sahab, S., and Oulfarsi, S., 2024, May. Supply Chain Risk Management and Supply Chain Resilience under Disruption Risks: Theoretical Exploration. In *2024 IEEE 15th International Colloquium on Logistics and Supply Chain Management (LOGISTIQUA)* (pp. 1–7). IEEE.
7 Ahamed, N., 2024. Supply Chain Resilience: Strategies for Mitigating Risk (Doctoral dissertation, University of Technology).
8 Sodiya, E.O., Jacks, B.S., Ugwuanyi, E.D., Adeyinka, M.A., Umoga, U.J., Daraojimba, A.I., and Lottu, O.A., 2024. Reviewing the Role of AI and Machine Learning in Supply Chain Analytics. GSC Advanced Research and Reviews, 18 (2), pp.312–320.
9 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf.
10 Marco-Ferreira, A., Fidelis, R., Horst, D.J., and Andrade Junior, P.P., 2023. Mitigating the Impacts of COVID-19: Failure Mode and Effect Analysis and Supply Chain Resilience (FMEA-SCR) Combined Model. *Modern Supply Chain Research and Applications*, 5(3), pp.158–175.
11 Carvalho, G., Medeiros, N., Madeira, H., and Cabral, B., 2022, December. A Functional FMECA Approach for the Assessment of Critical Infrastructure Resilience. In *2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS)* (pp. 672–681). IEEE.
12 Ghadir, A.H., Vandchali, H.R., Fallah, M., and Tirkolaee, E.B., 2022. Evaluating the Impacts of COVID-19 Outbreak on Supply Chain Risks by Modified Failure Mode and Effects Analysis: A Case Study in an Automotive Company. *Annals of Operations Research*, pp.1–31.
13 https://support.ptc.com/help/wrr/r12.0.2.0/en/index.html#page/wrr/ReferenceGuide/fmea/insert_fmea_key_record.html.
14 https://www.pharmamanufacturing.com/facilities/op-ex-lean-six-sigma/article/11364120/operational-excellence-fmea-a-risk-based-approach-to-sterility-assurance-pharmaceutical-manufacturing.
15 Wong, W.P., Saw, P.S., Jomthanachai, S., et al., 2023. Digitalisation Enhancement in the Pharmaceutical Supply Network using a Supply Chain Risk Management Approach. *Sci Rep 13*, 22287. https://doi.org/10.1038/s41598-023-49606-z.
16 https://www.ema.europa.eu/en/documents/scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use-ich-guideline-q9-quality-risk-management-step-5-first-version_en.pdf.
17 Grabill, N., Wang, S., Olayinka, H.A., De Alwis, T.P., Khalil, Y.F., and Zou, J., 2024. AI-augmented Failure Modes, Effects, and Criticality Analysis (AI-FMECA) for Industrial Applications. *Reliability Engineering & System Safety*, p.110308.

5

CYBER RESILIENCE AND IMPROVING CYBERSECURITY IN THE SUPPLY CHAIN

Cyber Resilience

Van't Schip (2024) argues that in the ever-evolving landscape of global commerce, the intricate web of supply chains has become the backbone of modern businesses. These intricate networks facilitate the seamless flow of goods, services, and information across borders, enabling companies to operate efficiently and meet the demands of their customers. For all these reasons, supply chain cybersecurity is increasingly in the cross-hairs of regulators.[1]

Salvi et al. (2022) insist cyber resilience is the most important contributor to digital resilience in the digital age.[2] As supply chains grow more complex and interconnected, the potential for cyber threats and vulnerabilities escalates, underscoring the critical importance of *cyber resilience* and having in place robust cybersecurity measures.

Aldasoro et al. (2022) argue that technology is a major threat to supply chains yet regularly misunderstood. Advances in IT drive efficiencies and respond to fast-changing markets, while also enabling massive data collection across supply chain processes. The shift towards digitalisation, automation, and technological integration is complex and not always smooth.[3]

There is a need for a strategic approach to leveraging technology for modern supply chains. Research indicates that supply chains are in the early stages of a digital transformation, likely the biggest change in supply chain management in years. Although the future is unclear, supply chain leaders must adapt to this new paradigm or risk being left behind.

Boh et al. (2023) contend cyber resilience is crucial in developing the foundation of security on which to build towards digital resilience but also caution against thinking of technology as a panacea to develop resilience.[4]

DOI: 10.4324/9781003604969-5

We live in an era where cyber attacks have become increasingly sophisticated and widespread, posing significant risks to the integrity and resilience of supply chains. Cybercriminals exploit weaknesses in digital systems, compromising sensitive data, disrupting operations, and causing financial losses that can ripple through entire industries. Consequently, organisations must prioritise cybersecurity as a strategic imperative, ensuring the protection of their supply chains from malicious actors and safeguarding their competitive advantage.

Garcia-Perez et al. (2023) assert that cyber resilience is crucial, especially at times of digital transformation, and that developing cyber resilience is sorely needed in the healthcare sector. This would have avoided many of the recent cyber breaches that impacted the NHS in the UK and health insurance companies in the USA.[5]

We must better understand the realm of supply chain cybersecurity, its significance, common threats, and the strategies employed to mitigate risks. We aim to empower businesses with the knowledge and tools necessary to fortify their supply chains against cyber attacks, fostering a secure and resilient environment for global trade.

Al-Hawamleh (2024) argues cyber resilience is vital to help fortify organisational defences against the evolving landscape of cyber threats while enhancing business continuity. The aim is to provide businesses with a robust and adaptive strategy that extends beyond traditional cybersecurity paradigms. By integrating governance and leadership principles, collaboration with external stakeholders, and continuous monitoring, this can foster a holistic approach to cyber resilience. Leveraging a behavioural perspective, we can consider human factors, user awareness, and decision-making processes, recognising the critical role of organisational culture in fostering a cybersecurity-aware ethos.[6]

Adenekan et al. (2024) insist the importance of cybersecurity in supply chain management cannot be overstated. Supply chains are intricate ecosystems that involve numerous stakeholders, including suppliers, manufacturers, logistics providers, and retailers. Each of these entities relies on interconnected digital systems and data exchange, creating potential entry points for cyber threats.[7]

Supply Chain Cybersecurity

Cybersecurity breaches within the supply chain can have far-reaching consequences. Data breaches can be hugely damaging. Sensitive information, such as intellectual property, trade secrets, and customer data, can be compromised, leading to financial losses, reputational damage, and legal liabilities. Operational disruptions can grind businesses to a halt. Cyber attacks can disrupt critical systems, causing delays, production stoppages, and logistical bottlenecks, ultimately impacting the entire supply chain. Financial

losses can be severe. The direct and indirect costs associated with cyber incidents, including remediation efforts, legal fees, and lost revenue, can be substantial and potentially catastrophic for businesses. Failure to implement adequate cybersecurity measures may result in non-compliance with industry regulations and standards, leading to penalties and legal consequences. High-profile cyber attacks can erode consumer trust and confidence, potentially causing long-term harm to a company's brand, reputation, and market position.

By prioritising cybersecurity within the supply chain, organisations can mitigate these risks, protect their assets, and maintain the integrity of their operations. Robust cybersecurity measures not only safeguard against financial and operational losses but also foster trust and confidence among stakeholders, enabling businesses to thrive in an increasingly digital and interconnected world.

Supply chains are vulnerable to a wide range of cyber threats, each with the potential to disrupt operations and compromise sensitive data. Understanding these threats is crucial for developing effective mitigation strategies.

Phishing attacks can cause significant damage beyond the initial compromise. Malicious actors employ social engineering techniques, such as fraudulent emails or websites, to trick individuals into revealing sensitive information or granting unauthorised access to systems. Malware and ransomware can cause long-lasting impact. Malicious software can infiltrate supply chain systems, causing data breaches, system failures, and even holding critical information or operations hostage for ransom payments. Distributed Denial of Service (DDoS) attacks cause temporary but deeply impactful damage. Cyber attackers overwhelm networks and systems with excessive traffic, rendering them unavailable or disrupting operations.

Advanced Persistent Threats (APTs) are very difficult to protect any organisation against. Sophisticated and targeted attacks, often sponsored by nation-states or organised cybercriminal groups, aim to gain long-term access to systems for data exfiltration or disruption. Internet of Things (IoT) vulnerabilities are so pervasive that they are difficult to identify and protect. The proliferation of connected devices in supply chain operations, such as sensors and tracking systems, introduces new entry points for cyber threats if not properly secured.

Third-party risks are hard to control. Supply chains involve multiple stakeholders, and a breach or vulnerability in one partner's systems can potentially compromise the entire network. Insider threats are difficult to identify. Disgruntled or negligent employees, contractors, or business partners with access to sensitive information or systems can intentionally or unintentionally cause data breaches or operational disruptions.

To effectively combat these threats, organisations must adopt a comprehensive approach to *cyber resilience* including a cybersecurity strategy that encompasses people, processes, and technology. Regular risk assessments,

employee training, robust access controls, and continuous monitoring are essential components of a strong cybersecurity posture within the supply chain.

Crosignani, et al. (2023) argue the consequences of supply chain cybersecurity breaches can be far-reaching and devastating for organisations. Beyond the immediate financial losses and operational disruptions, these incidents can have long-lasting impacts on a company's reputation, customer trust, and overall business performance.

One of the most significant impacts of a supply chain breach is the potential for data loss or theft. Sensitive information, such as intellectual property, trade secrets, and customer data, can fall into the wrong hands, leading to competitive disadvantages, legal liabilities, and reputational damage. Additionally, the loss of critical operational data can immobilise supply chain processes, causing delays, production stoppages, and logistical challenges.

Supply chain breaches can also result in substantial financial losses. Direct costs may include remediation efforts, legal fees, regulatory fines, and the implementation of enhanced security measures. Indirect costs, such as lost revenue due to operational disruptions, customer attrition, and reputational damage, can be even more significant and long-lasting.

Furthermore, supply chain breaches can erode consumer trust and confidence in a company's ability to protect sensitive information and maintain secure operations. In today's digital age, where customers prioritise data privacy and security, a high-profile cyber incident can severely tarnish a brand's reputation, leading to a loss of market share and diminished customer loyalty.

Case Studies

The Target data breach (2013) was huge in scale. In one of the largest data breaches in retail history, hackers gained access to Target's systems through a third-party vendor's credentials. Plachkinova & Maurer (2018) argue this breach compromised the personal and financial information of over 70 million customers, resulting in significant financial losses, legal fees, and a tarnished reputation for the retail giant.[8]

The NotPetya cyber attack (2017) had huge financial implications. The NotPetya ransomware attack, initially targeting Ukrainian businesses, quickly spread through global supply chains, affecting major corporations like Maersk, Merck, and FedEx. The attack caused widespread operational disruptions, resulting in billions of dollars in losses and highlighting the vulnerability of interconnected supply chain systems.[9]

These case studies underscore the severe consequences of supply chain cybersecurity breaches and the importance of implementing robust security measures to protect against such incidents.

Risk Mitigation

Hoang (2023) argues clawback provisions in employment contracts are a simple way to ensure executives take cyber risk seriously. CISOs that aren't getting the levels of investment in cybersecurity they need should consider their position. Raising security awareness amongst Executive Boards is an essential precursor to any cybersecurity strategy. Shareholders and Board must understand the importance of cybersecurity to their organisations and consider clawback and other mechanisms to prevent a situation where CEOs prioritise short-term gain at the expense of cybersecurity.[10]

Technology plays a pivotal role in securing the supply chain against cyber threats. By leveraging advanced solutions and innovative approaches, organisations can fortify their defences and enhance their ability to detect, respond to, and recover from cyber incidents.

A comprehensive cybersecurity strategy should incorporate cybersecurity tools and solutions, such as firewalls, intrusion detection and prevention systems (IDS/IPS), antivirus and anti-malware software, and data encryption technologies. These solutions help protect systems and data from unauthorised access, malware infections, and data breaches.

Blockchain and distributed ledger technologies offer enhanced transparency, traceability, and immutability within supply chains. By creating a tamper-proof record of transactions and data, these technologies can help mitigate risks associated with data manipulation, counterfeiting, and fraud.

Leveraging cloud computing and virtualisation technologies can enhance supply chain security by centralising data storage and management, enabling real-time monitoring, and facilitating rapid incident response and recovery efforts.

Internet of Things (IoT) security is essential. As the adoption of IoT devices in supply chain operations continues to grow, implementing robust security measures for these connected devices is crucial. This includes secure device configuration, regular software updates, and robust access controls.

Artificial intelligence (AI) and machine learning (ML) are important emerging technologies. AI and ML algorithms can analyse vast amounts of data to identify potential threats, detect anomalies, and provide predictive insights, enabling proactive risk mitigation and enhanced situational awareness within supply chain operations.

Implementing robust identity and access management (IAM) solutions, such as multi-factor authentication, role-based access controls, and privileged access management, can help prevent unauthorised access to critical systems and data within the supply chain.

Deploying real-time monitoring and incident response capabilities is essential for rapidly detecting and responding to cyber threats, minimising the impact of potential breaches, and facilitating swift recovery efforts.

By embracing these technological solutions and integrating them into a comprehensive cybersecurity strategy, organisations can significantly enhance

the security and resilience of their supply chains, protecting against cyber threats and ensuring business continuity.

Effective supply chain cybersecurity requires collaboration and information sharing among stakeholders. Supply chains are interconnected ecosystems, and a breach or vulnerability in one entity can potentially impact the entire network. Consequently, fostering open communication, establishing trusted partnerships, and promoting industry-wide cooperation are crucial for mitigating cyber risks.

Public–private partnerships can resolve deep-rooted problems. Collaboration between government agencies, law enforcement, and private sector organisations can facilitate the exchange of threat intelligence, best practices, and incident response strategies, enhancing overall supply chain security.

Industry associations and information sharing and analysis centres (ISACs) enable collaboration. Participating in industry-specific associations and ISACs enables organisations to share threat information, vulnerabilities, and mitigation strategies, promoting a collective defence against cyber threats.

Implementing robust supply chain risk management (SCRM) programmes that assess and manage risks across the entire supply chain, including third-party vendors and partners, can help identify and address potential vulnerabilities proactively.

Promoting cybersecurity awareness and providing comprehensive training to employees, suppliers, and partners can enhance overall security posture and reduce the risk of human error or insider threats within the supply chain.

Developing and regularly testing incident response plans and exercises in collaboration with supply chain partners can improve coordination, communication, and overall preparedness in the event of a cyber incident.

By fostering collaboration and information sharing, organisations can leverage collective knowledge, resources, and expertise to stay ahead of emerging cyber threats and enhance the overall resilience of their supply chains.

To safeguard your supply chain from cyber threats and ensure business continuity, it is crucial to prioritise cybersecurity as a strategic imperative. The importance of cybersecurity in supply chain management cannot be overstated. As supply chains become increasingly interconnected and digitised, the potential for cyber threats escalates, posing significant risks to operational continuity, data integrity, and financial performance. By understanding common cyber threats, implementing robust security measures, leveraging cutting-edge technologies, and fostering collaboration and information sharing, organisations can fortify their defences and maintain a secure and resilient supply chain ecosystem. Embracing a proactive and comprehensive approach to supply chain cybersecurity is no longer an option but a necessity for businesses seeking to thrive in the digital age.

Dependence on digital technologies, while beneficial, exposes supply chains to cyber risks affecting operations, brand perception, and consumer trust.

Notably, these risks can stem from partner organisations' security weaknesses. For instance, in 2018, Marriott Hotels revealed that cyber attackers had stolen data from 500 million customers through a breach at Starwood Hotels, acquired by Marriott in 2016. This incident underscores that even with robust internal security, vulnerabilities in partner systems can lead to significant data breaches.[11]

Cyber risks come from various sources, including external actors and internal misuse of systems. Additionally, there is a physical component to the cyber supply chain, involving servers and telecommunications devices. Proper sourcing and maintenance of this infrastructure are crucial for cybersecurity. Globalisation further complicates this, as physical components and software may be produced in different countries.

While technology offers significant benefits, it also introduces complex risks that supply chain leaders must strategically manage. Supply chain executives must consider a few fundamentals for managing cyber risks. The first is to understand cyber risks in the supply chain. The second is to develop a strategy and culture for managing these risks. The third is integrating with key partners. The fourth is deciding on investment in protection.

These fundamentals help managers raise awareness and better position supply chains to meet cyber threats. Supply chain professionals must create value-driven supply chains ready for digital challenges. But what do terms like *cybersecurity* or *cyber risk* mean? How can they drive understanding and action? Here are key definitions to grasp cyber risk in the supply chain.

Factors that influence cybersecurity include physical infrastructures and devices like SCADA systems, smartphones, computers, and servers. They include computer systems and embedded software enabling operations and connectivity. Networks between computer systems are also important. Embedded processors and controllers can impact on security. User access nodes and intermediary routing nodes are also factors, as are constituent data, such as DNS records. However, the most important factor remains people, prone to human error.

Supply Chain Cyber Risk

Cyber risk is an operational risk to information and technology assets, affecting confidentiality, availability, or integrity. It involves malicious electronic events causing business disruption and monetary loss. Cyber risks can affect both digital and physical assets and arise from internal or external vulnerabilities. These risks can be classified by their source (e.g., malicious actors, external organisations, non-malicious actors), areas of vulnerability (e.g., external partners' weaknesses), or specific targets (e.g., information systems, electronic devices, unwitting individuals).

Understanding these terms is crucial for managing cyber risks in supply chains. Risks can arise from mismanagement of information networks,

leading to data loss, intellectual property theft, or operational disruptions. This aspect of cyber risk is often confused with *information risk*, but they are not the same. Cyber risks cover a broader range of threats to both physical and digital assets. A *cyber attacker* is an individual or entity that perpetrates an attack. While cyber attackers are a common source of cyber risks, simple mismanagement of information and technologies can also pose risks. *Cybersecurity* refers to the technologies, processes, and practices designed to protect data, networks, and other assets from attacks, damage, or unauthorised access.

Supply chain cyber risks are an emerging threat that organisations are beginning to understand. A critical mistake is treating cyber risks like any other business risk. Traditional risk management focuses on discrete events, but cyber risks are constantly evolving. Thus, cyber risk management must be evolutionary, with continuous improvement of mitigation techniques.

A health analogy is apt: just as good hygiene minimises infection risk but doesn't guarantee health, companies need both good structures and constant adaptation to new threats. Misunderstanding cyber risks makes identifying vulnerabilities and predicting targets difficult. Attackers may not have clear targets until they gain entry, complicating the assignment of responsibility for defence. Often, organisations delegate cybersecurity to IT or legal departments due to this lack of clarity and this causes further problems. Understanding and managing cyber risks in supply chains require continuous adaptation and strategic integration with key partners.

Cyber risks require systematic integration across stakeholders. Organisations often focus on obvious targets like customer data and intellectual property, but breaches have broader implications. Supply chain managers are largely unaware of third-party risks, which are significant. McAfee estimates cyber crime costs the global economy $445 billion annually. Cyber risk is increasingly one of the most significant business risks.[12]

Cyber risks can have cascading effects on supply chains, impacting reputation and financial performance. For example, Yahoo's data breaches led Verizon to reduce Yahoo's valuation by $350 million.[13] Cyber incidents can also disrupt physical supply chains, shutting down suppliers and affecting operations. Third-party breaches are rising, with over 60% of breaches occurring through third parties.[14]

Most supply chain managers are unaware of third-party risks and remain company-centric in addressing them. The tendency to assign cybersecurity to IT or legal departments, often increases these vulnerabilities. Senior executives struggle with cybersecurity investment, often making siloed decisions. Joint investments in cybersecurity across the supply chain are rare.

Supply chain management lacks a systematic approach to cyber risk. Leading supply chain managers focus on collaboration with suppliers and partners to reduce risks. Although few organisations have figured out cyber supply chain security, best practices can be identified.

Engagement with industry leaders has helped identify *best practices* in supply chain cyber security. These practices are detailed in the following case study.

Best practices build on physical supply chain management concepts but adjust for cybersecurity risks: catalogue, map processes, clear strategy, critical systems, incident response planning, latest cyber defence systems, ongoing training and awareness, use AI and ML, unplug, treat cybersecurity like supply chain work, and active defence.

Understanding your supply chain and cataloguing your cyber inventory is the first step. Leading organisations map supply chain nodes and transitions, providing visibility into the people and processes relying on IT systems and existing risk protections. Cataloguing cyber inventory (hardware and software) is crucial for effective risk protection.

Next, create a clear cyber risk strategy addressing critical choices and directing work to improve cybersecurity. This includes identifying business-critical systems and building aggressive controls for them. A clear incident response plan is also essential.

Continuous improvement is key. Leading companies update systems with the latest defence mechanisms, collaborate cross-functionally to validate incoming equipment and systems, and ensure timely communication of risks and protections across the supply chain.

The people dimension is also vital. Ongoing training and awareness, including experiential training, are necessary. Leading organisations are intentional in digitising their supply chains, ensuring robust cybersecurity measures. These best practices help organisations manage cyber risks effectively, ensuring a secure and resilient supply chain.

New tools like AI and ML enhance capabilities but also increase cyber risk. Leading organisations assess which systems need connectivity and which can be "unplugged" without losing benefits. They use traditional supply chain management to ensure cybersecurity, treating it like any other supply chain capability. This includes using scorecards, action planning, leadership reviews, and problem-solving processes like Lean and Six Sigma. Continuous skill development and E2E strategic concepts (collaboration, integration, and synchronisation) are crucial.

The cyber risk environment is dynamic. Best practices include active defence tools like decoys and misdirection, though these have ethical and legal implications. Managers should research these thoroughly.

First principles for implementing best practices include understanding cyber risks in the supply chain. Managers often highlight a lack of understanding about cyber risks. They stress the importance of knowing the types and sources of cyber risk and using a quantitative approach to assess risks.

Cyber risks can be classified into cyber-espionage, DDoS attacks, crime ware, web app attacks, Insider misuse, miscellaneous errors, physical theft and loss, information skimmers, and point of sale intrusions.

Sources of cyber risks are less understood, but organisations can start by identifying these.

To understand supply chain cyber risks, we must assess attack vectors, tactics, and weaknesses.

Attack Vectors

Cyber risks come from strategic (targeted) or non-strategic (random) attackers. These can be state-sponsored, criminal, or general cyber attackers. Risks also come from non-malicious insiders who accidentally share sensitive data. For example, cloud computing introduces risks like data leaks and regulatory issues, not always from attackers.

Tactics

Examine how attackers breach systems or how data leaks occur. Often, weak links in supply chain partners (suppliers, distributors, retailers) are overlooked. Emerging technologies in manufacturing pose challenges due to unidentified design weaknesses. A holistic view of supply chain vulnerabilities, both technological and human, is essential. Technological risks include data manipulation and hacking, while human risks involve employee processes that enable attacks.

Weaknesses

Identify critical points in the supply chain that could be vulnerable. Both internal and external nodes in the global supply chain need scrutiny. Understanding the technological and human components helps in identifying how breaches occur.

Managing cyber risks in supply chains requires understanding the sources, methods, and critical points of vulnerability. This approach helps in developing effective strategies to mitigate these risks.

Cyber risks in supply chains can be categorised by what is at risk. Four main processes are especially vulnerable: managing information about demand, physical flow of goods, financial flows, and order management. Specific sub-processes like purchasing, supplier management, order management, inventory monitoring, manufacturing control, and financial payments are particularly at risk. Networks, computers, and devices used in these processes are susceptible to attacks like password sniffing, spoofing, denial of service, and hacking.

Physical assets in the supply chain can also be compromised. For example, attackers may target products with technology components. RFIDs in global supply chains are vulnerable to eavesdropping, unauthorised tracking, and tampering. The global nature of production adds complexity, with physical

components often made in China, Japan, South Korea, and Taiwan, and software development outsourced to countries like India and Ukraine. Mismanagement of these global suppliers can increase cyber risks.

Managers should categorise cyber risks to secure supply chains. New risks, such as those from e-marketplaces, include ensuring member legitimacy, data security, and accurate information. Emerging threats like document forgery, counterfeiting, and corporate identity theft are challenging to assess due to limited data. These risks can impact physical assets, cargo, and human resources.

Despite the difficulty in quantifying cyber risks, a systematic approach is essential. Managers must continuously adapt to evolving threats and integrate cybersecurity with key partners to protect supply chains effectively.

Effective risk management relies on assessing potential impacts. For cyber risks, this is crucial as they can have widespread effects. Most managers use a qualitative approach, like colour-coded scales, which is problematic for unique and complex risks. A quantitative approach is more accurate for assessing cyber risks.

Qualitative methods add ambiguity. Terms like "high risk" can mean different things to different people. For example, asking a group to estimate the likelihood of a "high risk" event can yield a wide range of answers, causing confusion. Similarly, "high impact" can mean anything from $10,000 to $10 billion in losses.

Assigning numbers to probabilities and expected losses, even in ranges, brings clarity. This quantitative approach can be managed using tools like Monte Carlo simulations in Excel. These simulations can quickly provide a range of expected losses, aligning with a company's risk tolerance.

Once probabilities and losses are assigned, the process is straightforward. Different groups within the organisation can complete this in less than half a day. The output can then be compared to the company's risk tolerance.

Understanding and managing cyber risks in supply chains require a strategic, quantitative approach. This ensures clarity and accuracy, helping organisations protect their operations and maintain resilience.

Critical business systems include proprietary information and devices crucial to business success. *Risk management* of critical business systems is crucial. Manage these systems aggressively and where necessary disconnect from the internet. Avoid IoT, cloud computing, AI, and ML where risk is too high. Use a small, skilled team over automated solutions. Mandate immediate software upgrades. Hold weekly cyber training. Implement multi-step password verification. Deploy advanced defence systems like trip wire detection and air gaps. Review cyber supply chain maps monthly. Understand and identify sources of cyber risk. Use a quantitative approach to assess risks.

Develop a cyber risk management strategy: A clear strategy is essential. Strategies may focus on strengthening security perimeters or building resilience to respond to breaches. Organisations must choose based on industry, product type, risk exposure, and tolerance.

Effective cyber risk management in supply chains requires continuous monitoring, aggressive management of critical systems, and a clear, adaptable strategy. This approach ensures supply chains remain secure and resilient.

Assume one device in the supply chain is always breached. Use a mix of preventive and resilience strategies. Cyber risk mitigation can follow existing frameworks like ISO 27001, ITIL, and NIST.

Cyber risk management frameworks: Numerous frameworks exist, including ASD, COBIT, HISO, NIST, CCPA, EU GDPR, ISO 27001, NZISM, CIS, HIPAA, ITIL, and PCI DSS.

Documentation and certifications are available online. Supply chain managers can use these frameworks to develop a holistic cybersecurity strategy. The *NIST Framework* is widely used for cyber risk management. It is a voluntary framework with standards, guidelines, and best practices to manage cybersecurity risks. Created to protect critical infrastructure and sectors vital to the economy and national security, it provides a common language for discussing cyber risk. This allows stakeholders to adapt the framework to their specific technologies, lifecycle phases, and sectors, ensuring everyone is aligned. The framework includes implementation tiers to benchmark an organisation's prevention and reaction capabilities, promoting a risk-based, outcome-focused approach.

The NIST Framework details five foundational functions of cybersecurity risk management: *Identify, Protect, Detect, Respond* and *Recover. Identify* is crucial to establish an understanding of cybersecurity risks to systems, assets, data, and capabilities. *Protect* is important to develop and implement safeguards to secure critical infrastructure services. *Detect* is vital to develop the ability to identify cybersecurity events. *Respond* implores us to take action regarding detected cybersecurity incidents. *Recover* encourages us to plan for resilience and restoration of impaired capabilities or services.

The NIST Framework is one of several models available for companies to build their cybersecurity strategy. Supply chain managers can adopt or adapt these frameworks as needed. However, developing a culture that supports the chosen risk mitigation strategy is crucial.

An organisation's culture, influenced by norms of behaviour and attitudes, is key to achieving a low-risk cyber supply system. This culture must be developed across the entire supply system, crossing company boundaries. Norms and behaviours are shaped by people systems, including rewards, rituals, promotions, compensation, communication, problem-solving, celebration, and role modelling. A few key systems and activities strongly influence norms and behaviour. Some organisational cultures support strong cybersecurity capability, while others resist it. Resistant cultures have unique cultures for each functional group or supply partner, leading to distrust. Cultures promoting cybersecurity encourage seamless, collaborative, end-to-end integrated systems. Benchmark companies establish common cyber principles, values, and standards, ensuring all business functions and systems support full collaboration to achieve business goals.

Tahmasebi (2024) argues cyber resilience includes anticipatory defences, stakeholder synergy, and the cultivation of a pervasive security-centric culture. Continuous vigilance, persistent innovation, and the integration of security as a core element of corporate ethos are paramount in mitigating cyber risks. Harnessing predictive analytics, cultivating a collaborative environment for unified cyber resilience, and instilling a lasting security mindset within organisational practices help to foster cyber resilience.[15]

Security best practices include common standards, values, and principles across the supply system. Learning culture across boundaries is vital. Rewarding attention to detail and risk management best practices is important. Continuous improvement is needed of cultural systems. Overlapping functional and company rewards systems helps. It is important to celebrate total value improvement with supply partners. Cross-discipline, company, and functional collaboration is necessary.

An effective strategy and cultural change within and across organisations are crucial for combating supply chain cyber risks. Organisations and their key suppliers and customers should follow a consistent supply chain cyber risk management strategy, adhering to a framework. This requires a cultural change and a different mindset in managing such risks. Benchmark supply chain leaders focus on total involvement in mitigating cyber risks, recognising that all people and technologies in a cyber environment represent potential risks. A culture built around the idea that cybersecurity is a complex problem requiring the entire organisation's effort is essential.

Integrating with key partners: Supply chain integration involves collaboration across various functions like IT, finance, and marketing, and with supply chain partners to achieve shared goals. Many companies still operate in isolation, assuming they can manage within their own walls. However, research shows that focusing only on individual processes harms overall supply chain performance, especially in cybersecurity.

Effective cybersecurity requires integration at three levels: functional, organisational, and end-to-end supply chain. This evolution in thinking helps companies better address cyber risks. Initially, companies may focus on a specific function, often IT, to manage cybersecurity. This approach is reinforced by organisational norms that channel IT-related concerns through the IT department. In some cases, the legal department handles cyber risks, viewing them as compliance issues.

These functional approaches often reflect a limited understanding of the full range of cyber risks and their impact on operations, financials, and brand perception. While starting with a functional focus can build a foundation of knowledge, it is insufficient for effective cybersecurity. A successful strategy requires a shift in mindset across the organisation.

Organisations must transition from a functional to an organisational focus, and finally to an end-to-end supply chain focus, retaining best practices at each stage. This comprehensive approach ensures that all parts of the

supply chain are considered, leading to better overall performance and security.

By integrating with key partners and adopting a holistic approach, companies can better manage cyber risks and enhance supply chain security. This makes clear that this is not an IT or legal issue, but rather a serious business risk that needs to be tackled by multiple camps within and across organisations.

An expanded view of cyber risks includes multiple functions within the organisations becoming involved in formulating the strategy and dealing with the risk. Managers in organisations realise that cyber risks represent an organisation-wide concern that needs to be addressed with the participation of several units, not just the IT department. This more integrated approach could include creating a Chief Information Security Officer (CISO), who would be charged with coordinating cybersecurity with the CIO, COO, and other executives involved in supply chain management. It would also likely involve creating a systems security plan (SSP). An SSP details current measures for securing a company's information systems and provides a critical starting point for improving those cybersecurity processes. While an improvement on the functional focus approach to cybersecurity, the organisational focus approach still lacks the involvement of other members of the supply chain. This leaves companies vulnerable, because the weakest link in their cybersecurity strategy may well be a third-party provider. Investment decisions related to cybersecurity are typically suboptimal without an end-to-end supply chain approach. Benchmark supply chain leaders focus on end-to-end integration to strengthen the weakest link in their supply chain and mitigate cyber risks.

End-to-end supply chain focus is key. Having a supply chain-wide view when addressing the scope of supply chain cyber risks is necessary to have an effective strategy. As with other E2E supply chain initiatives, E2E integration concerning cybersecurity rests on three core components: supply chain collaboration, end-to-end process management, and reciprocal flows of high-quality information to enable decision-making.

Supply chain collaboration is the process of working with strategic partners to identify, define, and pursue specific business opportunities that have the potential to increase overall supply chain value. In the context of supply chain cyber risk management, collaboration must start with a common understanding of the types and sources of cyber risk impacting the supply chain. Next, a quantitative assessment of probabilities and expected losses associated with relevant risks, and identification of the greatest opportunities and challenges that need to be addressed. Achieving this common understanding requires detailed mapping of the supply chain, from suppliers' suppliers to end users. Having a supply chain-wide view when addressing the scope of supply chain cyber risks is necessary to have an effective strategy. Making informed cybersecurity decisions requires data analytics that provide real-time information for leadership and management.

End-to-end process management focuses on linking decision-making across the supply chain into a single, seamless process. Cyber risks are not just IT or legal issues but serious business risks needing a multi-departmental approach.

Decisions on E2E process management in supply chains involve evaluating trade-offs, especially in cybersecurity. Understanding threats and making informed investments are crucial. Data and information are key tools for combating cyber risks. Real-time data analytics enable proactive and predictive decision-making, focusing on relevant threats and adaptable for different users.

Leading companies use E2E strategies to prevent and mitigate cyber attacks. They segment data and define access protocols with partners, allowing quick system quarantine during breaches and better understanding of compromised areas. They also gather incident data to use advanced analytics for identifying vulnerabilities.

Integration can be internal or with partners, focusing on collaboration, E2E process management, and high-quality information flows. This supports achieving cybersecurity and creating value for stakeholders. Approaches focusing on specific functions or organisations often have awareness gaps. Few manage cyber risks systematically, though some require supplier certification. Leading organisations can differentiate by adopting comprehensive risk strategies.

Senior executives often make cybersecurity investment decisions in silos, ignoring other critical supply chain organisations. For example, a large retailer might invest heavily without considering the broader supply chain context.

This shortened chunk maintains the original structure and key points, focusing on the importance of data, best practices, and the need for E2E integration in cybersecurity. Retailers invest heavily to protect customer data due to the high cost of breaches. However, suppliers may not be as motivated, as breaches cost them less. Cyber attacks impact both the targeted firm and its supply chain. Effective cybersecurity requires collaboration within the supply chain. Without it, firms may not invest optimally.

Our analysis compared collaborative and non-collaborative cybersecurity investments and the effects of strategic versus non-strategic attackers. Lack of collaboration often leads to underinvestment with non-strategic attackers. With strategic attackers, it can cause either underinvestment or overinvestment, depending on the indirect damages.

A game theory approach, the attacker–defender model, helps determine optimal cybersecurity investments. Each firm in the supply chain is a defender, deciding how much to invest. The attacker, representing potential threats, observes these investments and targets firms accordingly. The model uses a 2x2 matrix to depict scenarios based on whether the attacker is strategic and whether defenders collaborate.

The matrix helps organisations determine optimal investment levels by considering different variables, such as sector-specific threats. This approach, commonly used in counterterrorism, has been applied to cybersecurity to enhance supply chain security.

Best practices in cyber supply chain security include high collaboration where there is better coordination and consideration of indirect costs and benefits, and greater collaboration is needed where there is likely underinvestment and risk transfer to less secure members.

By adopting these practices, organisations can improve their cybersecurity posture and protect their supply chains more effectively. A lack of collaboration in the supply chain creates gaps in awareness regarding the true costs and benefits of cybersecurity investments, skewing decisions on where and how to invest to manage cyber risks.

Non-Strategic Attacker

If attackers are non-strategic (random attacks) and firms do not collaborate, they will underinvest in cybersecurity. Non-collaborative firms consider only direct costs and benefits, ignoring significant indirect costs and benefits from their supply chain. This leads to misallocation of investments, especially when non-strategic attacks have a large potential impact on the supply chain. Over time, this underinvestment grows, increasing vulnerabilities. Adopting an end-to-end supply chain collaboration approach is critical to map out mutual benefits of a collaborative cybersecurity strategy.

The more interdependent non-collaborative firms are, the more they misallocate cybersecurity investments. This misallocation is worst when non-strategic attacks have the largest potential to affect the supply chain. Over time, lack of investment among non-collaborative firms increases vulnerabilities.

Strategic Attacker

If an attacker is strategic (focused on a particular network), non-collaborative firms increase cybersecurity investments. However, this increases risks for the supply chain by transferring risk from more secure to less secure members. Vulnerable suppliers or third-party providers become more aggressively targeted, increasing overall cyber risks.

The risk transfer problem is worse in loosely connected supply chains. Stronger firms invest to protect themselves, transferring risks to weaker firms. This can only be addressed through end-to-end supply chain collaboration.

Collaborative investment decisions: Dominant supply chain players should invest in consortiums to improve the cybersecurity of vulnerable third parties. The main challenge is defining and creating value for all partners. Managers must assess the risk to supply chain value from various cyber threats.

Collaboration on cybersecurity investments can limit resource misallocation and negative consequences. Developing collaborative mechanisms for coordinating cybersecurity investments is critical for managing cyber threats.

Catalogue and identify all systems (hardware and software) that create cyber risk. Modify supply chain maps to document systems, cyber risks, people interaction, and existing protections. Develop a clear cyber risk strategy to guide efforts. Identify and aggressively manage business-critical systems. Create and follow an incident response plan. Treat cyber like supply chain work. Use supply chain tools and processes to address cyber risks. Apply end-to-end strategic concepts to manage supply chain cyber risk holistically. The latest cyber defence systems are vital. Continuously implement modern defence. By integrating practices, organisations can manage cyber risks and enhance supply chain security.

Validation: Engineering, IT, and procurement must validate incoming equipment and systems for cyber risk, covering the entire supply chain as most risks are external. Logistics, manufacturing, IT, procurement, and other supply chain disciplines must validate suppliers, external manufacturing, third-party logistics (3PLs), and other partner cyber systems interfacing with business systems.

Disconnect: Systems connected to the internet cannot be cyber-risk free. Unplug critical systems that can be managed without the internet. Industries like nuclear, information systems, and pharmaceuticals have used this practice for years on critical systems. This involves defining critical systems and using captive systems managed by dedicated experts to reduce cyber risk. As cyber risk grows, this practice is expanding to less technical industries.

Careful use AI and ML: Digitalisation of the supply chain creates new capabilities but also increases cyber risk with tools like AI and ML. These tools enhance supply chain efficiency by analysing large data sets but also expose the supply chain to higher cyber risks.

Security awareness: Annual cyber risk training is outdated. Training and awareness must be ongoing and experiential.

Acquisition integration: Validate acquisition systems before integration. This should be included in acquisition plans and resources.

Active defence: This is a tool to combat cyber risk, not hacking back. It has ethical and legal implications and should be thoroughly researched before use.

Digitalisation is transforming supply chains and increasing cyber risks. New cyber risks impact businesses through partner security weaknesses. To build robust cybersecurity in complex supply chains, internal and external stakeholders must collaborate. Managers need full involvement in understanding risks using a quantitative approach and developing strategies based on best practices. Organisations must integrate with key partners across the supply chain to manage cyber risks and decide on investments to protect it. Cyber risk in the supply chain is evolving. Supply chain leaders must incorporate cybersecurity strategies or face the consequences.

Notes

1 Van't Schip, M., 2024. The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things. *European Journal of Law Technology*, 15(1), pp.334–351.
2 Salvi, A., Spagnoletti, P., and Noori, N.S., 2022. Cyber-resilience of Critical Cyber Infrastructures: Integrating Digital Twins in the Electric Power Ecosystem. *Computers & Security*, 112, p.102507.
3 Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T., 2022. The Drivers of Cyber Risk. *Journal of Financial Stability*, 60, p.100989. https://doi.org/10.1016/j.jfs.2022.100989.
4 Boh, W., Constantinides, P., Padmanabhan, B., and Viswanathan, S., 2023. Building Digital Resilience against Major Shocks. *Mis Quarterly*, 47(1), pp.343–360.
5 Garcia-Perez, A., Cegarra-Navarro, J.G., Sallos, M.P., Martinez-Caro, E., and Chinnaswamy, A., 2023. Resilience in Healthcare Systems: Cyber Security and Digital Transformation. *Technovation*, 121, p.102583.
6 Al-Hawamleh, A., 2024. Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security. *International Journal of Computing and Digital Systems*, 15(1), pp.1315–1331.
7 Adenekan, O.A., Ezeigweneme, C., and Chukwurah, E.G., 2024. Strategies for Protecting IT Supply Chains against Cybersecurity Threats. *International Journal of Management & Entrepreneurship Research*, 6(5), pp.1598–1606.
8 Plachkinova, M., & Maurer, C., 2018. Teaching Case: Security Breach at Target. *Journal of Information Systems Education*, 29(1), pp.11–20.
9 Crosignani, M., Macchiavelli, M., & Silva, A.F., 2023. Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. *Journal of Financial Economics*, 147(2), pp.432–448.
10 Hoang, H.V., 2023. Better Prevention than Cure: Cybersecurity Risk and Clawback Provision. https://doi.org/10.2139/ssrn.4536035.
11 https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.
12 https://www.itgovernanceusa.com/blog/cyber-crime-costs-the-global-economy-445-billion-a-year.
13 https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b.
14 https://www.prevalent.net/blog/2024-third-party-risk-management-study.
15 Tahmasebi, M., 2024. Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. *Journal of Information Security*, 15(2), pp.106–133.

6

WORKFORCE RESILIENCE

Culture Change & Security Awareness

Workforce Resilience

Workforce resilience has become a critical attribute for organisations to thrive amidst uncertainty. A resilient workforce is the backbone of a successful company, capable of adapting to change, overcoming challenges, and driving innovation. We live in an era where disruptive forces, such as technological advancements, global economic shifts, and unforeseen events, can profoundly impact businesses. Cultivating a resilient workforce empowers organisations to navigate these turbulent times with agility, ensuring long-term success and competitive advantage.

Boh et al. (2023) caution against thinking of technology as a panacea to develop resilience and contend that digital resilience requires entities to develop a deeper understanding of how people, processes, and culture collectively act to shape the future of various entities during the next major shock.[1]

Olaniyi et al. (2024) contend that by fostering resilience within our workforce, we create a culture of continuous learning, innovation, and adaptability, enabling our organisation to stay ahead of the curve. They argue for greater use of artificial intelligence, automation, and rolling out employment policies that support workforce resilience through upskilling and retraining initiatives.[2]

Ajayi and Udeh (2024) maintain that workforce upskilling initiatives for emerging technologies can be made more successful by better understanding employees as individuals. Resilient employees possess the mental fortitude, emotional intelligence, and problem-solving skills to tackle obstacles head-on. They embrace change as an opportunity for growth and are willing to step out of their comfort zones.[3]

DOI: 10.4324/9781003604969-6

Moreover, a resilient workforce contributes to improved employee engagement, productivity, and overall well-being. When individuals feel supported and equipped to handle challenges, they are more likely to remain motivated, committed, and loyal to the organisation. This, in turn, translates into a positive work environment, reduced turnover rates, and enhanced customer satisfaction.

In today's volatile and unpredictable business environment, organisations face a myriad of challenges that can test their resilience. Economic downturns, market disruptions, and rapidly changing consumer preferences are just a few examples of the hurdles that businesses must navigate. Additionally, the COVID-19 pandemic has highlighted the importance of agility and adaptability, as companies were forced to pivot their operations and embrace remote work models.

Nguyen et al. (2024) argue that technological advancements, while presenting opportunities, also pose challenges. Staying ahead of the curve and integrating new technologies into existing processes can be daunting, requiring a workforce that is open to continuous learning and upskilling.[4]

Furthermore, globalisation and increased competition have intensified the need for organisations to differentiate themselves and remain competitive. Attracting and retaining top talent has become a critical factor in maintaining a resilient workforce capable of driving innovation and growth.

To cultivate a resilient workforce, organisations must adopt a multifaceted approach that addresses various aspects of employee development and organisational culture.

Develop a culture of adaptability and flexibility. Enhance communication and transparency within the organisation. Invest in employee training and development. Promote work–life balance and employee well-being. Embrace technology for remote work and collaboration. Build a diverse and inclusive workforce. Measure and evaluate the resilience of your workforce.

Fostering a *culture of adaptability and flexibility* is crucial for building a resilient workforce. We must encourage our employees to embrace change as an opportunity for growth and innovation.

Promoting a growth mindset is essential. Encourage employees to view challenges as opportunities for learning and personal development. Implement agile methodologies. Adopting agile practices enables rapid adaptation to changing circumstances and customer needs. Encouraging cross-functional collaboration is vital. Breaking down silos and facilitating cross-team collaboration foster knowledge sharing and diverse perspectives. By cultivating an environment that celebrates adaptability and flexibility, we empower our workforce to navigate uncertain times with resilience and agility.

Effective communication and transparency are essential for building trust and fostering resilience within our workforce. When employees feel informed and involved, they are better equipped to handle challenges and contribute to the organisation's success. We can enhance communication and transparency.

Regular and open dialogue is essential. Conduct regular town hall meetings, team huddles, and one-on-one check-ins to share information and address concerns. Transparent decision-making is important. Involve employees in the decision-making process and provide clear rationales for organisational changes or strategic shifts. Feedback loops are important. Establish robust feedback mechanisms that allow employees to voice their opinions, concerns, and ideas for improvement.

By fostering an environment of open communication and transparency, we create a sense of shared purpose and empowerment, enabling our workforce to navigate uncertainties with confidence and resilience.

Investing in employee learning and skill development are essential for building a resilient workforce capable of adapting to changing market demands and technological advancements. Through continuous learning through employee training and development programmes, we equip our workforce with the necessary tools and knowledge to thrive in uncertain times.

Upskilling and reskilling initiatives are vital, providing opportunities for employees to acquire new skills and knowledge relevant to their roles and the organisation's evolving needs. Leadership development programmes are crucial, cultivating strong leadership capabilities that can guide teams through challenging times and foster resilience. Mentorship and coaching: implement mentorship and coaching programmes that facilitate knowledge transfer and personal growth.

By prioritising continuous learning and development, we empower our workforce to embrace change, stay relevant, and contribute to the organisation's long-term success.

Promoting *work–life balance and employee well-being* is essential. A resilient workforce is built on the foundation of employee well-being. When individuals feel supported and cared for, they are better equipped to handle stress and navigate challenges with resilience. We can promote work–life balance and employee well-being. Flexible work arrangements are important to employees. Offering flexible schedules, remote work options, and family-friendly policies supports work–life integration. Employee assistance programmes are a vital lifeline and provide access to counselling, mental health resources, and wellness initiatives to support emotional and physical well-being. Encouraging breaks and downtime are crucial. It is important to promote taking breaks, vacations, and engaging in activities that promote work–life balance.

By prioritising employee well-being, we create a supportive environment that fosters resilience, reduces burnout, and enhances overall productivity and engagement.

Technology plays a pivotal role in enabling remote work and seamless collaboration, both essential components of a resilient workforce. By embracing the right tools and platforms, we can facilitate effective

communication, knowledge sharing, and productivity, even in the face of physical distance or disruptions.

Cloud-based collaboration tools are vital. Implement secure and user-friendly platforms for document sharing, video conferencing, and real-time collaboration. Project management software is relied upon. Adopting project management tools enables teams to track progress, assign tasks, and streamline workflows. Leveraging online learning platforms and virtual training sessions facilitates continuous skill development.

By leveraging technology effectively, we enable our workforce to remain connected, productive, and resilient, regardless of their physical location or external circumstances.

Diversity and inclusion are critical components of a resilient workforce. By fostering an environment that celebrates diverse perspectives, backgrounds, and experiences, we tap into a rich pool of ideas, creativity, and problem-solving approaches. This diversity of thought enables our organisation to adapt and thrive in uncertain times.

We can promote diversity and inclusion through inclusive recruitment practices. Implementing fair and unbiased hiring processes helps to attract and retain talent from diverse backgrounds. Diversity and inclusion training is important. Provide education and awareness programmes to promote understanding, respect, and appreciation for diverse perspectives. Establishing employee-led groups that celebrate and support various dimensions of diversity helps in fostering a sense of belonging and community.

By embracing diversity and inclusion, we cultivate a resilient workforce that is better equipped to navigate complex challenges, innovate, and succeed in an ever-changing business landscape.

Measuring and evaluating the resilience of your workforce is vital to ensure the effectiveness of our resilience-building strategies. This can be achieved through employee surveys and feedback. Conduct regular surveys and gathering feedback to assess employee sentiment, engagement, and resilience levels. Track key performance indicators (KPIs) related to productivity, innovation, and adaptability to gauge the impact of resilience initiatives. Resilience assessments are useful. Implement specialised assessments and tools to evaluate individual and organisational resilience, and identify areas for improvement.

By continuously measuring and evaluating the resilience of our workforce, we can make data-driven decisions, refine our strategies, and ensure our efforts are yielding the desired outcomes.

Case Studies

To illustrate the power of a resilient workforce, we can consider a few real-world examples of companies that have successfully navigated challenging times by cultivating resilience within their organisations.

Airbnb: During the COVID-19 pandemic, Airbnb faced an unprecedented crisis as travel ground to a halt. However, the company's resilient workforce, fostered through transparent communication, employee support programmes, and a strong culture of adaptability, enabled them to pivot their business model and emerge stronger. They embraced virtual experiences, enhanced cleaning protocols, and expanded into new markets, demonstrating remarkable resilience and agility.

Microsoft: As a technology leader, Microsoft has consistently adapted to disruptive changes in the industry. Their commitment to continuous learning, upskilling initiatives, and fostering a growth mindset has enabled their workforce to stay ahead of the curve. Microsoft's resilient workforce has been instrumental in driving innovation, embracing cloud computing, and expanding into new domains such as artificial intelligence and mixed reality.

Patagonia: The outdoor apparel company Patagonia is renowned for its commitment to sustainability and environmental stewardship. However, their resilience extends beyond their eco-friendly practices. Patagonia has cultivated a resilient workforce by promoting work–life balance, offering generous benefits, and fostering a culture of purpose and social responsibility. This resilient workforce has enabled the company to navigate challenges, maintain its values, and continue to innovate in sustainable fashion.

These examples demonstrate the power of a resilient workforce in overcoming adversity, seizing opportunities, and driving long-term success.

In today's rapidly changing and uncertain business landscape, cultivating a resilient workforce is no longer an option but a necessity. By embracing the strategies outlined, we can empower our employees to navigate challenges with agility, adapt to change, and thrive in the face of adversity.

Fostering resilience requires a holistic approach that addresses organisational culture, communication, employee development, well-being, and technological enablement. It demands a commitment to continuous improvement, measurement, and adaptation.

As we build a resilient workforce, we not only enhance our organisation's ability to weather storms but also unlock a competitive advantage. Resilient employees are more engaged, innovative, and productive, contributing to our long-term success and sustainability.

Fostering Resilience in Culture

Cybersecurity awareness plays a vital role. Workforce resilience is not a one-time endeavour but a continuous journey. As technology continues to permeate every aspect of our personal and professional lives, the need to cultivate a robust cybersecurity culture within organisations has become paramount. By embedding resilience into the fabric of our organisation, we create a workforce that is equipped to navigate the uncertainties of today and embrace the opportunities of tomorrow.

Cybersecurity awareness encompasses the knowledge, skills, and attitudes necessary to recognise and mitigate potential cyber threats, safeguarding sensitive information and ensuring business continuity. It plays a critical role in strengthening workforce resilience, with multifaceted dimensions and providing actionable insights for creating a secure and vigilant organisational culture. By fostering a deep understanding of cybersecurity principles, we can empower our workforce to become an active line of defence against ever-evolving cyber risks.

Workforce resilience is the cornerstone of organisational success in the face of cyber threats. A resilient workforce possesses the ability to adapt, respond, and recover from cyber incidents swiftly and effectively. By cultivating a culture of cybersecurity awareness, organisations can enhance their workforce's capacity to identify and mitigate potential risks, minimising the impact of cyber attacks and ensuring business continuity.

In today's digital age, cyber threats are not only persistent but also increasingly sophisticated. From malware and phishing attacks to data breaches and ransomware incidents, the consequences of a successful cyber attack can be devastating, resulting in financial losses, reputational damage, and operational disruptions. A resilient workforce, armed with the knowledge and skills to recognise and respond to these threats, becomes an invaluable asset in safeguarding the organisation's critical assets and maintaining trust with stakeholders.

Creating a strong *cybersecurity culture* within an organisation is crucial for fostering a resilient workforce. Culture shapes the attitudes, behaviours, and values that influence how individuals perceive and respond to cyber risks. By embedding cybersecurity awareness into the organisational DNA, we can cultivate a proactive and vigilant mindset, where every employee recognises their role in maintaining a secure digital environment.

Effective cybersecurity awareness initiatives should go beyond mere compliance or check-box exercises. Instead, they should aim to inspire a genuine understanding of the importance of cybersecurity and its direct impact on the organisation's success. When employees internalise the significance of cybersecurity and embrace it as a shared responsibility, they become active participants in safeguarding the organisation's digital assets.

To build an effective cybersecurity awareness programme, it is essential to understand the prevalent threats and vulnerabilities that organisations face.

Phishing attacks: Fraudulent attempts to steal sensitive information or gain unauthorised access through deceptive emails, text messages, or social engineering tactics.

Malware infections: The spread of malicious software designed to disrupt operations, steal data, or gain unauthorised access to systems.

Ransomware attacks: Cyber attacks that encrypt an organisation's data and demand a ransom payment for its decryption.

Data breaches: The unauthorised access, theft, or exposure of sensitive or confidential information.

Social engineering: Manipulative tactics used by attackers to exploit human psychology and trick individuals into revealing sensitive information or granting access to systems.

Vulnerabilities can arise from various sources, including outdated software, weak passwords, inadequate access controls, and lack of employee awareness. By understanding these threats and vulnerabilities, organisations can tailor their cybersecurity awareness initiatives to address specific risks and empower their workforce to recognise and respond appropriately.

Developing a comprehensive cybersecurity awareness programme is essential for fostering a resilient workforce. Risk assessment is necessary. Conduct a thorough assessment of potential cyber risks and vulnerabilities specific to your organisation. Establish clear and concise cybersecurity policies and guidelines that outline expectations, responsibilities, and best practices. Implement regular training and educational initiatives to equip employees with the knowledge and skills needed to identify and mitigate cyber threats. Utilise various communication channels to reinforce cybersecurity awareness messages and promote a culture of vigilance. Develop and regularly test incident response plans to ensure effective and coordinated responses to cyber incidents. Regularly evaluate and update the cybersecurity awareness programme to address emerging threats, embedding continuous improvement and evolving best practices.

Security Awareness

By implementing a comprehensive cybersecurity awareness programme, organisations can empower their workforce to become an active line of defence against cyber threats, fostering a culture of vigilance and resilience.

Effective training and education are pivotal components of any successful cybersecurity awareness programme. By equipping employees with the knowledge and skills necessary to recognise and respond to cyber threats, organisations can enhance their workforce's resilience and strengthen their overall cybersecurity posture.

Training and education initiatives should be tailored to the specific needs and roles within the organisation. For example, employees in customer-facing roles may require training on identifying and handling phishing attempts, while IT professionals may benefit from advanced training on incident response and threat analysis.

To maximise engagement and retention, a variety of training methods should be employed, including in-person training with instructor-led sessions that provide hands-on learning experiences and opportunities for interactive discussions. Online courses are essential, with self-paced, web-based training modules that allow employees to learn at their convenience. Simulations and exercises help with realistic scenarios that test employees' ability to identify and respond to cyber threats in a controlled environment. Use regular

communication and awareness initiatives, such as emails, posters, and informative videos, to reinforce cybersecurity best practices.

By investing in comprehensive training and education programmes, organisations can empower their workforce to become a formidable line of defence against cyber threats, fostering a culture of resilience and vigilance.

Winning hearts and minds is vital. While technical knowledge and skills are essential, truly embedding cybersecurity awareness into an organisation's culture requires winning the hearts and minds of employees. Effective cybersecurity awareness initiatives should go beyond mere compliance and instead inspire a genuine understanding of the importance of cybersecurity and its direct impact on the organisation's success.

To win the hearts and minds of employees, organisations should clearly articulate the rationale behind cybersecurity measures and how they protect the organisation's interests, as well as the personal and professional well-being of employees. Tailor cybersecurity awareness messages and training to specific roles and responsibilities, demonstrating the direct relevance to employees' daily tasks and responsibilities. Encourage a sense of shared responsibility and accountability for cybersecurity, empowering employees to take an active role in safeguarding the organisation's digital assets. Recognise and celebrate individuals or teams who exemplify cybersecurity best practices, fostering a positive and encouraging environment. Ensure that leadership and management actively promote and embody cybersecurity best practices, setting the tone for the entire organisation.

By winning the hearts and minds of employees, organisations can cultivate a genuine commitment to cybersecurity awareness, fostering a resilient and vigilant workforce that proactively safeguards the organisation's digital assets.

Fostering a culture of cybersecurity awareness is a continuous journey that requires sustained effort and commitment from all levels of the organisation. A strong cybersecurity culture is one where cybersecurity best practices are ingrained in the daily operations and decision-making processes, becoming second nature to every employee.

To create a culture of cybersecurity awareness, organisations should ensure that senior leadership and management actively promote and prioritise cybersecurity awareness, setting the tone for the entire organisation. Integrate cybersecurity into processes. Incorporate cybersecurity considerations into various business processes, such as onboarding, performance evaluations, and project planning.

Encourage open and transparent communication about cybersecurity concerns, allowing employees to voice their perspectives and contribute to continuous improvement. Recognise and celebrate individuals or teams who exemplify cybersecurity best practices, fostering a positive and encouraging environment. Regularly assess the effectiveness of cybersecurity awareness initiatives and adapt strategies based on feedback and evolving threats.

By creating a culture of cybersecurity awareness, organisations can cultivate a resilient and vigilant workforce that proactively safeguards the organisation's digital assets, ensuring long-term success and business continuity in the digital age.

Evaluating effectiveness of cybersecurity awareness initiatives is crucial for ensuring their impact and continuous improvement. By measuring and analysing KPIs, organisations can gauge the success of their efforts and make data-driven decisions to optimise their cybersecurity awareness programmes.

Conduct regular phishing simulations to assess employees' ability to identify and report suspicious emails, tracking metrics such as click rates and reporting rates. Monitor employee participation and completion rates for cybersecurity awareness training programmes to ensure widespread engagement.

Track the number of reported incidents, as well as the time it takes to respond and mitigate threats, to evaluate the effectiveness of incident response processes. Conduct periodic risk assessments to measure the overall cybersecurity posture of the organisation and identify areas for improvement. Gather employee feedback through surveys or focus groups to assess the perceived effectiveness of cybersecurity awareness initiatives and identify areas for enhancement.

By continuously measuring and analysing these metrics, organisations can identify strengths and weaknesses in their cybersecurity awareness programmes, allowing them to make informed decisions and allocate resources effectively to strengthen workforce resilience.

Cybersecurity awareness is not merely a luxury but a necessity for organisations seeking to thrive and protect their critical assets. By fostering a culture of cybersecurity awareness and empowering a resilient workforce, organisations can effectively mitigate cyber risks, safeguard sensitive information, and ensure business continuity.

Through comprehensive training and education initiatives, open communication, and leadership commitment, organisations can cultivate a proactive and vigilant mindset among their employees. By winning the hearts and minds of the workforce, cybersecurity best practices become ingrained in daily operations, creating a formidable line of defence against cyber threats.

Measuring the effectiveness of cybersecurity awareness initiatives is crucial for continuous improvement and adapting to emerging threats. By leveraging data-driven insights and employee feedback, organisations can optimise their strategies and allocate resources effectively, ensuring a resilient and secure digital future.

Remember, cybersecurity is a shared responsibility, and every individual plays a vital role in protecting the organisation's digital assets. Embrace cybersecurity awareness as a core value, and empower your workforce to become the frontline warriors in the battle against cyber threats.

Notes

1 Boh, W., Constantinides, P., Padmanabhan, B., and Viswanathan, S., 2023. Building Digital Resilience against Major Shocks. *Mis Quarterly*, 47(1), pp.343–360.
2 Olaniyi, O.O., Ezeugwa, F.A., Okatta, C., Arigbabu, A.S., and Joeaneke, P., 2024. Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies. *Automation, and Employment Policies* (April 24).
3 Ajayi, F.A., and Udeh, C.A., 2024. Review of Workforce Upskilling Initiatives for Emerging Technologies in IT. *International Journal of Management & Entrepreneurship Research*, 6(4), pp.1119–1137.
4 Nguyen, M., Malik, A., Sharma, P., Kingshott, R., and Gugnani, R., 2024. High Involvement Work System and Organizational and Employee Resilience: Impact of Digitalisation in Crisis Situations. *Technological Forecasting and Social Change*, 205, p.123510.

7

CONTINGENCY PLANNING, DISASTER RECOVERY (DR), AND BACKUP-AS-A-SERVICE (BAAS)

Contingency Planning

In terms of contingency planning, *NIST Special Publication 800–34, Rev. 1,* provides instructions for federal information system contingency planning. Contingency planning involves interim measures to recover services after a disruption, such as relocating systems, using alternative equipment, or manual methods. This offers specific recommendations for three platform types: are client/server systems, telecommunications systems, and mainframe systems.

There is a clear process for developing and maintaining a contingency planning programme, integrated into the system development life cycle. Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary for an effective plan. Conduct the business impact analysis (BIA). The BIA identifies and prioritises critical systems and components. Identify preventive controls. Measures to reduce system disruptions can increase availability and reduce costs. Create contingency strategies. Recovery strategies ensure quick and effective system recovery. Develop an information system contingency plan. The plan should include detailed guidance for restoring a damaged system based on its security impact level. Ensure plan testing, training, and exercises. Testing validates recovery capabilities, training prepares personnel, and exercises identify gaps, improving plan effectiveness. Ensure plan maintenance. The plan should be updated regularly to stay current with system and organisational changes.

There are three sample formats for contingency plans based on low-, moderate-, or high-impact levels, as defined by FIPS Publication 199 (FIPS 199). This defines three levels of potential impact on organisations or

DOI: 10.4324/9781003604969-7

individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). Each format includes three phases: Activation/Notification, Recovery, and Reconstitution. The Activation/Notification phase involves activating the plan and notifying personnel. The Recovery phase outlines actions for restoring operations at an alternative site. The Reconstitution phase includes testing system functionality and preparing for future outages.

Information systems are vital to mission/business processes. It is critical that these systems operate effectively without excessive interruption.

Salami et al. (2024) argue *contingency planning* supports the need for quick recovery after a service disruption by establishing plans, procedures, and technical measures. Each system's plan is unique, addressing its specific confidentiality, integrity, and availability requirements.[1]

Information system contingency planning involves strategies to recover systems, operations, and data. It includes restoring systems with alternative equipment. Use manual processes for short-term disruptions. Recover operations at an alternative location for long-term disruptions. Implement controls based on the system's security impact level.

This guides those responsible for preparing and maintaining information system contingency plans (ISCPs). It discusses essential elements, processes, and considerations for various system platforms, providing examples to help develop ISCPs.

Purpose

This helps organisations understand ISCP development through practical guidelines. While it establishes a baseline, each organisation may have specific needs. The document explains the relationship between contingency planning, security, emergency management, organisational resiliency, and the system development life cycle (SDLC). It helps personnel evaluate systems to determine planning requirements and priorities. Requirements from FIPS 199 and NIST Special Publication 800–53 are integrated throughout. Considerations for impact levels and associated security controls are presented to assist in developing appropriate strategies. Although largely independent of specific hardware, operating systems, and applications, technical considerations for common platforms are addressed.

Scope

Guidelines for federal organisations are set out. This process discusses technologies supporting contingency capabilities, recognising the rapid development and obsolescence of products. The document describes practices to enhance contingency planning for client/server systems, telecommunications systems, and mainframe systems.

It outlines principles for various incidents affecting information system operations.

These range from minor incidents causing short-term disruptions to disasters affecting operations for extended periods. Since information systems vary, specific incident types and measures are not detailed here. Instead, a process is provided to identify planning needs for effective contingency plans.

This does not cover facility-level information system planning (disaster recovery plans) or organisational mission continuity (COOP plans) except where needed to restore systems. It also does not address continuity of mission/business processes, which depend on other resources. Recovery of mission-essential functions is covered by COOP or business continuity plans, described in Section 2.2. The ISCP may be coordinated with disaster recovery, COOP, or business continuity planning if a system is needed during these events.

Information system: An information system is a set of resources for collecting, processing, maintaining, using, sharing, or disposing of information. Components include mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include firewalls, sensors, switches, routers, gateways, wireless access points, and network appliances. Servers can include database servers, authentication servers, email and web servers, proxy servers, domain name servers, and network time servers. Components can be commercially off-the-shelf or custom-developed and deployed in land-based, sea-based, airborne, and/or space-based systems.

Information systems face disruptions, from mild (e.g., power outage) to severe (e.g., fire). Vulnerabilities can be reduced through management, operational, or technical controls, but not all risks can be eliminated. Contingency planning mitigates system and service unavailability by enhancing system availability.

We must consider how federal information system contingency planning fits into risk management, security, and emergency preparedness programmes. It also covers other emergency preparedness plans and their relationship to information system contingency planning. Finally, it explains how integrating contingency planning throughout the SDLC promotes system compatibility and cost-effective responses to disruptions.

Contingency planning and resilience: Organisations must withstand hazards and sustain missions through environmental changes, whether gradual or sudden. Building a resilient infrastructure minimises disruption impacts on essential functions.

Resilience is the ability to adapt and recover from environmental changes. It is an end-state where organisations continue essential functions during disruptions. Resilient organisations adapt to changes and risks affecting critical functions. Risk management, contingency, and continuity planning are security and emergency management activities that can be implemented holistically as part of a resiliency programme.

Effective contingency planning starts with a policy and a business impact analysis (BIA) for each system. This prioritises systems and processes based on FIPS 199 impact levels and develops recovery strategies. FIPS 199 examines three security objectives: confidentiality, integrity, and availability.

Confidentiality protects information access and disclosure. *Integrity* guards against improper modification or destruction. *Availability* ensures timely and reliable information access.

Impact levels for each objective are high, moderate, or low, as defined in FIPS 199.

The highest individual security objective impact levels determine the overall system security impact level.

Contingency planning addresses the availability impact level of information systems. High-impact systems should consider high-availability and redundancy options, such as fully redundant load-balanced systems, data mirroring, and off-site database replication. These options are costly and should be reserved for high-impact systems. Lower-impact systems can use less expensive options and tolerate longer downtimes.

Effective contingency planning includes early incorporation and ongoing maintenance of security controls. NIST SP 800–53, Rev. 3, identifies nine contingency planning (CP) security controls. Not all controls apply to all systems. FIPS 199 categorisation determines applicable controls. For instance, low-impact systems do not need alternative sites, while moderate-impact systems require only basic backup controls. FIPS 199 allows tailoring of CP controls in NIST SP 800–53 to appropriate baselines.

Several CP controls reference environmental controls from the NIST SP 800–53 Physical and Environmental Protection (PE) family. These controls pertain to the location housing the system, including hardware and technology assets. Section 3.3 of NIST SP 800–53 offers more on environmental controls.

Organisations can use compensating security controls to meet CP control intents. These controls must provide comparable protection and have justified use.

Finkenstadt et al. (2024) go beyond this to argue businesses are increasingly leveraging strategic foresight and scenario planning to prevent disruptions. Generative AI can be used to provide rapid, cost-effective, and comprehensive contingency planning. This AI-driven approach enhances decision-making and provides effective risk reduction.[2]

Disaster Recovery

The ability to maintain operations and minimise disruptions is critical for success. Unexpected events such as natural disasters, cyber attacks, or supply chain disruptions can have devastating consequences for organisations, leading to financial losses, reputational damage, and even the potential for business failure.

Noor (2024) argues this is where business continuity (BC) and disaster recovery (DR) planning come into play, serving as essential strategies for mitigating risks and ensuring resilience in the face of adversity. Noor provides guidance on the formation of the BC and DR plans and setting the recovery time objectives.[3]

Sehra and Singh (2024) argue that at the core of an effective disaster recovery plan lies the selection of reliable suppliers who can support your organisation's ability to recover quickly and efficiently.[4] Nanda et al. (2024) contend that these suppliers play a crucial role in providing the necessary resources, services, and expertise to maintain business continuity during times of crisis. By carefully evaluating and choosing the right suppliers, you can significantly enhance your organisation's preparedness and increase its chances of weathering the storm.[5]

Reliable suppliers are the backbone of a robust disaster recovery plan. They provide the vital resources, services, and expertise necessary to maintain business operations during and after a disruptive event. Without reliable suppliers, organisations may find themselves ill-equipped to respond effectively, leading to prolonged downtime, lost revenue, and potentially irreparable damage to their reputation.

Furthermore, reliable suppliers can offer invaluable guidance and support throughout the disaster recovery process. They possess the specialised knowledge and experience to navigate complex situations, ensuring that your organisation can quickly adapt and respond to evolving circumstances. By leveraging the expertise of reliable suppliers, you can minimise the impact of disruptions and accelerate the recovery process, ultimately safeguarding your business's continuity.

Selecting the right suppliers for your disaster recovery plan is a critical decision that requires careful consideration of various factors. Here are some key elements to evaluate:

Assessing the supplier's track record and reputation: When evaluating potential suppliers, it is essential to thoroughly assess their track record and reputation within the industry. Look for suppliers with a proven history of delivering reliable services and successfully supporting organisations during times of crisis. Review their past performance, customer testimonials, and industry recognition to gauge their ability to meet your organisation's needs.

Evaluating the supplier's financial stability and resources: A supplier's financial stability and available resources are crucial factors in ensuring their ability to support your organisation during a crisis. Conduct thorough due diligence to assess their financial health, including reviewing their financial statements, credit ratings, and overall financial position. Additionally, evaluate their resource capacity, including personnel, equipment, and infrastructure, to ensure they have the necessary capabilities to meet your requirements.

Analysing the supplier's disaster recovery capabilities and procedures: Reliable suppliers should have robust disaster recovery capabilities and well-

defined procedures in place. Evaluate their disaster recovery plans, testing protocols, and incident response strategies to ensure they align with your organisation's requirements. Assess their ability to maintain continuity of services, their redundancy measures, and their capacity to scale up operations during emergencies.

Reviewing the supplier's contractual terms and service level agreements: Carefully review the supplier's contractual terms and service level agreements (SLAs) to ensure they meet your organisation's needs and provide adequate protection. Pay close attention to clauses related to performance guarantees, liability limitations, and termination conditions. Ensure that the terms and SLAs align with your organisation's risk tolerance and business continuity objectives.

Conducting site visits and inspections: Whenever possible, conduct site visits and inspections of the supplier's facilities and operations. This firsthand assessment can provide valuable insights into their preparedness, security measures, and overall operational readiness. Observe their procedures, infrastructure, and personnel to gain a comprehensive understanding of their capabilities.

Building strong relationships with suppliers: Beyond the technical and operational aspects, building strong relationships with reliable suppliers is essential for effective disaster recovery planning. Fostering open communication, trust, and collaboration can significantly enhance the success of your partnership.

Engage in regular meetings and discussions to align expectations, share updates, and address any potential concerns. Encourage transparency and open dialogue to foster a sense of trust and mutual understanding. Collaborative problem-solving and joint planning exercises can further strengthen the relationship and ensure a seamless response during times of crisis.

Creating a supplier management plan is crucial for ongoing monitoring and evaluation. To maintain the reliability and effectiveness of your suppliers, it is crucial to implement a comprehensive supplier management plan. This plan should outline processes for ongoing monitoring, evaluation, and continuous improvement.

Establish key performance indicators (KPIs) and metrics to measure the supplier's performance against agreed-upon service levels. Regularly review and analyse these metrics to identify areas for improvement or potential risks. Conduct periodic audits and assessments to ensure compliance with industry standards, regulatory requirements, and your organisation's policies.

Additionally, maintain open lines of communication with your suppliers to address any emerging challenges or changes in their operations or capabilities. Regularly review and update your supplier management plan to adapt to evolving business needs and industry trends.

In the ever-changing business landscape, where disruptions can strike at any moment, ensuring business continuity is paramount. By carefully

selecting and partnering with reliable suppliers, you can significantly enhance your organisation's ability to navigate through crises and maintain operational resilience.

Remember, choosing the right suppliers is not a one-time task; it requires ongoing monitoring, evaluation, and collaboration. By fostering strong relationships, implementing robust supplier management practices, and staying vigilant in your assessments, you can ensure that your disaster recovery plan remains effective and adaptable.

Backup-as-a-Service (BaaS)

In the ever-evolving digital landscape, data has become the lifeblood of modern businesses. As organisations generate and store vast amounts of critical information, ensuring its safety and availability has become paramount. Enter Backup-as-a-Service (BaaS), a cloud-based solution that revolutionises the way we approach data protection and disaster recovery.

BaaS is a comprehensive service that offloads the complexities of backup and recovery processes to a third-party provider. By leveraging the power of the cloud, BaaS enables businesses to securely store and manage their data off-site, providing a robust safeguard against potential disasters or data loss incidents.

Executives must explore the intricacies of BaaS, its benefits, and how it can empower organisations to achieve seamless disaster recovery, ensuring business continuity and data integrity.

In today's fast-paced business environment, data loss can have devastating consequences. Whether it's a natural disaster, cyber attack, hardware failure, or human error, the impact of data loss can be devastating. Downtime, lost productivity, and the potential for reputational damage can severely hinder an organisation's operations and bottom line.

Disaster recovery strategies are crucial for mitigating these risks and ensuring business continuity. Traditional on-premises backup solutions, while effective, often require substantial investments in hardware, software, and dedicated IT resources. Additionally, they can be vulnerable to localised disasters, leaving organisations exposed to potential data loss.

BaaS addresses these challenges by providing a robust, scalable, and cost-effective solution for data protection and disaster recovery.

Exploring the benefits of BaaS is an important consideration for seamless disaster recovery. Implementing BaaS offers numerous advantages that empower organisations to achieve seamless disaster recovery and maintain business continuity. By storing data in the cloud, BaaS ensures that your critical information is securely housed in a remote location, protecting it from local disasters or site-specific incidents. Cloud-based solutions are inherently scalable, allowing you to easily adjust your backup and storage capacity as your data needs evolve, without the need for expensive hardware

upgrades. BaaS providers typically offer automated backup schedules, ensuring that your data is regularly and consistently backed up, minimising the risk of data loss due to human error or oversight. In the event of a disaster, BaaS enables quick and efficient data recovery, minimising downtime and ensuring business continuity. By eliminating the need for on-premises backup infrastructure and dedicated IT resources, BaaS can significantly reduce the overall costs associated with data protection and disaster recovery. Reputable BaaS providers adhere to strict security and compliance standards, ensuring that your data is encrypted, securely transmitted, and stored in accordance with industry regulations.

Key features of BaaS solutions: While BaaS offerings may vary across providers, most solutions share a set of core features and functionalities designed to streamline data protection and disaster recovery processes.

At the heart of BaaS lies the ability to perform reliable and efficient backups of your data, as well as restore it when needed. This includes support for various backup types (full, incremental, differential) and customisable backup schedules. To optimise storage and bandwidth usage, BaaS solutions often employ data deduplication and compression techniques, reducing the amount of data that needs to be transferred and stored. Ensuring the security and privacy of your data is paramount. BaaS providers typically offer robust encryption methods and secure data transfer protocols to protect your information during transit and at rest.

A user-friendly, web-based console allows you to monitor and manage your backups, configure settings, and initiate recovery processes from a single, centralised location. Comprehensive reporting and alerting features keep you informed about backup status, potential issues, and any actions required, ensuring proactive monitoring and timely intervention.

Advanced BaaS solutions may include disaster recovery orchestration capabilities, enabling automated failover and failback processes to minimise downtime and ensure business continuity in the event of a disaster.

Choosing the right BaaS provider for your business is one of your most important decisions. With the growing popularity of BaaS, the market is saturated with numerous providers offering varying levels of services and capabilities. Selecting the right BaaS provider is crucial to ensure that your data protection and disaster recovery needs are met effectively.

Evaluate the provider's track record, uptime guarantees, and reputation for delivering consistent and reliable services. Assess the provider's security measures, data encryption methods, and compliance with relevant industry regulations and standards. Ensure that the provider can accommodate your current and future data growth, while maintaining optimal performance levels.

Review the provider's SLAs carefully, paying attention to backup and recovery time objectives, data retention policies, and support responsiveness. Consider the provider's compatibility with your existing IT infrastructure,

applications, and backup tools to ensure seamless integration and minimise disruptions. Evaluate the provider's pricing structure, including any additional fees for features or services you may require, and ensure it aligns with your budget and long-term cost projections.

Implementing BaaS has a huge bearing on the effectiveness of data protection and recovery. Adopting BaaS is a strategic decision that requires careful planning and execution. Conduct a thorough assessment of your organisation's data protection requirements, including the types of data, retention policies, recovery point objectives (RPOs), and recovery time objectives (RTOs).

Based on your assessment, develop a comprehensive backup and recovery strategy that aligns with your business objectives, compliance requirements, and disaster recovery goals. Choose a BaaS provider that meets your specific needs and configure the solution according to your backup and recovery strategy, including backup schedules, retention policies, and recovery processes.

Ensure seamless integration between your BaaS solution and your existing IT infrastructure, applications, and backup tools to minimise disruptions and streamline data protection processes. Conduct thorough testing and validation of your BaaS implementation, including backup and recovery scenarios, to ensure that your data protection and disaster recovery processes are functioning as expected.

Provide comprehensive training and education to your IT staff and end users on the proper usage and management of your BaaS solution, fostering a culture of data protection and disaster recovery preparedness. Continuously monitor and optimise your BaaS implementation, leveraging reporting and alerting features to identify potential issues, track performance, and make necessary adjustments to ensure optimal data protection and recovery capabilities.

Best practices are crucial in ensuring BaaS delivers on disaster recovery. To maximise the effectiveness of your BaaS solution and ensure seamless disaster recovery, it's essential to follow industry best practices.

Create a detailed disaster recovery plan that outlines the roles, responsibilities, and step-by-step procedures to be followed in the event of a disaster, ensuring a coordinated and efficient response. Conduct periodic testing and validation of your disaster recovery processes, including failover and failback scenarios, to identify and address any potential issues or gaps in your plan. Keep detailed documentation of your BaaS configuration, backup schedules, recovery processes, and any relevant system or application dependencies, ensuring smooth and efficient recovery operations. Establish and enforce role-based access controls to ensure that only authorised personnel can access and manage your BaaS solution, enhancing data security and reducing the risk of accidental or malicious data loss. Explore and implement automation and orchestration capabilities offered by your BaaS provider to streamline disaster recovery processes, minimising manual intervention and

reducing the risk of human error. Continuously review and update your backup and disaster recovery strategy to align with changing business requirements, evolving threats, and emerging best practices, ensuring your BaaS solution remains effective and relevant.

Case Studies

*Case studie*s of successful implementation of BaaS help embed the importance of seamless disaster recovery. To illustrate the real-world impact and benefits of BaaS, let's explore some case studies of organisations that have successfully implemented BaaS solutions for seamless disaster recovery:

Case Study 1: Global Automotive Manufacturing Company[6]

A multinational manufacturing company with operations spanning multiple countries faced significant challenges in ensuring data protection and disaster recovery across its distributed infrastructure. By adopting a comprehensive BaaS solution, the company was able to centralise and streamline its backup and recovery processes, reducing data loss risks and minimising downtime in the event of localised disasters.

The BaaS provider's robust encryption and secure data transfer capabilities ensured compliance with stringent industry regulations, while the scalable and flexible architecture allowed the company to seamlessly accommodate its growing data volumes without the need for costly infrastructure upgrades.

Case Study 2: Healthcare: Allina Health[7]

In the healthcare industry, data security and availability are paramount. A large healthcare provider recognised the need for a robust and reliable disaster recovery solution to safeguard patient records and ensure business continuity in the face of potential disasters.

By implementing a BaaS solution, the healthcare provider was able to securely store and manage its critical data off-site, leveraging the provider's state-of-the-art data centres and redundant infrastructure. The automated backup schedules and rapid recovery capabilities ensured minimal disruption to patient care and operational efficiency, even in the event of a major incident.

Case Study 3: Financial Services Firm: Arvest Bank[8]

For a financial services firm, data loss can have severe consequences, including regulatory fines, reputational damage, and loss of customer trust. To mitigate these risks, the firm adopted a BaaS solution that offered comprehensive backup and disaster recovery capabilities, as well as advanced features such as disaster recovery orchestration.

By automating failover and failback processes, the firm was able to minimise downtime and ensure seamless business continuity during critical events. The BaaS provider's robust reporting and alerting features enabled proactive monitoring and timely intervention, further enhancing the firm's disaster recovery readiness.

Advancements in Recovery

The landscape of BaaS and disaster recovery is constantly evolving, driven by technological advancements and changing business needs. Artificial intelligence (AI) and machine learning (ML) technologies will play a significant role in enhancing BaaS solutions, enabling intelligent data management, predictive analytics, and automated decision-making for optimised backup and recovery processes. With the rise of edge computing and the Internet of Things (IoT), BaaS providers will need to adapt their solutions to support distributed data environments, ensuring seamless backup and recovery for edge devices and IoT deployments.

As organisations embrace hybrid and multi-cloud architectures, BaaS solutions will need to evolve to support data protection and disaster recovery across multiple cloud platforms and on-premises environments. With the increasing threat of cyber attacks and ransomware, BaaS providers will need to enhance their security measures and offer advanced capabilities for data immutability, air-gapped backups, and ransomware recovery.

As data privacy and compliance regulations continue to evolve, BaaS providers will need to stay ahead of the curve, ensuring their solutions adhere to the latest industry standards and regulatory requirements. The adoption of containerisation and microservices architectures will drive the need for BaaS solutions that can seamlessly integrate with these modern application delivery models, providing granular backup and recovery capabilities.

In the ever-changing digital landscape, data protection and disaster recovery are no longer optional luxuries but essential components of a robust business continuity strategy. BaaS emerges as a powerful solution, offering organisations a scalable, cost-effective, and secure way to safeguard their critical data and ensure seamless recovery in the face of disasters.

By leveraging the power of the cloud, BaaS eliminates the need for costly on-premises backup infrastructure, while providing a comprehensive set of features and functionalities to streamline data protection and recovery processes. From automated backups and secure data transfer to rapid recovery and centralised management, BaaS empowers organisations to achieve seamless disaster recovery and maintain business continuity, even in the most challenging circumstances.

As we navigate the ever-evolving digital landscape, embracing BaaS as part of a comprehensive disaster recovery strategy becomes increasingly crucial. By partnering with the right BaaS provider and following industry best

practices, organisations can unlock the full potential of this transformative technology, ensuring the safety and availability of their data, and ultimately, the resilience of their business operations.

Notes

1 Salami, A.A., Igwenagu, U.T.I., Mesode, C.E., Olaniyi, O.O., and Oladoyinbo, O. B., 2024. Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security. *Journal of Engineering Research and Reports*, 26(5), pp.304–323.
2 Finkenstadt, D.J., Sotiriadis, J., Guinto, P., and Eapen, T., 2024. Contingency Scenario Planning Using Generative AI. *California Management Review Insights*. (January 22, 2024). https://cmr.berkeley.edu/2024/01/contingency-scenario-planning-using-generative-ai.
3 Noor, B., 2024. Incident Response and Disaster Recovery: Business Continuity Planning for Cloud-based Financial Services. https://www.researchgate.net/publication/381408881_Incident_Response_and_Disaster_Recovery_Business_continuity_planning_for_cloud-based_financial_services.
4 Sehra, S.K., and Singh, A., 2024. Analysis of Data Backup and Recovery Strategies in the Cloud. In *Applied Data Science and Smart Systems* (pp.409–415). CRC Press.
5 Nanda, A.K., Sharma, A., Augustine, P.J., Cyril, B.R., Kiran, V., and Sampath, B., 2024. Securing Cloud Infrastructure in IaaS and PaaS Environments. In *Improving Security, Privacy, and Trust in Cloud Computing* (pp.1–33). IGI Global.
6 https://www.commvault.com/resources/case-studies/a-renowned-auto-manufacturer-ensures-cyber-resilience.
7 https://www.commvault.com/resources/case-studies/case-study-allina-health.
8 https://www.commvault.com/resources/case-studies/case-study-arvest-bank.

8

SUPPLY CHAIN MANAGEMENT AND THE CYBER RISK LANDSCAPE

Cyber Risk Landscape and NIST CSF

The process of managing risks within the supply chain network is complex and requires ongoing monitoring and control, hence cybersecurity is a paramount concern.[1]

It is increasingly the case that direct and indirect cyber risks are so great that constant vigilance is required. Guidance is needed for companies so they can clearly establish a supplier risk management programme involving new and existing suppliers, and how to sustain those activities operationally.[2]

There are limitations of cybersecurity skills in small to medium-sized organisations, including enterprise leadership and non-IT professionals who are responsible for supplier relationships.[3]

To meet this need, guidance is provided in this chapter for enterprise leadership and IT leadership. The next chapter provides guidance for non-IT professionals.

Cybersecurity within the supply chain can be met by following the National Institute of Standards and Technology's Cyber Security Framework ("CSF") supply chain security practices as part of version 2.0 of the framework.[4] Other frameworks offer a similar approach. Also see the Centre for Internet Security 18 Critical Controls.[5] A framework for continuous control verification is MITRE ATT&CK™.[6]

Advice is there to support attributes of supplier risk management programmes; e.g., policies and procedures, roles and responsibilities, and establishing overall governance. Establish and sustain the supplier risk management programme including inventory of suppliers, risk assessment, and risk treatment. Cybersecurity requirements, language for contracts, and supporting the contract management process must be considered. Guidelines

DOI: 10.4324/9781003604969-8

for assurance that suppliers are adhering to their contract commitments is important. Planning and testing response to and recovery from supplier cybersecurity incidents is crucial.

The NIST CSF and other security control frameworks can offer a proactive approach for leveraging acquirer and supplier relationships to reduce cybersecurity risks. NIST documentation has been relied upon for this guidance and is extensively referenced throughout.[7]

Cybersecurity Supply Chain Risk Management (C-SCRM)

Technologies rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem. Cybersecurity Supply Chain Risk Management (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. C-SCRM practitioners identify, assess, and mitigate cybersecurity risks throughout the supply chain at all levels of their organisations associated with information and communications technology (ICT) products and services. Potential risks include malicious functionality, counterfeit devices, or vulnerabilities derived from poor manufacturing and development practices within the supply chain.

The supply chain ecosystem is composed of public and private sector entities – including acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers – that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilise or manage technology products and services.

Cybersecurity risks and threats evolve at an unprecedented rate, resulting in susceptibility to cyber exploitation. This exploitation often targets internet-connected devices, long-lived legacy technology, cloud applications, third-party services, and the free flow of suppliers.[8]

Emerging technologies can help, such as use of predictive analytics, as these targets can be exploited through numerous paths (vectors), ranging from a supplier servicing an asset, poor manufacturer security design and ongoing patching, installed networks, loaner/rental devices, manufacturer default passwords, supplier applications interfaced into systems, etc.[9]

Comprehensive threat analysis is necessary as the combination of exploits and exploitable targets is growing daily, allowing anyone from amateur hackers to malicious nation-state actors an opportunity to breach customer data, disrupt operations, and/or cause customer harm.[10]

Properly managing cyber risk within the supply chain requires a proactive strategy to protect customer information and sensitive data against an ever-increasing risk from bad actors outside, and sometimes within, the system.

Supply chain cybersecurity risk management also serves as a strategy to enable collaboration as well as supporting and increasing preparedness and business continuity planning and countermeasures.[11]

All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem. C-SCRM is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. Effective C-SCRM requires stakeholders across the enterprise to actively collaborate, communicate, and take actions to secure favourable C-SCRM outcomes.

A Systematic Process

This is a brief overview of C-SCRM and how it relates to the Cybersecurity Framework (CSF). Organisations implementing C-SCRM capabilities should not rely solely on this and should consult the additional documents referenced within.

Improve C-SCRM processes: The CSF can help an organisation become a smart acquirer and supplier of technology products and services. This approach focuses on ways the CSF can help. Use the CSF's GV.SC Category to establish and operate a C-SCRM capability. Define and communicate supplier requirements using the CSF.

The *supply chain ecosystem* is composed of public and private sector entities including acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilise or manage technology products and services.

Consider a laptop with hardware subcomponents (like the graphics processor, random-access memory, or network interface card) sourced from different countries and third-party manufacturers, and subject to distinct supply chain interactions. That laptop also contains software (and firmware) developed by different companies and people. How do we manage risk for complex ICT devices with multiple components?

The supply chain ecosystem includes other third parties such as business partners and various data and digital service providers. Practices can be applied to manage cybersecurity risks from such relationships as well.

Establishing C-SCRM Capability

The CSF has a Category within its Govern Function dedicated to C-SCRM: the Cybersecurity Supply Chain Risk Management (GV.SC) Category.[12] GV.SC contains the key outcomes that every organisation should achieve through its C-SCRM capability. Additionally, many of the subcategories

within the remainder of the CSF can be used to identify and communicate C-SCRM-related requirements internally for organisations and for their vendors.

Perform these activities to establish your organisation's C-SCRM capability:

> Task 1: Create a C-SCRM strategy, objectives, policies, and processes. [GV.SC-01]
> Task 2: Identify your organisation's technology suppliers and determine how critical each one is to your organisation. [GV.SC-04]
> Task 3: Establish C-SCRM roles and requirements and communicate them within and outside your organisation. This includes identifying C-SCRM roles and responsibilities [GV.SC02] and C-SCRM requirements. [GV.SC-05]

Consolidate activities between your C-SCRM capability and other internal capabilities:

- Integrate C-SCRM into cybersecurity and enterprise risk management, risk assessment, and improvement processes, and monitor the performance of C-SCRM practices throughout the technology lifecycle. [GV.SC-03, GV.SC-09] See the *Enterprise Risk Management Quick-Start Guide* for more information on C-SCRM integration.[13]
- Include your relevant suppliers in cybersecurity incident planning, response, and recovery activities. [GV.SC-08] See NIST's *Computer Security Incident Handling Guide* for more information on key practices for cybersecurity incidents.[14]

Top tips for Task 1: Create a C-SCRM Strategy, Objectives, Policies, and Processes

□ Establish a C-SCRM strategy that lays out the objectives of the capability.
□ Develop a C-SCRM plan (with milestones) and C-SCRM policies and procedures that guide implementation and improvement of the plan and the capability; socialise those policies and procedures with organisational stakeholders.
□ Develop and implement C-SCRM processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organisational stakeholders.
□ Establish a cross-organisational mechanism that ensures alignment between functions that contribute to C-SCRM management, such as cybersecurity, IT, legal, HR, engineering, etc.

Top tips for Task 2: Identify your Organisation's Technology Suppliers and Determine how Critical each one is to your Organisation

□ Develop criteria for supplier criticality based on, for example, the importance of the supplier's products or services to the organisation's business, sensitivity of data processed or stored by the supplier, and degree of access to the organisation's systems.
□ Prioritise suppliers into criticality levels based on the criteria. See NIST IR 8179, Criticality Analysis Process Model: Prioritising Systems and Components for more information on a structured method for prioritisation.[15]
□ Keep a record of all suppliers, prioritised based on the criticality criteria.

Top tips for Task 3: Establish C-SCRM Roles and Requirements and Communicate them Within and Outside your Organisation

C-SCRM Roles and Responsibilities

□ Identify one or more specific roles or positions that will be responsible and accountable for planning, resourcing, and executing C-SCRM activities.
□ Document C-SCRM roles and responsibilities in policy.
□ Create responsibility matrices (e.g., RACI charts) to document who will be responsible, accountable, consulted, and informed for C-SCRM activities and how those teams and individuals will be consulted and informed.
□ Include C-SCRM responsibilities and performance requirements in personnel descriptions to ensure clarity and improve accountability.
□ Document performance goals for personnel with C-SCRM responsibilities, and periodically measure them to demonstrate and improve performance.
□ Develop roles and responsibilities for suppliers, customers, and business partners to address shared responsibilities for applicable cybersecurity risks and integrate them into organisational policies and applicable third-party agreements.
□ Internally communicate C-SCRM roles and responsibilities for suppliers.
□ Establish rules and protocols for information sharing and reporting processes between the organisation and its suppliers.

C-SCRM Requirements

□ Establish security requirements for suppliers, products, and services commensurate with their criticality and potential impact if compromised.
□ Include all cybersecurity and supply chain requirements that suppliers must follow and how compliance with the requirements may be verified in default contractual language.

□ Define the rules and protocols for information sharing between the organisation and its suppliers and sub-tier suppliers in contracts.
□ Include security requirements in contracts based on their criticality and potential impact if compromised.
□ Define security requirements in SLAs for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle.
□ Specify in contracts the rights and responsibilities of the organisation, its suppliers, and their supply chains with respect to potential cybersecurity risks. Contractually require suppliers to do the following:
□ Disclose cybersecurity features, functions, and vulnerabilities of their products and services for the life of the product or the term of service.
□ Provide and maintain a current component inventory (e.g., software or hardware bill of materials) for critical products.
□ Vet their employees and guard against insider threats.
□ Provide evidence of performing acceptable security practices through, for example, self-attestation, conformance to known standards, certifications, or inspections.

Developing supplier requirements: An organisation should specify requirements for technology suppliers. Robustness of these requirements should correspond to supplier criticality.

Organisations can use two different methods for specifying supplier requirements:

1 Use CSF Categories and Subcategories

Not all Categories and Subcategories will apply to all suppliers. You can pick and choose requirements that fit your mission or business supplier criticality level. Select requirements for suppliers based on their criticality and your mission or business. To do that, review the list of CSF Categories and Subcategories, and determine which ones will be applicable to suppliers within each of the criticality levels, based on the risk appetite for each supplier criticality level.

When considering individual supplier agreements, determine if additional supplier requirements are needed based on existing criticality criteria, such as your mission or business, data type being processed, or digital product or service being provided.

2 Create CSF Target Profiles for Each Supplier Criticality Level

Express supplier requirements for each supplier criticality level.

Examples of CSF Categories and Subcategories that are Likely to Include Requirements for Suppliers

Govern

- *Organisational Context:* Legal, regulatory, and contractual requirements regarding cybersecurity including privacy and civil liberties obligations are understood and managed. [GV.OC-03]
- *Roles, Responsibilities, and Authorities:* Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced. [GV.RR02]
- *Cybersecurity Supply Chain Risk Management:* Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organisational stakeholders. [GV.SC]

Protect

- *Identity Management, Authentication, and Access Control:* Identities and credentials for authorised users, services, and hardware are managed by the organisation. [PR.AA-01]
- *Awareness and Training:* Individuals in specialised roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind. [PR.AT-02]

Identify

- *Risk Assessment:* The authenticity and integrity of hardware and software are assessed prior to acquisition and use. [ID.RA-09] Critical suppliers are assessed prior to acquisition. [ID.RA-10]
- *Improvement:* Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties. [ID.IM-02]

Detect

- *Continuous Monitoring:* Personnel activity and technology usage are monitored to find potentially adverse events. [DE.CM-03]

Respond

- *Incident Management:* Incidents are escalated or elevated as needed. [RS.MA-04]
- *Incident Response Reporting and Communication:* Internal and external stakeholders are notified of incidents. [RS.CO-02]

Recover

- *Incident Recovery Plan Execution:* The integrity of backups and other restoration assets is verified before using them for restoration. [RC.RP-03]
- *Incident Recovery Communication:* Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders. [RC.CO-03]

Create Target Profiles to Communicate Supplier Requirements by Supplier Criticality Level

Follow these steps to create Target Profiles for communicating C-SCRM requirements to your suppliers:

1. *Scope the Target Profile.* Decide which of your supplier criticality levels it will apply to, and determine any other restrictions to be placed on the Profile's scope, such as suppliers of a particular type of product or service only. You can create as many Target Profiles as you need to specify the requirements for all of your suppliers.
2. *Select the CSF Categories to include.* Identify which CSF Categories and Subcategories correspond to your requirements, and only include those Categories and Subcategories in the Target Profile.
3. *Determine what types of information to include in your Target Profile.* Target Profiles are flexible and can contain whatever types of information you want to communicate to your suppliers. The notional Profile excerpt below captures each selected Category's and Subcategory's relative priority, the internal practices that the supplier must follow, and references to additional sources of information on achieving the Category and Subcategory.
4. *Fill in the columns, and share the Target Profile.* Once the contents of the Target Profile have been internally reviewed and finalised, it can be shared with your suppliers as your set of C-SCRM requirements for them.

Additional Resources

Resources for Creating Target Profiles

- *Quick-Start Guide for Creating and Using Organisational Profiles* (including Target Profiles).[16]
- *A Guide to Creating CSF 2.0 Community Profiles* (Community Profiles have much in common with creating Target Profiles for numerous suppliers to follow).[17]
- *Quick-Start Guide for Using the CSF Tiers* (to help inform creation of Target Profiles).[18]

TABLE 8.1 Sample Target Profiles

Selected CSF Outcomes	*Target Priority*	*Target Internal Practices*	*Selected Informative References*
PR.PS, The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organisation's risk strategy to protect their confidentiality, integrity, and availability	High	1. Configure platforms to allow the installation of organisation-approved software only. 2. Verify the source of new software and the software's integrity before installing it. 3. Configure platforms to use only approved DNS services that block access to known malicious domains. 4. ….	• NIST SP 800–161r1, control SI-3 • ISO 27002:2022, control 8.7 • …
…			

- *Enterprise Risk Management Quick-Start Guide.*[19]
- *Informative Reference Mapping Quick-Start Guide* (Informative References for a Target Profile).[20]

To make this effective in practice follow the following steps:

- Review all NIST CSF 2.0 Categories and Subcategories.
- Develop C-SCRM strategy, objectives, policies, and processes.
- Identify your organisation's technology suppliers.
- Determine how critical each technology supplier is to your organisation and prioritise your suppliers.
- Establish C-SCRM roles and requirements.
- Communicate C-SCRM roles and requirements within and outside your organisation, including to technology suppliers.

NIST resources are shared to support you in establishing and operating your C-SCRM capability:

- *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (NIST IR 8276) summarises practices foundational to an effective C-SCRM capability.[21]
- *Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations* (NIST SP 800–161 Revision 1) guides organisations in identifying, assessing, and responding to supply chain risks at all levels.[22]

It is flexible and builds on an organisation's existing cybersecurity practices. Also, Appendix A identifies the C-SCRM-related controls from NIST SP 80053r5 and augments those controls with additional supplemental guidance, as well as providing new controls as appropriate.[23]

- *Criticality Analysis Process Model: Prioritising Systems and Components* (NIST IR 8179) provides information on prioritising suppliers by criticality levels.[24]
- The Software and Supply Chain Assurance Forum provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding C-SCRM, supply chain risks, effective practices and response strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.[25]
- NIST's C-SCRM Program website contains links to additional resources.[26]

Notes

1 Adenekan, O.A., Ezeigweneme, C., and Chukwurah, E.G., 2024. Strategies for Protecting IT Supply Chains against Cybersecurity Threats. *International Journal of Management & Entrepreneurship Research*, 6(5), pp.1598–1606.
2 Sawik, T., 2024. Supply Chain Cybersecurity: Direct and Indirect Cyber Risks. In *Stochastic Programming in Supply Chain Risk Management: Resilience, Viability, and Cybersecurity* (pp. 293–322). Cham: Springer Nature Switzerland.
3 Herburger, M., Wieland, A., and Hochstrasser, C., 2024. Building Supply Chain Resilience to Cyber Risks: A Dynamic Capabilities Perspective. *Supply Chain Management: An International Journal*, 29(7), pp.28–50.
4 https://www.nist.gov/cyberframework.
5 https://www.cisecurity.org/controls/cis-controls-list.
6 https://attack.mitre.org.
7 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1305.ipd.pdf.
8 Ibiyemi, M.O., and Olutimehin, D.O., 2024. Cybersecurity in Supply Chains: Addressing Emerging Threats with Strategic Measures. *International Journal of Management & Entrepreneurship Research*, 6(6).
9 Ananthi, P., Devi, K.N., Gopinath, D., and Karthikeyan, C., 2024, March. Enhancing Cybersecurity in the Supply Chain through Predictive Analytics for Cyber Threats. In *2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1–5). IEEE.
10 Kumar, M., Epiphaniou, G., and Maple, C., 2024. Comprehensive Threat Analysis in Additive Manufacturing Supply Chain: A Hybrid Qualitative and Quantitative Risk Assessment Framework. *Production Engineering*, pp.1–19.
11 Friday, D., Melnyk, S.A., Altman, M., Harrison, N., and Ryan, S., 2024. An Inductive Analysis of Collaborative Cybersecurity Management Capabilities, Relational Antecedents and Supply Chain Cybersecurity Parameters. *International Journal of Physical Distribution & Logistics Management*. https://www.researchgate.net/publication/380824161_An_inductive_analysis_of_collaborative_cybersecurity_management_capabilities_relational_antecedents_and_supply_chain_cybersecurity_parameters.

12 https://csf.tools/reference/nist-cybersecurity-framework/v2-0/gv/gv-sc.
13 https://doi.org/10.6028/NIST.SP.1303.ipd.
14 https://doi.org/10.6028/NIST.SP.800-61r2.
15 https://doi.org/10.6028/NIST.IR.8179.
16 https://doi.org/10.6028/NIST.SP.1301.
17 https://doi.org/10.6028/NIST.CSWP.32.ipd.
18 https://doi.org/10.6028/NIST.SP.1302.ipd.
19 https://doi.org/10.6028/NIST.SP.1303.ipd.
20 https://doi.org/10.6028/NIST.SP.1309.ipd.
21 https://csrc.nist.gov/pubs/ir/8276/final.
22 https://doi.org/10.6028/NIST.SP.800-161r1.
23 https://doi.org/10.6028/NIST.SP.800-53r5.
24 https://doi.org/10.6028/NIST.IR.8179.
25 https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca.
26 https://scrm.nist.gov.

9

SUPPLIER RISK MANAGEMENT SETUP (ADVICE FOR SMES)

SME Supplier Risk Management

SMEs must implement robust strategies to deal with supply chain risk and improve resilience or they will not survive. This is in the nature of having limited internal resources. SMEs are particularly at risk of supply chain disruption, which can prove catastrophic.[1]

Guidance is sorely needed for SMEs and non-IT professionals to help improve supply chain cybersecurity as there are major shortcomings in existing approaches.[2]

This chapter provides advice specifically for SMEs. The previous chapter provided guidance for enterprise and IT leadership. This chapter provides guidance particularly useful for non-IT professionals. This is general advice and covers the key issues they will need to consider. It broadly covers components of a supplier risk management programme and the foundational groundwork required to manage supplier cybersecurity risk.

1) Define supplier risk: Define risks to your organisation. Key risks that should be considered depend on the *mission of your organisation* and the nature of its relationships with suppliers.[3] Cyber risk must be considered in the context of supplier risk, to include other drivers of enterprise business risk. Assess cyber risk and its impact across risk areas including but not limited to operational risk impacting day-to-day operations, safety risk impacting customers, employees, contractors, etc. Competitive risk impacts the ability to achieve goals (may include intellectual property, trade secrets, go to market, etc.). Quality risk impacts products services and business practices (may include product quality/sabotage/illicit re-use or re-sale, product service integrity, etc.). Reputation risk impacts damage to or loss of customer, business partner, or public confidence or perceived image.

DOI: 10.4324/9781003604969-9

Compliance risk impacts losses and legal penalties for failure to comply with laws and regulations. Secondary risk involves the transfer of risk to business partners (may include avoiding, reducing, or transferring risk). Geopolitical risk involves the impacts of political events or instability, trade barriers, taxes, or economies.

2) Define roles and responsibilities: Having identified the key organisational risks, assign an executive sponsor to own the supplier cyber risk management programme and establish programme governance.

This role should provide governance, including:

- Set the agenda.
- Align vision, goals, milestones, and metrics.
- Communicate risk appetite.
- Direct resources to support goals.
- Remove obstacles.
- Receive updates.

It is crucial at this stage that the executive team should have accountability for business risks, and authority to prioritise, influence, and obtain organisational resources to address those risks. High-level executive leadership is essential.[4]

One method for structuring ownership and accountability within the enterprise is use of the "RACI" model – Responsible, Accountable, Consulted, Informed – which lays out roles and responsibilities for any activity or group of activities.[5]

Supply chain cybersecurity is a business risk, and not a technology risk.

3) Define supplier scope: Define the term "supplier" as it relates to your organisation. This may include any individual or entity that provides any type of service and/or product to the organisation. The word supplier may commonly refer to: supplier, vendor, service provider, consultant, external partner, third party, or business partner, etc.

Based on your definition, you will need to gather and document the entire inventory of your suppliers. You may need to consider multiple sources to gather this information – e.g., accounts payable, contracting, expense processes, etc. Knowing the size and scope before starting is important in order to prioritise resources and set realistic expectations on the size and complexity of the task.

4) Establish policies and procedures: Having defined the scope, you will need to define or update the policies supporting the supplier risk management programme at your organisation to formalise the organisation's supplier risk management approach.

Define policies: The organisation's policies should drive the definition of supplier risk management metrics and reporting requirements in support of the programme goals. Metrics should articulate the supplier risk posture of the supplier risk programme in the context of the organisation's key business

risks (established above). The metrics and targets should therefore be agreed with the sponsor and should be biased toward driving risk posture improvements and showing progress over time, rather than point-in-time or activity-based measures.

Metrics can be very useful. Distribution of suppliers by risk tier or by most relevant business risk impact are useful metrics. Number of suppliers not covered by a current security assessment is important for monitoring. Number of suppliers with known open risks and severity of those risks is useful for monitoring improvement. Contract consistency (inclusion of security requirements), volume of supplier assessments planned, in-process and up-coming are important metrics. Regulatory issues due to cyber concerns, externally reported incidents, and supplier audit findings are more overt forms of metrics.

Define supplier tiering: Tiering suppliers can be used to drive differences in both the assessment approach and other requirements – e.g., frequency of periodic re-assessments. Prioritisation is important to make the task manageable. A good approach is to establish tiers of suppliers which include dimensions such as spend, criticality of product or service to the mission of the organisation, safety, hosting or access to sensitive data or systems, etc. The tiering structure and prioritisation rules should be agreed and approved by the sponsor and governance committee.

5) Define supplier risk assessment approach: Risk assessment is crucial for effective supplier management.

Define lifecycle scope: The supplier risk management programme should encompass the end-to-end supplier lifecycle from pre-contracting through to termination of the supplier and its products and/or services, including any requirements for records retention and destruction. While supplier onboarding is a sensible place to start the implementation of the programme, it is important that the scope of the programme cover the full lifecycle. It should be noted however that the focus here is risk assessment of the supplier, not risk assessment of the supplier's product. Lifecycle touchpoints to consider within the assessment programme include pre-contract/exploratory/innovation/business alliance development activities. Consistency of language and terms across all contracts is important. Ongoing monitoring, re-assessing supplier risk over time/re-validation (periodic or trigger-based). Examples of triggers include acquisition of supplier by another entity, change in scope of relationship, etc. End-of-relationship considerations/exit checklist (e.g., return of assets) are also crucial.

New suppliers acquired through mergers and acquisitions should be subjected to the same lifecycle approach and governed by the same programme principles. Perform a gap assessment and, as necessary, programme alignment and integration. When acquiring a legacy supplier risk management programme, any differences in acquired supplier risk assurance metrics may require re-assessment of particular suppliers.

Define risk treatment: Adopting accepted industry frameworks has the benefit of inherited acceptance and recognition from regulators, government entities, and the suppliers themselves, which helps reduce friction in the redlining and auditing processes.

Internationally recognised frameworks include the National Institute of Standards and Technology (NIST) Cyber Security Framework and the International Organization for Standardization (ISO) 27000-series.

A consistent risk assessment framework should be developed to ensure standardisation of assessment and treatment options across all lines of business tailored to supplier tiering and the assessor organisation's skills and resources. Common risk assessment approaches include supplier self-assessment questionnaires, which can be managed manually using spreadsheets, or automated with commercially available software. Evidence-based audits by the assessor or an independent third-party certification are useful. Framework audits and certifications act as proxies for assurance (e.g., ISO, NIST, commercial third-party certifications) and external sources of assurance (e.g., AICPA SOC 1/2/3 reports).

On-site assessments/supplier audits and external "outside-in" risk monitoring and scoring solutions that provide external risk monitoring are also useful as these involve gathering data and reporting cybersecurity posture based on the publicly visible digital footprint of suppliers.

The organisation must define an approach to treatment of identified supplier risk to include criteria for mitigating risk (implementing compensating controls). Transfer of risk is essential (e.g., cyber insurance, third-party credit card processing service, third-party service that leverages identity management trust framework). Accepting risk is necessary where a business decision is informed by an understanding of the risk vs the business value. Avoiding risk is needed to find an alternative supplier or alternative solution to meet the business need.

Outsourced approach to supplier risk management: Another option for organisations to consider is contracting a specialised third party to perform supplier risk assessments. Third parties that provide such services may have the skills and scale to perform this work more efficiently than doing it in-house. These and other service providers may also provide additional services to perform questionnaire-based or on-site assessments as well as conduct external risk monitoring using tools mentioned above.

Any organisation looking to outsource risk assessments may consider subscribing to a third-party risk management services partner. A number of for-profit and not-for-profit providers are available.

6) Supplier risk management as part of business operations: Having established the programme, the organisation needs to put in place the structure to sustain that programme on an ongoing basis. The following activities are recommended:

People

- Assign executive sponsor.
- Establish required staffing and skills:
  a Role matrix supporting the processes.
  b Skills inventory supporting the role matrix.
  c Projection of required staffing for each role based on demand.
- Train stakeholders and provide continual awareness of the programme.

Process

- Establish executive governance that monitors health of the programme overall, including strategic direction, resourcing, etc.
- Establish operational governance dealing with performance to plan, issue management, coordination of activities, including assessments and audits with supports, etc.
- Establish and maintain a risk register or ideally integrate with an enterprise risk management programme.
- Maintain the current supplier inventory, including a current supplier relationship owner. The recommendation is that procurement, as the gatekeeper of the contracting process, plays this role.
- Provide sponsorship and organisational change management to ensure the required changes are harmonised with existing processes and integrated in business operations.
- Track and communicate supplier risk posture and visibility.
- Harmonise supplier assessment/engagement processes across functions and geographies to provide better user experience for both internal stakeholders and suppliers.
- Document processes such as auditing, project management, task management, compliance, etc.

Tooling

- Establish a single authoritative database for suppliers for the organisation.
- Harmonise supplier assessment/engagement tools across functions and geographies to provide better user experience for both internal stakeholders and suppliers.
- Ensure tooling provides capabilities for real-time visibility to the status of supplier risk management activities.
- Leverage advanced technology for analytics and process automation to achieve higher scalability and efficiency.

Controlling

- Collect data (ideally automatically) to drive metrics and measures.
- Establish owners, targets, audience, communication cadence for metrics and measures.
- Engage in benchmarking with industry partners to continuously improve the programme and processes.

Supplier Risk Governance

1) Define Organisation's Supplier Risk Management Policy, and Establish Roles and Responsibilities.

Define and publish policy: The supplier risk management policy should be defined in consultation with the executive sponsor of the supplier risk management programme and, depending on the size of the organisation, representation from legal, procurement, IT, security, privacy, compliance, quality, and facilities. Define and document your organisation's supplier risk management policy.

Policy documents should contain the purpose, scope, definition of terms used, roles and responsibilities, policy requirements (including pre-contracting due diligence, contracting, supplier governance and ongoing monitoring, and expiration/termination of supplier contract and relationship), exception management, approval matrix, effective date, and version history.

Establish roles and responsibilities: In addition to selecting an executive sponsor, it is important that the organisation define a business function that is directly responsible for owning the supplier inventory and maintaining its currency and accuracy. While IT may provide the underlying system, the inventory and process are more typically owned by procurement, finance, or legal.

2) Identify suppliers: It is foundational to identify a list of suppliers providing products or services to your organisation. The information gathered in this crucial step will drive prioritisation and enable risk scoring for each supplier. For some suppliers, further granularity may be required; for example, a large supplier with multiple geographies, services, and subsidiaries, which may have independent contracts representing different types of risk.

For existing suppliers, there can be many sources for inventory information. Some starting suggestions would be within departments like accounts payable, business associate agreements, contracts, IT inventory (CMDB, network, etc.), procurement, value added resellers (VARs) / aggregators, and data export from an enterprise resource planning (ERP) system.

Once existing suppliers are identified, it is important to maintain the currency and accuracy of the inventory by capturing any new, changing, or retired supplier relationships. Additional suggestions for process triggers to update the inventory include legal counsel, project management office (PMO), departmental strategic decisions, procurement teams, and risk committee.

In addition to the above process triggers, a periodic review of the supplier inventory is necessary to ensure accuracy, with frequency depending on the size and turnover within your organisation's supplier inventory.

In terms of a supplier inventory system, where organisational resources allow, there are commercially available software options which enable workflow automation, collaboration, links to contract repository and risk assessments, data resiliency, version control, etc.

3) Prioritise suppliers: Once a complete list of suppliers with their products/services is captured, the next step is prioritising the suppliers so that risks can be adequately managed. Prioritisation categories and their associated weights will vary between organisations.

Below is a suggested starting point for prioritisation categories:

Annual spend: Referencing contracts, accounts payable, or procurement should produce the annual spend on a per-supplier or per-service basis. This "spend analysis" can be useful in prioritisation, especially when deciding which suppliers may be strategic vs transactional. The difference between a strategic and transactional supplier is determined by the relationship and the services they will provide. A strategic supplier typically has a long-term relationship and provides ongoing services for critical functions or business processes. A transactional supplier typically has a shorter duration contract and has limited scope and/or is project-focused.

Sensitive/confidential data: Referencing Business Associate Agreements, departmental assessments or the IT inventory may produce artefacts surrounding sensitive data types and counts. This prioritisation category may be important due to regulatory compliance and/or customer risk. Within this prioritisation, the volume of data as well as the sensitivity of each record should be considered.

Customer risk: Managers can provide valuable input and help rate any potential impact to customer risk. For example, the lack of availability of products, services, and technology may pose significant customer risk and should be considered in this exercise.

Revenue impact: Reference the ERP system, accounts payable, and other financial and sales departments to identify which suppliers' products or services directly affect or impact revenue-generating services.

Operational impact/business criticality/geopolitical: Similar to revenue impact, work with stakeholders to understand if the in-scope products or services would have an impact on day-to-day operations (regardless of revenue). IT may also become a good resource for this information if the organisation has a mature disaster recover/business continuity programme and has performed a business impact analysis (BIA).

Regulatory compliance: Similar to the efforts performed in the "sensitive data" analysis, work with those teams to understand if the product or service is in-scope for any regulatory compliance issues (HIPAA, Sarbanes-Oxley, GxP, etc.).

Reputational impact: Work with legal counsel and departments to understand if any services or platforms may have reputational impact for the organisation (e.g., customer-facing websites, scheduling applications, etc.).

When identifying critical services and their level of criticality, organisations may consider the financial, operational, or strategic importance of the service, and any critical operations (including but not limited to critical functions) and core business lines therein that rely on it. They may consider the level of tolerance for disruption set by the organisation regarding the critical operations and core business lines that rely, or will rely, on the service. Another key factor is the nature of any data or information shared with the service provider. In particular, whether these data require increased security measures because they are crucial for the organisation's critical operations, required for regulatory purposes, confidential, or sensitive (including but not limited to personal data). Organisations may take into account the impact of disruption to the relevant service or service provider on the confidentiality, integrity, or availability of these data. Another measure of criticality is the substitutability, or lack thereof, of a service. Services that are easily and readily substitutable may be less critical.

The criticality of a service can vary over time. Services that were originally not critical can become so gradually or upon the occurrence of certain events. Likewise, services that were critical can become less critical, or even become non-critical over time. Organisations can assess the criticality of a service prior to entering into a third-party service relationship and re-assess it regularly during scheduled review periods, when planning to change their use of the service, and when there is a material change to the service or the service provider (e.g., a corporate reorganisation or transaction, such as a merger, which may impact the provision of the relevant service).

Tiering the supplier: Based on the outcome of the identification and prioritisation steps, the organisation should tier its suppliers based on risk.

This tiering will allow for systematic risk assessment of suppliers. The organisation should define an appropriate tiering structure based on the inventory data and risk spread. This could be a High–Medium–Low tiering, or a similar two- or four-tier model, or others.

Onboarding due diligence can be carried out proportionate to the criticality of the relevant service.

Tools we can leverage as part of due diligence include those supporting analysis of relative benefits, costs, and risks of the proposed arrangement. They also include assessment of the service provider's ability to provide the relevant service.

These may include the service provider's:

- Operational and technical capability and track record.
- Financial soundness.
- Internal controls and risk management, its ability to manage ICT, cyber, and operational risks.
- Management of supply chain risks, including oversight of nth-party service providers.

- Geographic dependencies and management of related risks.
- Competencies of key personnel involved in service delivery.
- Conflicts of interest.
- Recent or pending relevant complaints, investigations, or litigation.
- Ability to deliver the critical service allowing compliance with legal and regulatory obligations.
- Ability to support business strategy and plans, including objectives for innovation.
- Business continuity plans, contingency plans, disaster recovery plans, and other plans, including, if applicable, recovery time objectives, maximum tolerable downtime and similar concepts.
- Level of substitutability of the service.

4) Assess supplier risk: There are many methods to assess supplier cybersecurity risk. The following two approaches applied separately or in combination represent best practices for small and medium-sized organisations.

Rely on Certifications (e.g., ISO 27000, NIST, PCI, SOC 2, other Third-party Certifications etc.)

Rather than performing an in-house assessment of the supplier's cybersecurity posture, an alternative is to place reliance on one or more external certifications held by the supplier, provided independently by an authorised third party. There are varying levels of assurance and timing considerations for external certifications; an assessment based on a certification by itself does not guarantee the supplier's cybersecurity posture. Additional analysis and review may be necessary for strategic suppliers (i.e., critical, high, tier 1, tier 2, etc.)

The following certifications are common examples which provide broad-based coverage for cybersecurity controls assurance:

TABLE 9.1 Sample Cybersecurity Control Certifications

Description	*AICPA SOC 2*	*ISO 27001*	*Commercial Third-party Assessments and Certifications*
	The AICPA & CIMA SOC 2 report evaluates an organisation's information systems relevant to security, availability, processing integrity, confidentiality, or privacy. SOC 1 reports are also available; however, these are focused on IT controls supporting financial accounting accuracy.	An information security standard, part of the ISO 27000 family of standards, which specifies a management system to bring information security under management control and gives specific control requirements.[6]	Other proprietary third-party assessments and certifications provided by different vendors are available with different levels of industry penetration and acceptance. For the most part these certifications are based on or take elements of other established standards such as NIST CSF and ISO 27000-series.
Rationale for Inclusion	Widely recognised framework by non-IT/IS professionals.	International standard with a relatively high adoption rate.	Third-party certifications provide an alternative way for suppliers to provide assurance on their security posture.

Assessment of supplier's cybersecurity posture: For strategic suppliers, organisations should perform an assessment as frequently as needed for business operations, but at a minimum annually. Based on the outcome of the assessment, contracts may need to be updated, and executive management informed for awareness and to enable them to make decisions about the relationship.

Once the assessment is completed and returned, review the colour coding of the results and the comments made by the supplier. While the reality is that there may be shades of grey in some of the responses, controls need to be assessed, and therefore if the supplier is unable to meet one of these requirements fully, it is necessary to consider the amount of risk the organisation is willing to assume by engaging with the supplier. As already mentioned above, it may be advantageous to contract with qualified assessor organisations for this risk assessment activity.

As part of the assessment process, third-party security services provide data on a supplier's public-facing cybersecurity posture. Such services provide a useful data point but should not be considered as much assurance of an organisation's cybersecurity posture.

5) Respond to supplier risk assessment: The supplier risk management programme's executive sponsor is required (potentially in consultation with legal counsel) to take a position on the amount of risk the organisation is willing to accept. The output of the supplier inventory, prioritisation, and assessment process should be reviewed initially (and then periodically thereafter) with senior leadership so that supplier risks can be understood and measured in the context of that risk appetite, and appropriate recommendations can be made.

Once the risk posture of the supplier is identified and measured, if the risk level falls within the risk appetite established by the executive sponsor, the next step is for the organisation to ensure that the contract with that supplier adequately covers the necessary controls. Robust documentation should be maintained showing identified risks, decisions taken in response and, where appropriate, requirements for supplier accountability for implementation of mitigations of identified risks.

If the risk level falls outside the risk appetite of the organisation, the following steps are recommended:

1. Document the identified risks and business impact for the organisation.
2. Determine if additional controls or mitigations (which may include cybersecurity insurance) can be implemented by the supplier within a satisfactory timeframe.
3. Inform the executive sponsor of the recommendation.

If the decision from the executive sponsor is to continue the relationship, the purchasing organisation should work with the supplier to update the contract to reflect additional control requirements and mitigations to be implemented in line with committed timeframes.

Changing requirements in a current contractual engagement with a supplier may result in the organisation bearing the price of cybersecurity enhancements implemented by its suppliers. To combat this effect, organisations may strategically plan to include cybersecurity requirements when contracts with vendors expire and/or are renewed. As a result, suppliers may choose to absorb the cost of cybersecurity enhancements in order to retain the business of the purchasing organisation.

If the supplier is unable or unwilling to update or modify its practices or capabilities to meet the required risk level, the executive sponsor must decide whether to accept the risk and continue the relationship or terminate the engagement.

If the decision from the executive sponsor is to terminate the relationship, the organisation should initiate its sourcing process to find an alternative supplier, using the same cybersecurity risk assessment approach as part of the selection process.

Additional controls measures firms could implement to protect data can be set out in an outsourcing policy and, where appropriate, in contracts.

Supplier firms must implement robust controls for data in transit, data in memory, and data at rest. Depending on the materiality and risk of the arrangement, these controls may include a range of preventive and detective measures, including but not necessarily limited to:

- *Configuration management.* This is a particularly important measure. In the context of cloud, misconfiguration of cloud services can be a major cause of data breaches.
- *Encryption and key management.*
- *Identity and access management,* which should include stricter controls for individuals whose role can create a higher risk in the event of unauthorised access (e.g., systems administrators). Firms should be particularly vigilant about privileged accounts becoming compromised as a result of phishing attacks and other leaking or theft of credentials.
- *Monitoring of* "*insider threats*" (i.e., employees at the firm and at the third party who may misuse their legitimate access to firm data for unauthorised purposes maliciously or inadvertently). The term "employee" should be construed broadly for these purposes and may include contractors, secondees, and sub-outsourced service providers.
- *Access and activity logging.*
- *Incident detection and response.*
- *Loss prevention and recovery.*
- *Data segregation* (if using a multi-tenant environment).
- *Operating system, network, and firewall configuration.*
- *Staff training.*
- *The ongoing monitoring of the effectiveness of the service provider's controls*, including through the exercise of access and audit rights.

- *Policies and procedures to detect activities* that may impact firms' information security (e.g., data breaches, incidents, or misuse of access by third parties) and respond to these incidents appropriately (including appropriate mechanisms for investigation and evidence collection after an incident).
- *Procedures for the deletion of firm data* from all the locations where the service provider may have stored it following an exit or termination, provided that access to the data is no longer needed by the firm. When deciding when to delete data, firms will need to consider their obligations under data protection law and their potential data retention obligations.

Where data is encrypted, firms should ensure that any encryption keys or other forms of protection are kept secure by the firm or outsourcing provider. The ability of service providers to respond to customer-specific data security requests may vary depending on the service being provided. Generally, the more standardised the service, the more difficult it might be for the service provider to accommodate these requests. The overall effectiveness of the service provider's security environment should be at least as effective as their in-house security environment.

Contracts And Performance

1. *Contracts and cybersecurity risk:* All supplier relationships involving the procurement of goods or services that are enabled by, or dependent on, technology or data involve a degree of cybersecurity risk. Contracts by themselves do not mitigate risks completely. They *may* facilitate the transfer of risk to a supplier or insurance provider, but are more commonly effective in:

    - Clarifying the roles and responsibilities for the controls that the contracting parties commit to enact to manage the risk.

        a What is the buyer committing to do in order to ensure security?
        b What is the supplier committing to do in order to ensure security?

    - Stipulating mechanisms whereby the contracting parties can gain visibility to adherence (or not) to the contractual commitments made over time – e.g., sharing independent audit reports, scan/test reports, on-site audits, etc.
    - Establishing service level agreements, patching vehicles, and disclosure requirements in the case of a security incident or new vulnerability being discovered. Language should include definitions of a breach or incident, committed timeframes for customer notification, root cause analysis, restoration of service, producing a patch or implementation of long-term resolution, etc.

- Ensuring that the supplier applies the same contractual requirements to any subcontractors/suppliers they involve in the provision of the product or service to the customer.

A contract may give the purchasing organisation a level of confidence in the safeguards promised by the supplier, as it forms the basis on which a legal claim can be made in the event losses are suffered through a cybersecurity incident. However, it is important that the purchasing organisation understands that after-the-fact legal recourse may be of little comfort when stacked against the reality of operational losses, reputational damage (regardless of actual liability), or even customer harm in the event of an incident. Therefore, even with the contractual assurances provided by the supplier, the purchasing organisation should ensure that the value created for the organisation by entering into a relationship with the supplier outweighs the potential risks to its stakeholders (customers, employees, other suppliers, communities, the environment, and any stock-holders).

2) Contractual clauses: The requirements are designed to be specific enough to be actionable and drive accountability on the part of the supplier, while being modest enough in their aspirations that they represent a minimum level of security good practice that any organisation of any scale should be able to meet. If an organisation's supplier is unable or unwilling to meet the requirements articulated in this template, that may be an indicator of their scale and level of maturity and consequently may be a cause for concern.

Guidance on the redlining process (that is, the process by which the legal representatives of each contracting party negotiate on the contractual language) follows. However, it is important to note that as a generic starting point, the relevance and importance of the different controls described in the template will depend on the nature of the relationship with the supplier and the risk that represents for your operations and those whose data you hold or who rely on your products and services. Therefore, establishing which threats and which supplier relationships are most critical to your operations and to the stakeholders is an essential starting point.

Understanding that the audience for this document is non-technical, each control within the contractual boilerplate is tagged to one or more of these threats to help the purchasing organisation understand the implications if a supplier is unable or unwilling to commit to a given control in the contract.

Before commencement of the contracting process, consult Table 9.2 and identify the most relevant threats and how your organisation and customers could be put at risk through an incident at the supplier, or how the relationship with the supplier could introduce them into your environment.

This language can then be added into your own contract document, or into the supplier's document if the contracting is to take place on their paper.

If the supplier is unwilling to add these requirements into their contract you should insist that they demonstrate equivalence. These requirements are considered to be the minimum base which any organisation should be willing to meet (they are after all in the supplier's own self-interest).

Consider leveraging the template in Table 9.2.

3) Guidance on the redlining process: The intended audience for this is small to medium-sized organisations, typically those without dedicated cybersecurity subject matter experts on staff. This chapter therefore attempts to provide a contracting template that incorporates technical concepts into a workable format, without requiring an in-depth cybersecurity knowledge.

Contract clauses should be based upon guiding principles. Clauses should be structured with a "common core" set of requirements which are applicable to any supplier relationship and "supplemental" requirements specific to the type of supplier relationship. Note: the supplemental requirements are not mutually exclusive and multiple requirements may be applicable to a single contract. Furthermore, there may be relationship types outside of this list which are not effectively covered. In that case, it is advisable to seek independent guidance from a qualified cybersecurity subject matter expert.

Clauses should be designed with enough specificity to be actionable and enforceable, while also representing a value-adding but basic cybersecurity maturity level. This maturity level is intentional to minimise the redlining during the contracting process. If the customer's supplier is unable or unwilling to meet these requirements, it may require additional due diligence because that may be an indicator of their relative scale and level of capability to meet the organisation's needs and consequently may be a cause for concern. Similarly, if the relationship is particularly sensitive or critical, it may be advisable to contract independent subject matter expertise to give case-specific guidance going beyond the lowest common denominator cybersecurity practices that this chapter lays out.

Keeping those principles in mind, as with any negotiation, it is common for compromises to be made in order to arrive at an agreement that is acceptable to both parties. Not all of the stipulations of the template language below will be equally important in every case. Their importance will depend on the nature of the supplier relationship and the impact a cybersecurity incident may have on each party. For example, if the nature of the relationship is such that the supplier is hosting or has access to the customer organisation's data, some controls may be more important than if the supplier is simply providing a product without access to the data.

Another common scenario is for the supplier to insist on their own contractual language as the basis for the agreement. In this case you can either ask that this contractual template be inserted into that document or ask the supplier to map their requirements to this template and demonstrate how they meet or exceed their terms.

Ultimately, if the supplier is unwilling to meet one or more of the terms of this recommended contract language, the organisation must decide whether to

TABLE 9.2 Cybersecurity Threats and Impacts by Supplier Relationship Type

Threat	*Potential Impact of Attack (non-technical audience)*	*Examples of Supplier Relationships*
Email phishing attack	Email "phishing" is the most common form of cyber attack. It typically involves the victim receiving a malicious email that persuades them to either click on a link or open an attachment. Links may take the victim to a look-alike or malicious website where they are either persuaded to enter their user I.D. and password (thereby giving those details to the attacker), or the malicious website or email attachment may download malware to the victim's computer. Different malware has differing functionality – e.g., spying on the user, giving the attacker control of the computer or other computers on the same network, or holding the victim's data ransom (see below). Phishing is not restricted to email – other vehicles could be unsolicited SMS messages, instant message app messages, or even malicious USB devices.	A supplier storing/processing sensitive data on your behalf. A supplier with access credentials to your computer systems, for example for tech support or to input orders.

Threat	*Potential Impact of Attack (non-technical audience)*	*Examples of Supplier Relationships*
Ransomware attack	Ransomware is a type of malware whereby the attacker encrypts the victim's data, making it inaccessible, and demands payment to release it. Ransomware is among the most common cybercrimes and victimises organisations of all sizes. Unavailability of mission-critical data or software can disrupt an organisation's ability to serve customers or operate as a business. Like the effects of a fire or other disaster, many organisations never recover from a period of downtime exceeding a week. Ransomware affects not only "traditional" computer systems (desktops, tablets, etc.) but also connected "smart" devices such as thermostats, building control systems, security cameras, etc.	A supplier that is the sole supplier for a mission-critical product or service (if they are down, you are down). A supplier that is the exclusive holder of data critical to your mission. A provider of IT hosting, IT support services, cloud-based software, or software within devices that your organisation sells or depends upon.

Threat	*Potential Impact of Attack (non-technical audience)*	*Examples of Supplier Relationships*
Loss or theft of equipment or data	Theft of media storage, files, or devices holding sensitive data.	A supplier storing/processing sensitive data on behalf of the customer organisation. A supplier with access credentials to the customer's computer systems. A supplier with physical access to devices or network of the customer organisation.
Accidental or intentional data loss	Accidental loss of data; for example, downloading data onto a laptop which is then lost or stolen, mailing data storage, which is lost in the mail, leaking of data by an insider to other organisations not authorised to access it.	A supplier storing/processing sensitive data on behalf of the customer organisation. A supplier with access credentials to the customer's computer systems. A supplier with physical access to devices or network of the customer organisation.
Attacks against connected IoT devices	Tampering with the proper functionality of "smart" or connected devices or making those devices unavailable, for example by shutting them down or locking legitimate users out of them.	A supplier of IoT or smart devices. A supplier with access credentials to systems. A supplier with physical access to devices or network of the customer organisation.

proceed regardless or seek alternatives. The decision to proceed with the relationship should be based on whether the potential derived value is greater than the potential risk to the organisation and, more specifically, its customers, employees, environment, and shareholders/owners in the event of a cybersecurity incident.

4) Guidance on how the buyer might obtain assurance: Contracts define the vehicles for the buyer to gain assurance that the controls promised are actually in place, be they technical controls implemented within a product, or process controls that the supplier executes as part of how they provide their service or maintain/support their product over time.

Unfortunately, suppliers may have little incentive to provide transparency, especially to smaller customers with less leverage/purchasing power. Moreover, even if such transparency were provided, small organisations have limited capacity and capability to digest and understand the information. Therefore, for small organisations it is important to focus on the most important supplier relationships based on potential impact. In addition, consider the following:

Security is expensive. A supplier may be cutting the costs of their security programme to reduce overall IT expenses.

Security is hard. All other things being equal, larger suppliers (with more demanding larger customers) are more likely to have the scale which enables them to secure their products and services, whereas smaller companies may find this more challenging.

Security is a moving target. Whereas functionality may still meet the need five or ten years from now, the security may no longer be adequate as security threats are constantly evolving. Consider the useful life of the product and beware high-risk engagements with little in the way of long-term relationship or support.

Regulatory compliance is not equal to security. Compliance with regulation does not necessarily mean good security. A security programme that is designed to only comply with regulations may be putting an organisation at significant risk.

Indicators of good practice. While a customer organisation may not be able to audit a supplier or test the security of their products or services, there are still indicators of good practice:

- The supplier proactively tests their controls, regular penetration tests, or in good cases red team exercises.
- Regular independent audit of their security controls.
- The supplier demonstrates openness and transparency about their security controls.
- The supplier has industry certifications such as ISO 27000-series, SOC 2, or other proprietary for-profit third-party certifications. Their products may comply with standards such as NIST CSF. While these indicators

have limitations, they may point to a company culture that embraces the need for good security practices.
- Supplier holds cyber insurance. While cybersecurity insurance is still an evolving field, underwriters often ask businesses for minimum levels of cybersecurity maturity before they are willing to assume a company's risk by selling them a cybersecurity insurance policy. This is therefore another potential indicator that the company is doing the right things. More comments on cybersecurity insurance follow below.

5) Guidance on contractual forms of risk transfer (e.g., cyber insurance): Cybersecurity insurance is a growing business within the insurance industry and is an option for organisations to limit their exposure to some of the costs in the event of a security incident.

Some important considerations before purchasing cyber insurance follow:

- First- vs third-party insurance: Is the policy providing the insured compensation for the impact from a breach/incident or only compensating the affected supplier?
- Does the insurance cover only the legal fees or liability claims, or does it also cover loss of revenue/business or personal injury claims (given the care context)?
- Does the insurance cover acts of war or terrorism? Note that some of the highest profile ransomware incidents of recent years have been attributed to governments rather than criminals, and therefore some insurance providers have considered them acts of war or terrorism and have disputed claims.
- Cyber insurance is not a replacement for cybersecurity. Any short-term payout may well turn out to be insignificant compared to the long-term customer safety, reputational, or financial losses incurred as a result of an incident.

Another form of risk transference is identity federation. Organisations engaging with suppliers may opt to transfer identity risks to the supplier by requiring the supplier to issue or procure identity credentials certified by a Trust Framework that the buying organisation trusts. This allows the organisation to transfer the risk and expense of identity credentials to its suppliers rather than issue and manage supplier credentials themselves.

When federating identity management with suppliers, the organisation may consider requiring the supplier's credentials to participate in a trust framework using a level of assurance that offers the buying organisation (relying party) insurance coverage in the event of identity compromise.

Audit Process

1) Defining the audit process: What does contractual verification mean and who performs contractual verification? *Contractual verification simply means the process through which we can reasonably determine whether a supplier is meeting its contractual requirements and, if not, what remediations are necessary to close deficiencies.*

An organisation's resources may limit its ability to gain assurance that the security controls defined in the contract are operating effectively. It is important that every business in the supply chain – regardless of size – be considered for contractual verification. Risk of downstream suppliers may impact an organisation's direct suppliers. This is often referred to as "Nth-party vendor risk".

2) Identify controls to be verified and method of verification: Now it's time to put these concepts into practice and verify the contractual obligations in place and establish the frequency with which those contracts need to be verified. The organisation should review the controls designed to mitigate risk and their implementation, including how well the control is supported by documented policy and procedures. Additionally, it is important to monitor the effectiveness of the control over time and report on degradation in effectiveness or failure of the control which could trigger a re-assessment and audit.

Regardless of whether the control was in place at the time the contract was signed or has been implemented since, the organisation has a number of techniques available in order to gain assurance that the contract terms are being honoured. The option(s) chosen will depend on:

- The risk the supplier represents to the organisation.
- The capability and capacity of the organisation's internal resources to audit the supplier or request evidence, to interpret the responses received from the supplier, and to form a judgement.
- The organisation's ability to hire external specialist resources to gain assurance.
- The contractual right to audit the supplier or their goodwill in supporting the organisation's requests for assurance.

Options for gaining assurance that contractual agreements are being met include:

- Enquiry with the supplier through ad hoc requests for information or regular touchpoints (for example as part of quarterly business reviews) whereby the organisation requests assurances from the supplier (i.e., attestation) that they are meeting the terms of the contract.
    a Pros – easily done.
    b Cons – the organisation is reliant on the supplier's collaboration and level of control over their own environment and processes.

- Enquiry with the supplier supplemented by some previously agreed KPIs.
    a Pros – commits the supplier to provide specific details.
    b Cons – the organisation is reliant on the supplier's collaboration and requires subject matter expertise to interpret the data provided by the supplier.
- Independent proxies for assurance, such as valid ISO 27000-series certification or PCI DSS compliance.
    a Pros – such certifications are independent and require little subject matter expertise to interpret the response.
    b Cons – these certifications are unlikely to provide details for all of the controls which are most important to mitigate the risk the supplier represents to the organisation.
- Subscribe to an "outside-in" cybersecurity risk monitoring and scoring service. These services provide external risk monitoring for a fee, gathering data and reporting cybersecurity posture based on the publicly visible digital footprint of suppliers.
    a Pros – these services provide an easily digestible rating and a detailed report for the supplier to respond to, much like a credit rating and report.
    b Cons – they typically only provide insight into the supplier assets that are visible from the public internet and are prone to false positives and assets or systems being tagged to an organisation incorrectly.
- Obtain an independent controls assessment such as AICPA SOC 1/2/3 reports (ideally at the supplier's expense).
    a Pros – these reports are standard and provide independent assurance from a qualified auditor.
    b Cons – the organisation will still require a level of subject matter expertise to interpret the output and draw a conclusion on the risk any gaps represent.
- Conduct an audit of the controls or hire a third party to do so (ideally at the supplier's expense).
    a Pros – good quality assurance.
    b Cons – expensive, time-consuming, and assumes the organisational resources and the contractual right to audit already agreed with the supplier.

3) Conducting supplier audits: An audit should review the controls designed to mitigate risk and their implementation, including how well the control is

supported by documented policy and procedures. Additionally, it is important to monitor the effectiveness of the control over time and report on degradation in effectiveness or failure of the control, which could trigger a re-assessment and audit.

The first step in conducting a supplier audit is to determine which controls in the contract are to be included in the audit. Contracts with suppliers and third-party partners must be used to implement appropriate measures designed to meet the objectives of an organisation's cybersecurity programme and cyber supply chain risk management plan.

The next step is to determine the verification method for each control, including reports and other artefacts, attestation, or testing.

The frequency of audits depends on many risk factors. For example, the organisation may audit based on the supplier risk tier or change in the relationship. Some suppliers, such as those that pose little regulatory, operational, or security risk, can be assessed as part of the normal course of business operations, such as during initial onboarding and on a periodic basis. Organisations may do an audit for low-risk suppliers every two or three years.

In addition to inherent regulatory, operational, and security risks, certain events change risk and should trigger an audit. These events would include mergers and acquisitions, the launching of new product lines, entering new geographic regions, and the deploying of new software that could have an impact on risk.

4) Maintaining the verification process: Regardless of the methods an organisation chooses to evaluate a supplier's compliance with the agreements, the assessment methods should be periodically reviewed and updated. To the extent possible, the verification methods should be standardised, automated, and streamlined.

The processes associated with contractual verification of supplier risk are not single events. A verification life cycle must be put into place and maintained. This includes not only the assessments and audits of suppliers but also continuously assessing internal third-party risk management policies, procedures, and controls.

5) Eliminating gaps in contractual compliance: As supplier contractual compliance verifications are completed, gaps may be discovered that may require the organisation to employ various risk treatment options such as:

- *Mitigate* – when a supplier presents a moderate or high risk, the organisation may choose to work with the supplier and implement remediation or mitigation controls.
- *Transfer* – when a supplier presents a moderate or high risk, the organisation may choose to transfer the risk to an insurance policy.
- *Accept* – conversely, if the risk is high or moderate from a low-impact supplier, the organisation may decide to accept it as is.

- *Avoid* – when a critical supplier presents a high risk and there is no agreed-to remediation or mitigation plan, the organisation may choose to avoid the risk altogether and terminate the agreement with the supplier.

An organisation should explore the above options as required; however, the organisation and suppliers should collaborate to remedy any identified gaps in a mutually acceptable way, and the remedy and milestones/timelines should be documented and agreed to in writing.

These contractual gaps to be remedied should be tracked throughout the life cycle of the supplier contract. Supplier relationships may be based on multiple contracts, which adds complexity to the verification and remediation process. Systematic and automated approaches are becoming available to help manage workflows, timelines, dependencies, approvals, and deliverables required through the contractual gap remediation process.

Response and Recovery

Establish procedures for response and recovery: The fact that small to medium-sized organisations are limited in their ability to assess risk and to hold suppliers accountable for meeting the terms of their contract means that being prepared for *when* an incident happens is especially valuable.

Organisations need to develop plans which can be put into action in the event of a supplier-related cybersecurity incident. Two types of plans must be considered:

1. *Response plans,* which support the ability to detect and contain the impact of a potential cybersecurity incident.
2. *Recovery plans,* which implement appropriate activities to maintain and/or to restore any capabilities or services that were impaired due to a cybersecurity incident.

NIST CSF establishes effective response, recovery planning, and testing protocols. To limit the impact of cyber incidents, we need planning and testing procedures in place so that an organisation can better respond to, and recover from, a supplier data or service availability incident.

Incident response and recovery processes can be summarised with the following stages:

1. *Preparation:* Establish and train a response team.
2. *Detection and analysis:* The organisation must establish mechanisms for suppliers to alert the organisation in a timely manner in the event of a breach or incident and understand the implications for the organisation.

3. *Containment, eradication, and recovery:* Depending upon the severity of the incident and the extent to which the organisation is impacted, the organisation can evaluate and determine the appropriate response to mitigate any impact and restore capabilities as needed.
4. *Post-incident activity:* After the organisation has adequately handled the incident, a report is produced detailing the cause, the costs, and what steps can be taken to prevent a similar incident from occurring in the future.

Establishing the team: As organisations rely on third-party suppliers to perform services, it is natural that some critical operations get moved into the cloud or outsourced completely. These operations may have a role in the incident response and recovery following a security or privacy incident at another supplier. For example, the organisation may need the assistance of its IT managed service provider if another supplier such as the HR and payroll processor has a data breach. For this reason, key supplier roles and responsibilities must be considered as part of the incident response and recovery process.

Suppliers should be included in the response plan as part of the contractual relationship. This may require adjusting the terms of the contract with a supplier, for example their hours of support or response time SLAs.

The roles and responsibilities of suppliers should also be captured in the response plan. One tool to effectively identify roles and responsibilities is a RACI matrix (Responsible, Accountable, Consulted, and Informed). A RACI may also help identify gaps in roles and responsibilities during the contracting period to ensure that all responsibilities are adequately addressed.

The RACI matrix is also an effective starting point to develop testing for the response and recovery plans. Each task assigned to the supplier in the matrix should be included in the test plan and evaluated from both a process and a performance standpoint. The organisation should develop written procedures and checklists that can be shared with the supplier.

It is also necessary to test a supplier's ability to perform assigned tasks identified in the RACI. Organisations should develop test plans that integrate these tasks into their workflows, then establish minimum performance requirements. Suppliers should be notified of tests in advance, but also required through contractual clauses to participate in the organisation's incident response and recovery exercises. The level of participation and performance requirements will be dependent on the supplier's risk tier – e.g., clinical suppliers may have a higher degree of active participation. Similarly, refusal of a critical supplier to participate in such exercises should be considered and treated as a supplier risk in and of itself.

1) Creating the plan: Every organisation should have an incident response plan. Suppliers should be given a designated point of contact and backup

within the organisation who would be informed in the event of an actual or suspected security incident. This point of contact should then assemble the incident team and work through a predefined incident plan. This plan may have much in common with the approach for an internal incident within the organisation, but it may differ given other factors specific to an incident at a critical supplier.

The overall response and recovery plan should consider the following (this is not an exhaustive list):

A. In the event of a security incident the supplier's internal communications may be disrupted and the supplier may be unable or unwilling to share detailed specifics during the initial stage of a major incident. Therefore, the organisation should take contingency action while waiting on information from the supplier.

B. The plan should have predefined processes to:

i Suspend VPN/Business-to-Business connectivity with the supplier if it exists.
ii Suspend any remote access the supplier may have to the organisation's information systems and assets.
iii Change passwords of user IDs belonging to supplier employees, and/or disable user accounts.
iv Monitor email inbound from the impacted supplier; increase email filter sensitivity.
v Alert employees who interact with the impacted vendor.
vi Ensure antivirus signatures are current.
vii Ensure critical systems are patched and up to date.
viii Ensure backups are operating effectively.
ix Avoid premature use of terms such as "data breach" which can have specific legal and regulatory ramifications; use instead "security event".
x Notify pre-identified points of contact and reinforce staff training on how to deal with requests for information from regulators, media, social media, or public interest channels.
xi Engage specialist third parties (for example cybersecurity forensics), as appropriate.
xii Request from the supplier incident details, including:

- Timeline.
- Indicators of compromise.
- Impacted systems.
- Source of malware/compromise if known (e.g., credential phish).
- Any information on likely target.
- Any information on lateral movement tactics and techniques.
- Actions taken.

2) Testing the plan: One of the most effective ways to close gaps in incident readiness is to perform tabletop exercises. These scenario-based simulations walk the organisation through a crisis and challenge the participants to assess the effectiveness of their established processes. Critical suppliers with a significant role in the scenario should be included in the exercise. The exercise will help identify gaps in processes, roles and responsibilities, and communication protocols.

These exercise scenarios should be as realistic as possible, attempting to stress existing processes that are relevant to a supplier's operations. Some questions an exercise scenario can address include:

How would a catastrophic ransomware incident at a key supplier affect the organisation's ability to execute its mission?
How robust is the supplier's customer support and call centre redundancy?
Who is in charge if leadership can't be reached immediately?
How are systems and lines of communication set up to ensure an effective failover when a data centre or cloud service provider is affected?
What communication must be conveyed to customers, regulators, the media, etc.?
What mitigations could be put in place? For example:

- Is the contact list current?
- What are the priorities (e.g., critical orders, key customers)?
- What backup or workarounds exist for the impacted supplier's product or service?
- What manual processes can be established in advance (e.g., where are they stored, how are they trained and disseminated)?
- Are there off-line copies of critical data such as customer contact lists, bank accounts, etc., and are they kept secure and up to date?
- Should increased safety stocks, or agreements with peers to share safety stocks, be considered for certain critical products or materials as mitigation for an interruption in supply?

These exercises are intended to identify processes, procedures, and communication improvement opportunities in a collaborative environment rather than an actual emergency.

3) Post-testing activity: Events and exercises may reveal supplier process or capability improvement opportunities to reduce potential impacts on an organisation's operations. Questionnaires or other mechanisms, whether a document, spreadsheet, or application, are useful in documenting these opportunities and essential to tracking the remediation of identified gaps in supplier business continuity and IT service disruptions plans. Additionally, periodically re-evaluate supplier relationships and contracts for changes in their business management, continuity management, and IT infrastructure.

Supplier risk management is an ongoing process. The advice provided is for small to medium-sized organisations operating in the sector that don't necessarily have in-house cybersecurity subject matter experts.

Notes

1 Safari, A., Balicevac Al Ismail, V., Parast, M., Gölgeci, I., and Pokharel, S., 2024. Supply Chain Risk and Resilience in Startups, SMEs, and Large Enterprises: A Systematic Review and Directions for Research. *The International Journal of Logistics Management*, 35(2), pp.680–709.
2 Kwong, J., and Pearlson, K., 2024. Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/957a908a-cf71-47e7-84ac-ee3a2d8c088c/content.
3 Healthcare and Public Health Sector Coordinating Council, 2020. Health Industry Cybersecurity Supply Chain Risk Management Guide.
4 Aarland, M., 2024. Cybersecurity in Digital Supply Chains in the Procurement Process: Introducing the Digital Supply Chain Management Framework. *Information & Computer Security*. https://www.semanticscholar.org/paper/Cybersecurity-in-digital-supply-chains-in-the-the-Aarland/da35d5d0589ab04e037d2e8bf4a68b6092c0b9e5.
5 https://racichart.org/the-raci-model.
6 https://www.iso.org/isoiec-27001-information-security.html.

10

THIRD-PARTY RISK MANAGEMENT AND SURFACE RISK ASSESSMENT

Third-Party Risk Management

In the ever-evolving landscape of cybersecurity, organisations often rely on third-party vendors, suppliers, and partners to support various aspects of their operations. However, this interdependence can pose significant challenges in maintaining robust cybersecurity measures. Third parties, ranging from cloud service providers to software vendors and contractors, introduce potential vulnerabilities that can compromise an organisation's security posture.

Tran et al. (2024) contend that cybersecurity awareness plays an important role in shaping attitudes and intention.[1] In this context, it is not just employees making changes to IT infrastructure – contractors, vendors, developers, and other third parties may be making even greater changes daily and subject to even higher levels of risk.

Third parties may see your organisation as just one of thousands of clients. They often don't have a good understanding of your organisation, its culture, its corporate strategies, its business needs, its resourcing constraints, or its operational challenges. But also vice versa. That gap must be bridged to improve security.

Thakur (2024) argues security awareness training is highly beneficial, but this does not stop at employees; all key parties making regular changes benefit from training and awareness activities and to reduce time and resource this can be carried out on a risk-based approach.[2]

Chaudhary (2024) argues security awareness training tailored to different stakeholders is vital. One of the primary challenges is the lack of control and visibility over third-party security practices. Organisations have limited insight into the cybersecurity measures implemented by their partners,

DOI: 10.4324/9781003604969-10

making it difficult to assess and mitigate potential risks effectively. Additionally, third parties may have varying levels of cybersecurity awareness and expertise, leading to inconsistent or inadequate security measures across the supply chain.[3]

Another challenge arises from the complexity of managing multiple third-party relationships. Each partnership may have unique security requirements, data-sharing protocols, and communication channels, making it arduous to maintain a consistent and comprehensive approach to cybersecurity. Furthermore, the integration of third-party systems and applications with an organisation's internal infrastructure can introduce vulnerabilities if not properly managed and secured.

Allahham et al. (2024) argue there are technical controls and monitoring that can be put in place using big data and artificial intelligence, enabling risk alerting for management. However, the human factors involving third parties are often overlooked.[4]

Addressing the challenges posed by third parties in cybersecurity requires a proactive and comprehensive approach that emphasises human security education and awareness. By equipping third-party personnel with the knowledge and skills necessary to identify and mitigate cyber threats, organisations can significantly enhance their overall security posture.

Human security education and awareness programmes should be tailored to the specific needs and roles of third-party personnel. These programmes should cover a wide range of topics, including cybersecurity fundamentals, threat identification and prevention, data protection and privacy regulations, secure coding practices (for software vendors), incident response and reporting procedures.

Additionally, these programmes should incorporate intelligence on live threat vectors, from previous security incidents, practical exercises, simulations, and real-world scenarios to reinforce the learned concepts and promote active engagement.

Empowering third parties through human security education and awareness offers numerous benefits for organisations. By ensuring that third-party personnel are well-versed in cybersecurity best practices, organisations can mitigate the risks associated with third-party vulnerabilities and data breaches. Many regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), mandate organisations to ensure the security and privacy of data shared with third parties. Empowering third parties through education and awareness can help organisations meet these compliance requirements. By investing in the cybersecurity education of third-party personnel, organisations demonstrate their commitment to maintaining a secure and trustworthy partnership. This can foster stronger collaboration and facilitate smoother integration of third-party systems and services. Proactive cybersecurity measures, including human security education and awareness, can help organisations avoid the

substantial financial and reputational costs associated with data breaches and cyber incidents involving third parties. Organisations that prioritise the cybersecurity empowerment of their third-party partners can differentiate themselves in the market, positioning themselves as trusted and secure partners for potential clients and customers.

Strategies for implementing human security education and awareness programmes are important for embedding cultural change. Implementing effective human security education and awareness programmes for third parties requires a strategic and comprehensive approach.

Perform thorough risk assessments to identify the specific third-party relationships and personnel that require focused cybersecurity training and awareness initiatives. Regular supplier and service reviews enable communication between security and the third parties to mutually improve services to become both a good supplier and good customer, provide security support or awareness, agree corrective actions, and mitigate risks. Design training programmes that cater to the unique roles, responsibilities, and cybersecurity challenges faced by different third-party personnel. Incorporate interactive elements, real-world scenarios, and hands-on exercises to maximise engagement and knowledge retention.

Develop and communicate clear policies and guidelines outlining the cybersecurity expectations and requirements for third-party personnel. These policies should cover areas such as data handling, access controls, incident reporting, and compliance with relevant regulations. Implement ongoing training and awareness initiatives to ensure that third-party personnel remain up to date with the latest cybersecurity threats, best practices, and regulatory changes.

Utilise technology solutions and automation tools to streamline the delivery and tracking of cybersecurity training and awareness programmes for third parties. This can include online training platforms, gamification techniques, and automated assessment and reporting mechanisms. Facilitate open communication channels and knowledge-sharing platforms where third-party personnel can collaborate, exchange best practices, and seek guidance on cybersecurity-related matters. Regularly monitor and evaluate the effectiveness of the human security education and awareness programmes for third parties. Collect feedback, analyse metrics, and make necessary adjustments to ensure continuous improvement and alignment with evolving cybersecurity needs.

Case Studies

Case studies are useful in showcasing the impact of successful empowerment initiatives. Several organisations have successfully implemented initiatives to empower third parties through human security education and awareness, resulting in improved cybersecurity postures and strengthened partnerships.

Bank of America: This major bank recognised the importance of cybersecurity education for its third-party vendors and contractors. They developed a comprehensive online training programme that covered topics such as data protection, secure coding practices, and incident response procedures. Completion of this training was made a mandatory requirement for all third-party personnel accessing the bank's systems and data. As a result, the bank experienced a significant reduction in third-party-related security incidents and improved compliance with industry regulations.

Microsoft Corp: As a leading software provider, this company understood the critical role of secure coding practices in mitigating vulnerabilities and ensuring the security of their products. They implemented a rigorous cybersecurity training programme for their third-party software development partners, focusing on secure coding methodologies, threat modelling, and secure software development life cycles (SDLC). This initiative not only enhanced the security of their software offerings but also fostered stronger partnerships with their third-party developers, leading to increased trust and collaboration.

The Cigna Group (CI): Recognising the sensitivity of patient data and the importance of compliance with healthcare regulations, this organisation prioritised cybersecurity education for its third-party medical service providers and vendors. They developed tailored training programmes that covered topics such as HIPAA compliance, data encryption, and incident response protocols specific to the healthcare industry. This initiative not only strengthened the organisation's overall security posture but also demonstrated its commitment to protecting patient privacy, enhancing its reputation and trustworthiness within the healthcare community.

Collaborative Approaches

To support organisations in their efforts to empower third parties through human security education and awareness, various resources are available.

Many industry associations and professional organisations offer cybersecurity training programmes, certifications, and educational resources specifically tailored for third-party personnel. Examples include the International Information System Security Certification Consortium (ISC2), SANS Institute, and the National Cybersecurity Center (NCC).

Government agencies and regulatory bodies often provide guidance, best practices, and educational materials related to cybersecurity and data protection. Organisations can leverage resources from agencies like the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), and the European Union Agency for Cybersecurity (ENISA).

A wide range of online training platforms and educational resources are available, offering self-paced courses, webinars, and interactive learning experiences. Examples include Coursera, edX, and Cybrary.

Attending cybersecurity conferences and events can provide valuable opportunities for third-party personnel to learn from industry experts, participate in workshops, and network with peers. Events like the RSA Conference, Black Hat, and the SANS Cyber Security Training & Certifications can offer valuable insights and knowledge-sharing opportunities.

Many vendors and service providers offer specialised training and documentation related to their products and services. Organisations should leverage these resources to ensure that third-party personnel are proficient in the secure implementation and usage of the specific technologies and solutions they employ.

Collaborative approaches are helpful to cybersecurity involving third parties. Enhancing cybersecurity through the empowerment of third parties requires a collaborative and inclusive approach. Organisations should actively involve third-party partners in their cybersecurity initiatives, fostering open communication, knowledge sharing, and joint efforts to mitigate risks and strengthen overall security postures.

Create dedicated committees or working groups that include representatives from both the organisation and its third-party partners. These forums can facilitate discussions, coordinate cybersecurity efforts, and ensure alignment on security policies, procedures, and best practices.

Collaborate with third-party partners to perform comprehensive risk assessments and security audits. This collaborative approach allows for a holistic understanding of potential vulnerabilities, shared risks, and the identification of areas requiring focused attention and mitigation strategies.

Establish coordinated incident response plans that outline roles, responsibilities, and communication protocols in the event of a cybersecurity incident involving both the organisation and its third-party partners. Regular testing and simulations can help validate the effectiveness of these plans and ensure seamless collaboration during critical situations.

Facilitate the sharing of cybersecurity-related information, threat intelligence, and best practices among the organisation and its third-party partners. This can involve establishing secure communication channels, hosting regular meetings or forums, and leveraging industry-specific information sharing and analysis centres (ISACs).

Engage in collaborative cybersecurity exercises and simulations that involve both the organisation and its third-party partners. These realistic scenarios can help identify potential gaps, test incident response capabilities, and foster a culture of continuous improvement and preparedness.

Work towards aligning cybersecurity policies, standards, and control frameworks across the organisation and its third-party partners. This alignment ensures a consistent and cohesive approach to cybersecurity, reducing potential vulnerabilities and facilitating seamless integration of security measures.

By fostering collaborative approaches to cybersecurity involving third parties, organisations can leverage collective expertise, share resources, and

establish a unified front against cyber threats, ultimately enhancing the overall security posture of the entire ecosystem.

In the ever-evolving landscape of cybersecurity, the role of empowered third parties will become increasingly crucial. As organisations continue to rely on external partners and vendors for various aspects of their operations, ensuring their cybersecurity preparedness and awareness is paramount.

By investing in human security education and awareness programmes for third parties, organisations can mitigate risks, enhance compliance, foster trust, and strengthen their overall security posture. Empowered third-party personnel, equipped with the knowledge and skills to identify and mitigate cyber threats, become valuable assets in an organisation's cybersecurity strategy.

The future of cybersecurity will demand a collaborative and inclusive approach, where organisations and their third-party partners work together to address shared risks, exchange threat intelligence, and implement coordinated incident response plans. By fostering open communication, knowledge sharing, and joint efforts, organisations can leverage the collective expertise and resources of their third-party ecosystem, creating a unified front against cyber threats.

As technology continues to evolve and cyber threats become more sophisticated, the importance of human security education and awareness will only intensify. Organisations that prioritise the empowerment of their third-party partners through comprehensive training programmes, collaborative initiatives, and continuous learning will be better positioned to navigate the complexities of the cybersecurity landscape and maintain a resilient and secure operational environment.

Kwong and Pearlson (2024) contend that SMEs are particularly struggling with supply chain cybersecurity and especially with Third Party Risk Management (TPRM). Facing significant cyber threats, organisations are transforming to enhance capabilities amid growing uncertainties. Those investing in TPRM maturity navigate complexities more agilely, becoming more sustainable, resilient, and trustworthy, often through digital transformation.[5]

Employees view TPRM practices positively, especially in organisations investing in capability and agility to meet evolving expectations. Organisational cultures are increasingly supportive of managing ESG risks and opportunities related to third parties, using more quantitative assessments despite data quality concerns. However, according to a Deloitte report on Third Party Risk Management many miss synergies between sustainability and resilience initiatives.[6]

Chukwu et al. (2024) argue organisations must prioritise supply chain resilience and ensure all third parties they partner with engage fully. They contend this must involve emerging technologies to provide transparency such as AI-driven risk assessment and mitigation to drive improvement in TPRM.[7]

Embedding strong resilience practices across the extended enterprise is a priority, shifting from "Just in Time" to "Just in Case". This involves better integration of business strategy and risk, supported by technology. Mature TPRM practices aim to deepen trust with third parties through transparency, reliability, capability, and humanity, moving governance from questionnaires to collaborative innovation and performance discussions.

Rapidly evolving third-party risks drive organisations to pursue digital transformation for operational excellence in TPRM. Automation, smarter segmentation, due diligence, and monitoring, using internal and external data, ensure oversight is proportionate to risks.

TPRM has potential to enhance performance, especially in mature organisations. These organisations better understand and manage complex risks, reflecting higher optimism among those involved in third-party management. Investment priorities include revisiting TPRM frameworks to ensure they are fit for purpose and adopting human-centric, systems-driven approaches. This highlights the need for top talent to interpret data and drive action.

I recommend tangible actions for organisations to develop the appropriate TPRM capabilities to address supply chain and third-party management challenges. This includes integrating business strategy with risk management, supported by technology, to enhance transparency, reliability, and performance.

Organisations transforming TPRM practices navigate complexities more effectively, becoming more sustainable and resilient. Digital transformation, automation, and smarter segmentation ensure oversight is proportionate to risks, driving operational excellence in TPRM.

Larger and mature organisations, having invested in TPRM over the years, are better equipped to handle interconnected risks. They leverage their resources to address issues like reducing supply chain-related carbon emissions and managing rising energy costs, creating a competitive advantage.

Investing in TPRM capabilities helps organisations navigate complexities and improve resilience. Larger and mature organisations, with their resources and experience, are better positioned to manage third-party risks and leverage them for competitive advantage. Continued focus on technology and data investment remains a top priority for enhancing TPRM practices.

Increasing dependence on third parties makes the cost of falling behind on TPRM maturity higher. Third-party incidents or failures now have a larger impact, leading to potential customer loss, revenue decline, and reputational damage. Regulatory fines and financial losses due to third-party actions are also growing concerns.

Organisations aim to invest in TPRM capabilities to stay robust and agile amid evolving third-party risks. As third-party relationships grow in number and complexity, TPRM teams must adapt to maintain performance.

To address these challenges, organisations should integrate business strategy with risk management, supported by technology. This includes creating

risk-based actionable intelligence and triggers for remedial actions, such as off-boarding high-risk third parties.

Organisations face pressures like managing evolving risks, compliance, and building trust with third parties. They need to produce actionable insights and respond to challenges. Data must be consolidated and analysed across the enterprise, incorporating external sources to clarify dependencies.

Key challenges include the loss of human centricity, evolving risks, lack of alignment with external providers, rapidly changing regulations, and increasing ESG pressure. Geopolitical challenges, multi-year inflation, logistics disruption, supplier overreliance, and economic slowdown are also key challenges.

To balance expectations and capability, organisations should complement in-house capability with external assistance, digitise, and automate processes while retaining a human touch. Increase subcontractor visibility through dialogue and technology, work as a community, aligning data feeds and certifications. Revisit segmentation to focus resources effectively.

There is no one-size-fits-all approach. Organisations must determine their level of risk mitigation to balance evolving risks and expectations. Those optimistic about TPRM are better positioned to achieve this balance, acting as a competitive differentiator.

The optimum state of TPRM is a moving target, with consequences of falling behind being significant. This includes increased costs, inability to meet commitments, and adverse third-party incidents. Understanding complex dependencies is challenging.

Organisations must invest in TPRM capabilities to navigate headwinds and improve resilience. This includes integrating business strategy with risk management, supported by technology, to enhance transparency, reliability, and performance. Investing in TPRM helps organisations manage third-party risks and leverage them for competitive advantage.

Organisations are increasingly supportive of managing ESG risks and opportunities related to third parties, using more quantitative assessments despite data quality concerns. However, many miss synergies between sustainability and resilience initiatives.

Organisations must strategically reposition ESG initiatives with resilience efforts to enhance sustainability and resilience. This includes integrating business strategy with risk management, supported by technology, to improve transparency, reliability, and performance. Investing in TPRM capabilities helps organisations navigate complexities and leverage third-party risks for competitive advantage.

Organisations must integrate business strategy with risk management, supported by technology, to enhance transparency, reliability, and performance. Investing in TPRM capabilities helps navigate complexities and improve resilience. Larger organisations, with more resources, are better positioned to manage third-party risks and leverage them for competitive advantage.

Visibility into subcontractor relationships remains challenging, impacting resilience initiatives. This exposes organisations to hidden concentration risks, which may go undetected until a third-party incident occurs. Organisations must enhance transparency, traceability, and trackability across third-party relationships and subcontractors for informed decision-making and agility.

According to an EY report on Third Party Risk Management, organisations must do better to prepare for third-party risks and ensure ongoing monitoring.[8]

To build a successful TPRM programme and operational resilience, organisations should consider aligning their plans to an existing operational resilience framework, such as the Digital Operational Resilience Act, NIS2 Directive, and the UK Operational Resilience Framework. These frameworks set criteria and expectations for cybersecurity, information technology, third-party dependency management, and business continuity planning and testing. Perform an impact assessment and gap analysis against the currently proposed drafts.

Fully understand, document, and maintain your third-party inventory. Develop policies and procedures. Lack of coordination between internal stakeholders was cited as the biggest pain point for organisations.

While initial due diligence is vital, more robust ongoing monitoring of third parties enables more dynamic risk reporting. Establish a governance structure. Regardless of ownership, TPRM requires input from multiple functions and teams, making well-defined governance crucial. It is recommended to have a consistent global policy with local addendum for multi-jurisdictional organisations.

TPRM programmes that integrate automation and external data providers into the supplier lifecycle and embed cross-functional workflows – e.g., procurement, cyber risk, resiliency – are more effective in managing third-party risk and reporting to senior leadership. More than half of organisations send one aggregated/centralised questionnaire, while others send multiple questionnaires from different risk domains.

Jenkins (2024) emphasises that organisations increasingly rely on third-party vendors, suppliers, and partners to streamline operations, enhance productivity, and drive innovation. Yet, this reliance on external entities also introduces significant cybersecurity risks. Third-party security breaches have become a major concern, as they can potentially expose sensitive data, disrupt operations, and tarnish an organisation's reputation.[9]

Cybercriminals often target third-party vendors as an entry point into an organisation's network, exploiting vulnerabilities in their systems or leveraging their trusted access. Consequently, it is crucial for businesses to implement robust third-party security measures and continuously assess their exposure to potential risks.

Neglecting third-party security can have severe consequences for an organisation. A breach originating from a third-party vendor can lead to data breaches, financial losses, regulatory fines, and reputational damage.

Moreover, the interconnected nature of modern supply chains amplifies the impact of such incidents, as a single breach can ripple through multiple organisations.

Implementing comprehensive third-party security measures is essential for mitigating these risks. This involves conducting thorough due diligence on potential vendors, establishing clear security requirements and contractual obligations, and regularly monitoring and assessing their security posture.

Risk Assessment

Yousaf and Zhou (2024) argue organisations must also prioritise continuous surface risk assessment. This proactive approach involves continuously monitoring and assessing an organisation's entire attack surface, including its own systems, applications, and networks, as well as those of its third-party vendors and partners.[10]

Continuous surface risk assessment enables organisations to identify and address potential vulnerabilities and threats in real time, rather than relying on periodic assessments that may miss emerging risks. By continuously monitoring their attack surface, organisations can stay ahead of evolving cyber threats and respond swiftly to potential breaches or incidents.

Implementing a continuous surface risk assessment strategy offers numerous benefits to organisations. By continuously monitoring the attack surface, organisations can identify potential vulnerabilities and risks before they are exploited by cybercriminals. Continuous monitoring enables organisations to detect and respond to security incidents more quickly, minimising the potential impact and reducing the risk of data breaches or operational disruptions. Many industries and regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), require organisations to implement robust security measures and demonstrate ongoing risk assessment and management. Proactive risk identification and mitigation can help organisations avoid the substantial financial costs associated with data breaches, regulatory fines, and reputational damage. By demonstrating a strong commitment to cybersecurity and continuous risk assessment, organisations can differentiate themselves from competitors and build trust with customers and partners.

Implementing a continuous *surface risk assessment strategy* is important. Organisations must maintain an up-to-date inventory of all their assets, including systems, applications, networks, and third-party connections. This inventory serves as the foundation for continuous monitoring and risk assessment. Leveraging threat intelligence sources, such as security advisories, vulnerability databases, and industry reports, can help organisations stay informed about emerging threats and potential attack vectors.

Regular vulnerability scanning and penetration testing should be conducted across the entire attack surface, including third-party systems and

connections, to identify and prioritise vulnerabilities for remediation. Implementing tools and processes for continuous monitoring of the attack surface enables organisations to detect and respond to potential threats and incidents in real time.

Developing and regularly testing incident response plans ensures that organisations are prepared to respond effectively to security incidents, minimising the potential impact and facilitating swift recovery.

Tools and technologies are very helpful for ensuring third-party security and continuous surface risk assessment. Organisations can leverage vendor risk management platforms. These platforms facilitate the assessment, monitoring, and management of third-party risks, enabling organisations to enforce security requirements, track compliance, and manage vendor relationships.

Automated vulnerability scanning tools can identify and prioritise vulnerabilities across an organisation's systems, applications, and networks, as well as those of third-party vendors. Penetration testing tools simulate real-world attacks and help identify vulnerabilities that may be overlooked by automated scanning tools.

Security information and event management (SIEM) solutions collect and analyse security-related data from various sources, enabling organisations to detect and respond to potential threats and incidents in real time. Threat intelligence platforms provide up-to-date information on emerging threats, vulnerabilities, and attack vectors, enabling organisations to stay informed and proactively address potential risks.

Best practices help make transparent the optimum approach to enhancing cybersecurity measures. Implementing third-party security measures and continuous surface risk assessment is crucial, but it is equally important to follow security best practices to ensure their effectiveness. Set the expectation of at least the same level of security from your third parties and hold them to account on these security measures.

Cultivating a security-conscious culture and mindset throughout the organisation, from top leadership to frontline employees, is essential for effective risk management. Security policies and procedures should be regularly reviewed and updated to reflect changing threats, regulatory requirements, and industry best practices.

Providing ongoing security awareness training. Educating employees on cybersecurity risks, best practices, and their role in maintaining a secure environment is crucial for minimising human-related vulnerabilities. Encouraging collaboration and information sharing within the organisation, as well as with industry partners and relevant authorities, can enhance threat intelligence and improve overall security posture. Periodic risk assessments and security audits should be conducted to evaluate the effectiveness of existing security measures and identify areas for improvement.

Case Studies

Case studies are useful to demonstrate successful third-party security and continuous surface risk assessment. As an experienced CISO I have worked with countless organisations over the years to successfully implement third-party security measures. I can share the impact of implementing security measures and continuous surface risk assessment strategies, demonstrating the benefits of these approaches:

1. *Built Technologies:* A leading fintech implemented a comprehensive vendor risk management programme, including continuous monitoring of third-party systems and connections. This proactive approach enabled the bank to identify and mitigate a potential data breach originating from a vendor's system, preventing significant financial losses and reputational damage.[11]
2. *Chapters Health System:* A large health organisation adopted a continuous surface risk assessment strategy, leveraging automated vulnerability scanning and threat intelligence platforms. This approach helped the organisation identify and address vulnerabilities in its systems and those of its third-party vendors, ensuring compliance with HIPAA regulations and protecting sensitive patient data.[12]
3. *Nexus Technologies:* A leading IT solutions company implemented a robust third-party security programme, including thorough due diligence, security requirements, and continuous monitoring of vendor systems. This approach enabled the company to quickly identify and remediate a vulnerability in a third-party component, preventing potential exploitation and protecting its customers' data and systems.[13]

In today's interconnected business environment, third-party security and continuous surface risk assessment are critical components of an effective cybersecurity strategy. By implementing robust measures to assess and mitigate third-party risks, and continuously monitoring and assessing the entire attack surface, organisations can proactively identify and address potential vulnerabilities and threats.

The key messages are that third-party security breaches pose significant risks to organisations, including data breaches, financial losses, regulatory fines, and reputational damage. Continuous surface risk assessment enables organisations to identify and address potential vulnerabilities and threats in real time, staying ahead of evolving cyber threats. Implementing a continuous surface risk assessment strategy involves maintaining an asset inventory, leveraging threat intelligence, conducting vulnerability scanning, implementing continuous monitoring, and developing incident response plans. Various tools and technologies, such as vendor risk management platforms, vulnerability scanners, penetration testing tools, SIEM solutions,

and threat intelligence platforms, can support third-party security and continuous surface risk assessment efforts. Following best practices, such as fostering a strong security culture, regularly reviewing and updating security policies, providing ongoing security awareness training, encouraging collaboration and information sharing, and conducting regular risk assessments and audits, is essential for enhancing overall cybersecurity measures.

By prioritising third-party security and continuous surface risk assessment, organisations can effectively mitigate risks, protect sensitive data, maintain operational continuity, and build trust with customers and partners.

Cybersecurity is an ongoing journey, and we must remain committed to helping organisations navigate the ever-evolving landscape of cyber threats. Tools and techniques such as third-party security assessments, continuous surface risk monitoring, and cybersecurity controls are important in enhancing your security posture and staying ahead of potential risks.

Notes

1 Tran, D.V., Nguyen, P.V., Le, L.P., and Nguyen, S.T.N., 2024. From Awareness to Behaviour: Understanding Cybersecurity Compliance in Vietnam. *International Journal of Organizational Analysis*. https://www.researchgate.net/publication/380395978_From_awareness_to_behaviour_understanding_cybersecurity_compliance_in_Vietnam.
2 Thakur, M., 2024. Cyber Security Threats and Countermeasures in Digital Age. *Journal of Applied Science and Education (JASE)*, 4(1), pp.1–20.
3 Chaudhary, S., 2024. Driving Behaviour Change with Cybersecurity Awareness. *Computers & Security*, p.103858.
4 Allahham, M., Sharabati, A., Al-Sager, M., Sabra, S., Awartani, L., and Khraim, A., 2024. Supply Chain Risks in the Age of Big Data and Artificial Intelligence: The Role of Risk Alert Tools and Managerial Apprehensions. *Uncertain Supply Chain Management*, 12(1), pp.399–406.
5 Kwong, J., and Pearlson, K., 2024. Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs, pp. 6656–6664. https://scholarspace.manoa.hawaii.edu/items/993cbf7f-45b8-456f-b707-a84cbdec8a56.
6 https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-global-tprm-survey-report-2023.pdf.
7 Chukwu, N., Yufenyuy, S., Ejiofor, E., Ekweli, D., Ogunleye, O., Clement, T., Obunadike, C., Adeniji, S., Elom, E., and Obunadike, C., 2024. Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration. *Int. J. Sci. Manag. Res*, 7(3), pp.46–65.
8 https://www.ey.com/en_gl/insights/risk/2023-ey-global-third-party-risk-management-survey.
9 Jenkins, S., 2024. Cybersecurity Threats Prompt Proactive Approach. *Chemical Engineering*, 131(1).
10 Yousaf, A., and Zhou, J., 2024. From Sinking to Saving: MITRE ATT &CK and D3FEND Frameworks for Maritime Cybersecurity. *International Journal of Information Security*, 23(3), pp.1603–1618.
11 https://www.upguard.com/customers/built-technologies.
12 https://www.upguard.com/customers/chapters-health-system.
13 https://www.upguard.com/customers/nexus-technologies.

11

INVENTORY MANAGEMENT, THREAT INTELLIGENCE, AND MONITORING

Asset Inventory Management

Oyedokun and Campbell (2023) contend that in today's digital landscape, where businesses heavily rely on technology and data, effective asset inventory management has become a critical component for ensuring operational efficiency, cybersecurity, and successful supplier relationships.[1]

Faulk Jr (2024) argues executive leaders often complain they don't receive reliable or consistent information over IT asset management yet there is significance in maintaining an accurate and up-to-date inventory of an organisation's assets, including hardware, software, and digital resources.[2]

Asset inventory management is the process of identifying, tracking, and managing an organisation's assets throughout their lifecycle. It involves cataloguing all assets, monitoring their usage, and ensuring their proper maintenance and disposal. Olivero (2022) argues automating identification using asset discovering tools is a good way to support cybersecurity.[3]

Kotenko et al. (2022) argue the case for automation in asset inventory management. By implementing a robust asset inventory management strategy, organisations can gain better control over their assets, mitigate risks, and optimise resource allocation.[4]

We must delve into the importance of effective asset inventory management, and its role in cybersecurity and supplier relationships, and explore best practices and tools for successful implementation.

The role of asset inventory management in cybersecurity should not be underestimated. Cybersecurity is a paramount concern for organisations of all sizes and across all industries. Effective asset inventory management plays a crucial role in maintaining a strong cybersecurity posture by providing visibility into an organisation's digital assets and their potential vulnerabilities.

DOI: 10.4324/9781003604969-11

Yaseen (2024) puts forward the case for greater automation as without a comprehensive asset inventory, organisations may overlook critical software updates or patch management, or fail to identify and address potential entry points for cyber threats. An accurate inventory enables organisations to identify and prioritise assets based on their criticality, ensuring that the most sensitive and valuable assets receive the necessary security measures and resources.[5]

Furthermore, asset inventory management facilitates the implementation of access controls and data protection measures. By maintaining a detailed inventory of authorised users and their respective access levels, organisations can prevent unauthorised access to sensitive data and systems, reducing the risk of data breaches and cyber attacks.

In today's interconnected business environment, organisations often rely on third-party suppliers and vendors to provide various products and services. Effective asset inventory management is crucial for maintaining strong supplier relationships and ensuring compliance with contractual obligations.

By having a comprehensive inventory of assets, organisations can accurately track and manage licences, subscriptions, and maintenance agreements with suppliers. This transparency not only ensures compliance with licensing terms but also facilitates better budgeting and resource allocation for software and hardware renewals or upgrades.

Moreover, asset inventory management enables organisations to monitor and validate the performance of supplier-provided assets, ensuring that they meet the agreed-upon service levels and specifications. This accountability fosters trust and strengthens the relationship between organisations and their suppliers, leading to more productive and mutually beneficial collaborations.

Common challenges in asset inventory management make achieving this tricky. While the benefits of effective asset inventory management are undeniable, organisations often face several challenges in implementing and maintaining a robust inventory management system.

Ensuring that asset inventory data is accurate, up to date, and complete can be a daunting task, especially in large and complex organisations with numerous assets distributed across multiple locations. Tracking assets throughout their entire lifecycle, from procurement to disposal, can be challenging, particularly when assets are frequently moved, upgraded, or decommissioned.

In organisations with decentralised operations or multiple departments, maintaining a centralised and consistent asset inventory can be difficult due to siloed data and lack of coordination. Implementing and maintaining an effective asset inventory management system often requires dedicated resources, including personnel, software tools, and infrastructure, which can be a challenge for organisations with limited budgets or staffing constraints. Integrating asset inventory management systems with existing IT infrastructure, databases, and other systems can be complex, requiring significant effort and expertise.

Develop and implement well-defined policies and procedures for asset inventory management, including guidelines for asset acquisition, tracking, maintenance, and disposal. These policies should be communicated and enforced across the organisation. Maintain a centralised and consolidated asset inventory database to ensure data consistency, accuracy, and accessibility. This centralised repository should serve as a single source of truth for all asset-related information.

Leverage automated asset discovery and tracking tools to streamline the process of identifying and cataloguing assets across the organisation. These tools can help reduce manual effort and improve data accuracy. Integrate the asset inventory management system with other relevant systems, such as IT service management (ITSM), configuration management databases (CMDBs), and financial systems, to ensure data consistency and enable seamless information exchange.

Define clear roles and responsibilities for asset inventory management within the organisation. Designate asset owners, custodians, and stakeholders responsible for maintaining and updating asset information. Perform regular audits and reconciliations to verify the accuracy and completeness of asset inventory data. This process should involve physical inspections, software licence audits, and data validation against other systems.

Implement training programmes and awareness campaigns to educate employees on the importance of asset inventory management and their roles and responsibilities in maintaining accurate asset data.

Tools and technologies are available for asset inventory management. Asset inventory management software solutions designed to manage and track assets throughout their life cycle. These tools typically offer features such as asset discovery, cataloguing, reporting, and integration with other systems.

Asset tracking and barcoding systems are crucial. Physical asset tracking systems use barcodes, RFID tags, or other identification methods to track the location and movement of assets within an organisation.

Centralised repositories that store and manage information about IT assets, configurations, and their relationships, CMDBs can be integrated with asset inventory management systems to provide a comprehensive view of an organisation's IT infrastructure.

Cloud-based platforms offer asset inventory management capabilities, often with scalable and flexible deployment options, and the ability to access asset data from anywhere. Mobile applications enable field technicians or remote employees to scan and update asset information on the go, improving data accuracy and real-time visibility.

Automated asset discovery tools can automatically discover and catalogue IT assets across an organisation's network, reducing manual effort and improving data completeness.

Developing an effective asset inventory management strategy requires a structured approach and careful planning. Clearly define the objectives and

scope of the asset inventory management initiative. Determine which asset types (hardware, software, digital resources) and organisational units or locations will be included in the inventory. Perform a baseline assessment to understand the current state of asset inventory management within the organisation. Identify existing processes, tools, and data sources, as well as gaps and areas for improvement.

Establish comprehensive policies and procedures for asset inventory management, covering areas such as asset acquisition, tracking, maintenance, disposal, and data governance. Evaluate and select the appropriate tools and technologies to support asset inventory management based on the organisation's requirements, budget, and existing infrastructure.

Clearly define the roles and responsibilities of stakeholders involved in asset inventory management, including asset owners, custodians, IT staff, and management. Ensure that the asset inventory management system integrates seamlessly with other relevant systems, such as ITSM, CMDBs, and financial systems, to facilitate data exchange and consistency.

Create training programmes and communication plans to educate employees on the importance of asset inventory management and their roles and responsibilities in maintaining accurate asset data. Define key performance indicators (KPIs) and establish regular reporting mechanisms to monitor the effectiveness of asset inventory management and identify areas for improvement. Establish processes for continuous improvement, including regular audits, data validation, and process optimisation, to ensure the asset inventory management strategy remains effective and aligned with organisational objectives.

Case Studies

Case studies help to illustrate the benefits and practical applications of effective asset inventory management. We can explore a few real-world case studies:

Khaleeji Bank: A bank implemented a comprehensive asset inventory management system to gain better control over its IT assets and ensure compliance with regulatory requirements. By centralising asset data and integrating with their ITSM and CMDB systems, the bank achieved significant cost savings through optimised software licensing, improved security posture, and streamlined IT operations.[6]

Gloucestershire Hospitals NHS Foundation Trust: A health organisation faced challenges in managing its diverse range of medical equipment and devices across multiple facilities. By implementing an asset tracking system with barcoding and RFID technology, the organisation was able to accurately track the location and maintenance schedules of critical medical assets, improving patient safety and reducing equipment downtime.[7]

Wacom: A manufacturing company struggled with managing accurate asset inventory that included core systems, all its platforms, and users across

any network. By implementing an automated asset discovery and inventory management solution, the company gained visibility into its software assets, enabling accurate licence tracking and optimised software procurement and deployment.[8]

These case studies demonstrate the real-world impact of effective asset inventory management on various aspects of an organisation, including cost savings, compliance, security, and operational efficiency.

As technology continues to evolve and organisations become increasingly reliant on digital assets, the importance of effective asset inventory management will only continue to grow. In the context of cybersecurity and supplier relationships, several key trends and developments are shaping the future of asset inventory management.

Increased adoption of Internet of Things (IoT) devices in both consumer and industrial settings means organisations will need to adapt their asset inventory management strategies to account for these connected devices, ensuring proper security measures and lifecycle management.

AI and ML technologies are expected to play a significant role in enhancing asset inventory management by enabling automated asset discovery, predictive maintenance, and intelligent decision-making based on asset data analysis.

As cyber threats continue to evolve, asset inventory management will become increasingly critical for identifying and mitigating potential vulnerabilities, enabling organisations to prioritise security measures and allocate resources effectively.

Stricter regulations and compliance standards, particularly in industries such as healthcare, finance, and critical infrastructure, will drive the need for more robust and auditable asset inventory management practices.

The growing adoption of cloud-based and managed services will necessitate new approaches to asset inventory management, ensuring visibility and control over assets hosted and managed by third-party providers.

As organisations become more reliant on third-party suppliers and vendors, effective asset inventory management will play a crucial role in supplier risk management, enabling organisations to monitor and validate the performance and security of supplier-provided assets.

To stay ahead of these trends and meet the evolving demands of cybersecurity and supplier relationships, organisations must continuously adapt and enhance their asset inventory management strategies, leveraging emerging technologies, best practices, and industry standards.

Effective asset inventory management is a critical component of modern business operations, playing a vital role in ensuring cybersecurity, maintaining strong supplier relationships, and driving operational efficiency. By implementing robust asset inventory management practices, organisations can gain visibility and control over their assets, mitigate risks, optimise resource allocation, and foster trust and accountability with suppliers and partners.

As we navigate an increasingly complex and interconnected digital landscape, the importance of asset inventory management will only continue to grow. Organisations that prioritise effective asset inventory management will be better positioned to protect their valuable assets, maintain a strong cybersecurity posture, and cultivate successful and mutually beneficial supplier relationships.

Threat Intelligence

Threat intelligence is a powerful tool in this endeavour, enabling organisations to proactively identify, analyse, and respond to potential threats before they can cause significant harm. In the ever-evolving landscape of cybersecurity, businesses face an array of threats that can potentially compromise their operations, data, and reputation.

Rasel et al. (2024) argue that in threat intelligence sharing between key parties in the supply chain, one area of particular concern is the potential for cybersecurity threats originating from suppliers and third-party vendors. As companies increasingly rely on external partners for various services and products, it becomes crucial to implement robust measures to mitigate the risks associated with these relationships.[9]

Sarker (2024) contends that by leveraging AI and automation in threat intelligence, businesses and others in their supply chain can gain invaluable insights into the tactics, techniques, and procedures employed by cyber adversaries, empowering them to fortify their defences and safeguard their critical assets.[10]

Ampel et al. (2024) insist that a proactive approach is vital to understand the intricacies of threat intelligence and its vital role in protecting businesses against cybersecurity threats emanating from suppliers.[11]

We will explore the key components of an effective threat intelligence programme, best practices for implementation, and real-world case studies that illustrate the tangible benefits of embracing this strategic approach.

Zacharis et al. (2024) argue AI-driven threat intelligence and forecasting can help speed up and improve cybersecurity and that understanding cybersecurity threats from suppliers is crucial.[12]

Suppliers and third-party vendors play a crucial role in the modern business ecosystem, providing essential goods and services that enable companies to operate efficiently and competitively. However, this interdependence also introduces potential vulnerabilities that cybercriminals may exploit to gain unauthorised access to sensitive information or disrupt operations.

Cybersecurity threats from suppliers can manifest in various forms. Supply chain attacks mean that malicious actors may infiltrate the supply chain by compromising software, hardware, or firmware components, enabling them to gain a foothold within the target organisation. Inadequate security measures or negligence on the part of suppliers can lead to data breaches,

exposing sensitive information such as customer records, intellectual property, or financial data.

Insider threats are an ever-present risk. Disgruntled or malicious employees within supplier organisations may intentionally or unintentionally compromise the security of their partners' systems and data. Suppliers may inadvertently introduce malware or facilitate phishing attacks, providing cybercriminals with a potential entry point into the target organisation's network.

Failure to adhere to industry-specific regulations and standards by suppliers can expose businesses to legal and financial risks, as well as reputational damage. Recognising these potential threats is the first step towards implementing effective countermeasures and minimising the impact of cybersecurity incidents originating from suppliers.

Safeguarding your business against cybersecurity threats is a paramount concern. The consequences of falling victim to cybersecurity threats from suppliers can be severe and far-reaching. Beyond the immediate financial losses and operational disruptions, businesses may face long-term reputational damage, loss of customer trust, and regulatory penalties. In some cases, the ramifications can even extend to legal liabilities and potential lawsuits.

Safeguarding your business against these threats is not only a matter of risk mitigation but also a strategic imperative for maintaining a competitive edge. By proactively addressing cybersecurity vulnerabilities and implementing robust security measures, businesses can safeguard valuable intellectual property, customer information, and other sensitive data from unauthorised access or theft. Minimise the risk of operational disruptions caused by cyber attacks, ensuring uninterrupted service delivery and productivity. Demonstrate a commitment to data privacy and security, fostering customer confidence and loyalty. They can adhere to industry-specific regulations and standards, avoiding costly penalties and legal consequences. Protect the company's brand and reputation, which can be severely impacted by high-profile cybersecurity incidents.

By implementing robust cybersecurity measures and leveraging threat intelligence, businesses can proactively identify and mitigate potential risks, ensuring the protection of their critical assets and maintaining a competitive advantage in the market.

Threat intelligence plays a pivotal role in safeguarding businesses against cybersecurity threats originating from suppliers. By leveraging this strategic approach, organisations can gain valuable insights into the tactics, techniques, and procedures employed by cyber adversaries, enabling them to stay ahead of emerging threats and implement effective countermeasures.

Threat intelligence can help protect your business. Threat intelligence enables organisations to identify and monitor potential threats in real time, providing early warning signals and allowing for proactive mitigation efforts. By analysing threat data and intelligence, businesses can identify

vulnerabilities within their systems, supply chain, or third-party vendor relationships, enabling them to prioritise and address these weaknesses before they can be exploited. In the event of a cybersecurity incident, threat intelligence can provide valuable insights into the nature of the attack, its potential impact, and effective mitigation strategies, enabling a more rapid and targeted response.

By assessing the likelihood and potential impact of various threats, businesses can prioritise their security efforts and allocate resources more effectively, ensuring that critical areas are adequately protected. Threat intelligence can aid in evaluating the cybersecurity posture of suppliers and third-party vendors, enabling businesses to make informed decisions about partnerships and implement appropriate risk mitigation measures. Leveraging threat intelligence can help organisations demonstrate compliance with industry-specific regulations and standards, minimising the risk of penalties and legal consequences.

By incorporating threat intelligence into their cybersecurity strategy, businesses can gain a comprehensive understanding of the threat landscape, enabling them to proactively identify and mitigate potential risks, and ultimately safeguard their operations, data, and reputation.

Implementing an effective *threat intelligence programme* requires a holistic approach that encompasses various key components. These components work in tandem to ensure the efficient collection, analysis, and dissemination of threat intelligence, enabling organisations to make informed decisions and take appropriate actions.

The foundation of any threat intelligence programme lies in the ability to collect and integrate data from diverse sources, including open-source intelligence (OSINT), proprietary threat feeds, security logs, and industry-specific repositories.

Collected data must be analysed and contextualised to derive meaningful insights and identify potential threats. This process involves leveraging advanced analytical techniques, such as machine learning and natural language processing, to identify patterns, correlations, and emerging trends.

Based on the analysed intelligence, organisations can develop threat models and conduct risk assessments to understand the potential impact of identified threats on their operations, assets, and supply chain.

Continuous monitoring and detection mechanisms are essential to identify and respond to emerging threats in real time. This may involve deploying specialised tools and technologies, such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), and advanced threat hunting capabilities.

When a threat is detected, organisations must have well-defined incident response and mitigation processes in place. This includes developing playbooks, establishing communication channels, and implementing appropriate countermeasures to contain and neutralise the threat.

Collaboration and information sharing: Effective threat intelligence relies on collaboration and information sharing within the cybersecurity community. Participating in industry-specific forums, sharing threat data, and leveraging collective intelligence can significantly enhance an organisation's ability to identify and respond to emerging threats.

Threat landscapes are constantly evolving, necessitating a commitment to continuous improvement and adaptation within the threat intelligence programme. Regular reviews, assessments, and updates are crucial to ensure the programme remains relevant and effective in addressing emerging threats.

By integrating these key components into a cohesive threat intelligence programme, organisations can establish a robust cybersecurity posture, enabling them to proactively identify and mitigate potential threats originating from suppliers and other sources.

Implementing an effective threat intelligence programme within your business requires a strategic and structured approach. Begin by clearly defining the objectives and scope of your threat intelligence programme. Identify the critical assets, processes, and supply chain relationships that require protection, and align your programme's goals with your organisation's overall cybersecurity strategy.

Conduct a comprehensive assessment of your organisation's current cybersecurity capabilities, including existing tools, processes, and personnel. Identify gaps and areas for improvement to determine the resources and investments required for an effective threat intelligence programme. Assemble a dedicated team of cybersecurity professionals with expertise in threat intelligence, analysis, and incident response. This team will be responsible for driving the programme's implementation, monitoring, and continuous improvement.

Identify relevant data sources, both internal and external, and establish mechanisms for data collection and integration. This may involve leveraging existing security tools, subscribing to threat intelligence feeds, or partnering with industry-specific information-sharing communities.

Invest in advanced analytical tools and develop robust processes for data analysis and threat modelling. This may involve leveraging machine learning, natural language processing, and other advanced techniques to derive meaningful insights from the collected data.

Deploy specialised tools and technologies for continuous threat monitoring and detection. This may include implementing SIEM systems, IDS/IPS, and advanced threat hunting capabilities.

Create detailed incident response and mitigation playbooks that outline the steps to be taken in the event of a cybersecurity incident. These playbooks should be regularly reviewed and updated to ensure their effectiveness and alignment with evolving threats.

Encourage collaboration and information sharing within your organisation, as well as with industry peers and relevant cybersecurity communities.

Participate in threat intelligence-sharing initiatives and leverage collective knowledge to enhance your programme's effectiveness.

Establish processes for regular reviews, assessments, and updates to your threat intelligence programme. Continuously evaluate its effectiveness, identify areas for improvement, and adapt to emerging threats and evolving best practices.

Invest in comprehensive training and awareness programmes to ensure that all relevant stakeholders, including employees, suppliers, and third-party vendors, understand the importance of threat intelligence and their roles in maintaining a robust cybersecurity posture.

By following these steps and implementing a comprehensive threat intelligence programme, your business can proactively identify and mitigate potential cybersecurity threats originating from suppliers, safeguarding your critical assets, operations, and reputation.

Effective utilisation of threat intelligence requires adherence to industry best practices to ensure maximum impact and return on investment. Define clear roles and responsibilities within your threat intelligence team and across relevant stakeholders. Ensure that everyone understands their specific tasks, responsibilities, and lines of communication.

Prioritise threat intelligence based on the potential risk and impact to your organisation. Focus your efforts on addressing high-risk threats that could significantly disrupt operations, compromise sensitive data, or damage your reputation. Leverage automation and machine learning techniques to streamline data collection, analysis, and threat detection processes. This can help reduce manual effort, improve efficiency, and enhance the accuracy of threat identification.

Integrate threat intelligence into your existing security processes and tools, such as SIEM systems, IDS/IPS, and vulnerability management programmes. This enables a more comprehensive and coordinated approach to threat mitigation. Encourage cross-functional collaboration between your threat intelligence team, security operations centre (SOC), incident response team, and other relevant stakeholders. This collaboration ensures effective communication, coordinated response efforts, and a holistic approach to cybersecurity.

Continuously monitor and update your threat intelligence sources to ensure you have access to the latest and most relevant information. Stay informed about emerging threats, new attack vectors, and evolving tactics employed by cyber adversaries. Implement robust access controls and data protection measures to safeguard your threat intelligence data and systems. Ensure that only authorised personnel can access and modify sensitive information, and implement encryption and secure communication protocols.

Conduct regular assessments and audits of your threat intelligence programme to evaluate its effectiveness, identify areas for improvement, and ensure compliance with industry standards and regulations. Participate in

industry-specific threat intelligence-sharing initiatives and collaborate with peers, security researchers, and relevant organisations. This collaborative approach can enhance your understanding of emerging threats and facilitate the development of effective countermeasures.

Provide ongoing training and education to your threat intelligence team, as well as relevant stakeholders across the organisation. Ensure that everyone understands the importance of threat intelligence, their roles and responsibilities, and the latest best practices and techniques.

By adhering to these best practices, your organisation can maximise the effectiveness of your threat intelligence programme, enabling proactive identification and mitigation of cybersecurity threats originating from suppliers and other sources.

Case Studies

Case studies can help bring to life the importance of threat intelligence to protect against supplier threats. To better understand the practical application of threat intelligence in safeguarding businesses against cybersecurity threats from suppliers, let's explore some real-life case studies:

Case Study 1: Lasselsberger[13]

A leading supplier of building materials faced significant supply chain risk. By leveraging their threat intelligence programme, they were able to ensure they could quickly identify threats and take proactive measures. They analysed potential attack patterns, identified indicators of compromise (IoCs), and implemented targeted security controls to prevent threats from propagating into their systems.

Additionally, the threat intelligence team collaborate with the supplier to share relevant information and can assist in incident response efforts. This coordinated approach enables them to contain a breach and mitigate the risk of further damage.

Through their proactive threat intelligence efforts, the building materials supplier was able to effectively protect their operations, safeguard sensitive data, and maintain business continuity without significant disruptions.

Case Study 2: Gorillas[14]

A grocery delivery service provider recognised the importance of protecting customer data and maintaining compliance. They implemented a robust threat intelligence programme to monitor potential threats. Through continuous monitoring and analysis of threat data, the threat intelligence team identified potential vulnerabilities. They promptly worked collaboratively to address any issue before it could be exploited by malicious actors.

The threat intelligence programme enabled them to assess the cybersecurity posture. This allowed them to make informed decisions and implement appropriate risk mitigation measures, ensuring the protection of sensitive data and compliance with regulatory requirements.

Case Study 3: Mercury Financial[15]

A financial organisation recognised the significant risks posed by cybersecurity threats originating from suppliers and third-party vendors. They invested in a comprehensive threat intelligence programme to proactively identify and mitigate these risks.

Through their threat intelligence efforts, the financial organisation uncovered potential threats targeting their employees and contractors. This proactive approach and effective utilisation of threat intelligence enabled them to mitigate the potential impact of phishing campaigns, protect customer data, and maintain the integrity of their financial systems and operations.

These case studies illustrate the real-world benefits of implementing a robust threat intelligence programme and the critical role it plays in safeguarding businesses against cybersecurity threats originating from suppliers and third-party vendors.

Tools and resources are available for threat intelligence. Effective threat intelligence requires access to the right tools and resources to collect, analyse, and disseminate relevant information.

Specialised threat intelligence platforms, such as ThreatConnect, ThreatQuotient, and Recorded Future, provide centralised repositories for collecting, analysing, and sharing threat data from various sources.

Security information and event management (SIEM) solutions, like Splunk, QRadar, and LogRhythm, enable the collection, correlation, and analysis of security logs and events, providing valuable insights for threat detection and response.

Subscribing to threat intelligence feeds from reputable sources, such as AlienVault OTX, Emerging Threats, and Abuse.ch, can provide up-to-date information on emerging threats, indicators of compromise (IoCs), and threat actor activities.

Open-source intelligence (OSINT) tools like Maltego, Shodan, and Censys enable the collection and analysis of publicly available data, including social media, forums, and online repositories, to uncover potential threats and vulnerabilities.

Vulnerability scanners like Nessus, Qualys, and Rapid7 InsightVM can help identify and assess vulnerabilities within your organisation's systems and those of your suppliers, enabling proactive mitigation efforts.

Advanced threat hunting platforms, such as Sqrrl, Cyphon, and Huntress, leverage machine learning and behavioural analytics to detect and respond to sophisticated threats that may evade traditional security controls.

Incident response and forensics tools like EnCase, FTK, and Volatility can assist in incident response and forensic analysis, enabling thorough investigation and remediation of cybersecurity incidents.

Joining industry-specific information sharing and analysis centres (ISACs), such as the Financial Services ISAC (FS-ISAC) or the Health Information Sharing and Analysis Centre (H-ISAC), can provide access to valuable threat intelligence and facilitate collaboration with peers.

Adhering to industry-recognised frameworks and standards, such as the NIST Cybersecurity Framework, ISO 27001, and the CIS Critical Security Controls, can help ensure a comprehensive and structured approach to threat intelligence and cybersecurity management.

Investing in professional training and certifications, such as the Certified Threat Intelligence Analyst (C|TIA) or the GIAC Cyber Threat Intelligence (GCTI) certification, can enhance the skills and knowledge of your threat intelligence team.

By leveraging these tools and resources, your organisation can effectively collect, analyse, and disseminate threat intelligence, enabling proactive identification and mitigation of cybersecurity threats originating from suppliers and other sources.

Safeguarding your business against cybersecurity threats from suppliers is a critical endeavour in today's interconnected world. Don't wait until it's too late – take action now to protect your critical assets, operations, and reputation.

As the cybersecurity landscape continues to evolve, the importance of threat intelligence in safeguarding businesses against threats from suppliers and other sources will only continue to grow. The future of threat intelligence lies in its ability to adapt to emerging challenges and leverage cutting-edge technologies to stay ahead of cyber adversaries.

One of the key trends shaping the future of threat intelligence is the integration of artificial intelligence (AI) and machine learning (ML) capabilities. These technologies can enhance the speed and accuracy of threat detection, enabling real-time analysis of vast amounts of data and identifying previously unknown patterns and anomalies.

Additionally, the rise of cloud computing and the Internet of Things (IoT) will necessitate the development of specialised threat intelligence solutions tailored to these environments. As businesses increasingly adopt cloud services and interconnected devices, ensuring the security of these platforms and safeguarding against potential threats will become paramount.

Furthermore, the future of threat intelligence will likely involve increased collaboration and information sharing among organisations, industries, and even nations. By fostering a culture of collective intelligence and leveraging shared resources, businesses can gain a more comprehensive understanding of the global threat landscape and develop more effective countermeasures.

Moreover, the integration of threat intelligence with other cybersecurity disciplines, such as incident response, vulnerability management, and risk

assessment, will become increasingly seamless. This holistic approach will enable organisations to proactively identify and mitigate threats while also enhancing their overall cybersecurity posture.

Supply chains have become increasingly complex, spanning multiple organisations and geographical boundaries. As a result, the attack surface – the sum of all potential entry points for cyber threats – has expanded significantly.

Amoo et al. (2024) argue the rise of IoT and higher levels of working from home since the pandemic have contributed to the attack surface, as have emerging threats. Cybersecurity in the supply chain is a critical concern, as a breach at any point can have far-reaching consequences, compromising sensitive data, disrupting operations, and eroding customer trust.[16]

We live in an era where cyber threats are constantly evolving, and attackers are becoming more sophisticated in their methods. Supply chains, with their intricate web of interconnected systems and third-party dependencies, are particularly vulnerable to these threats.

Continuous Monitoring

Attack surface monitoring is the process of continuously identifying, assessing, and mitigating potential vulnerabilities and exposures that could be exploited by cyber adversaries. It involves mapping and analysing the entire attack surface, including hardware, software, networks, data, and human elements, to detect and address potential weaknesses before they can be exploited.

Osazuwa and Musa (2024) contend that we have an ever-expanding attack surface and security operations need to use emerging technologies as part of their attack surface monitoring if they are to maintain adequate control. A single weak link in the chain can expose the entire ecosystem to cyber risks, making it imperative for organisations to adopt a proactive and continuous approach to monitoring their attack surface.[17]

In the context of supply chains, attack surface monitoring is particularly crucial due to the numerous interconnections and dependencies involved. It enables organisations to gain visibility into the cyber risks posed by their suppliers, partners, and third-party vendors, as well as their own internal systems and processes.

The importance of *continuous attack surface monitoring* cannot be overstated. Continuous attack surface monitoring is essential. Cyber threats are constantly evolving, and new vulnerabilities are discovered regularly. Continuous monitoring ensures that organisations can quickly identify and respond to emerging threats, minimising the risk of successful attacks.

Supply chains are not static entities; they are dynamic, with new partners, technologies, and processes being introduced regularly. Continuous monitoring allows organisations to adapt to these changes and maintain an up-to-

date understanding of their attack surface. Many industries have stringent cybersecurity regulations and compliance requirements. Continuous attack surface monitoring helps organisations demonstrate their commitment to cybersecurity and meet these regulatory obligations.

By continuously monitoring their attack surface, organisations can proactively identify and mitigate potential risks before they can be exploited by cyber adversaries, reducing the likelihood and impact of successful attacks.

Implementing continuous attack surface monitoring in the supply chain offers numerous benefits:

Continuous monitoring provides organisations with a comprehensive view of their attack surface, including all interconnected systems, third-party dependencies, and potential vulnerabilities. This visibility enables better decision-making and more effective risk management.

By continuously identifying and addressing vulnerabilities, organisations can strengthen their overall security posture, reducing the risk of successful cyber attacks and data breaches.

Continuous monitoring allows organisations to assess and manage the cyber risks posed by their suppliers and third-party vendors, enabling them to take appropriate measures to mitigate potential threats.

In the event of a cyber attack, continuous monitoring can aid in rapid incident response and recovery efforts by providing valuable insights into the nature and scope of the attack, as well as potential entry points and affected systems.

Many industries have strict cybersecurity regulations and compliance requirements. Continuous attack surface monitoring can help organisations demonstrate their commitment to cybersecurity and meet these regulatory obligations.

By proactively identifying and addressing vulnerabilities, organisations can potentially avoid the significant financial and reputational costs associated with successful cyber attacks and data breaches.

While continuous attack surface monitoring offers numerous benefits, it also presents several challenges and limitations. Supply chains can be highly complex, involving numerous interconnected systems, technologies, and third-party dependencies. Monitoring the entire attack surface in such an environment can be a daunting task, requiring significant resources and expertise.

Continuous monitoring generates a vast amount of data, which needs to be effectively managed, analysed, and acted upon. Organisations may struggle with data overload, making it difficult to identify and prioritise critical vulnerabilities.

Automated monitoring tools can sometimes generate false positives, leading to unnecessary investigations and wasted resources. Finding the right balance between sensitivity and specificity is crucial.

Implementing and maintaining an effective continuous attack surface monitoring programme requires skilled cybersecurity professionals with specialised knowledge and expertise. Attracting and retaining such talent can be a challenge for many organisations.

Integrating monitoring tools and processes with existing systems and workflows can be complex, particularly in heterogeneous environments with legacy systems and multiple vendors.

Effective attack surface monitoring in the supply chain requires cooperation and information sharing among all parties involved, including suppliers and third-party vendors. Ensuring this level of collaboration can be challenging, particularly when dealing with smaller or less mature organisations.

Develop a well-defined strategy that outlines the scope, objectives, and processes for continuous attack surface monitoring, ensuring alignment with the organisation's overall cybersecurity and risk management goals.

Implement automated tools and solutions to streamline the monitoring process, reduce manual efforts, and improve efficiency. Automation can help organisations keep pace with the ever-changing threat landscape and the dynamic nature of supply chains.

Establish a risk-based approach to prioritising vulnerabilities based on factors such as criticality, likelihood of exploitation, and potential impact. This will help organisations allocate resources effectively and address the most pressing threats first.

Encourage collaboration and information sharing among all stakeholders in the supply chain, including suppliers, partners, and third-party vendors. This can help identify and address potential vulnerabilities more effectively.

Regularly review and update the attack surface monitoring programme to ensure it remains effective and aligned with evolving threats, technologies, and business requirements. Continuously seek opportunities for improvement and incorporate lessons learned from past incidents or exercises.

Ensure that the continuous attack surface monitoring programme is tightly integrated with the organisation's incident response and recovery plans. This will enable a more coordinated and effective response in the event of a cyber attack or data breach.

Invest in ongoing training and awareness programmes for employees, suppliers, and partners to promote a strong cybersecurity culture and ensure that everyone understands their role in maintaining a secure attack surface.

Continuous attack surface monitoring relies on a range of tools and technologies to identify, assess, and mitigate potential vulnerabilities. Some of the commonly used tools and technologies include:

Vulnerability scanners scan systems, networks, and applications for known vulnerabilities and misconfigurations, providing insights into potential entry points for cyber attacks. Penetration testing tools simulate real-world cyber attacks to identify vulnerabilities and weaknesses in an organisation's defences. These tools can be used to assess the effectiveness of existing security controls and identify areas for improvement.

SIEM solutions collect and analyse security-related data from various sources, including network devices, servers, and applications. This data can be used to detect potential threats, identify vulnerabilities, and support

incident response efforts. Threat intelligence platforms provide up-to-date information on emerging cyber threats, vulnerabilities, and attack vectors. This information can be used to proactively identify and mitigate potential risks.

As more organisations adopt cloud services, cloud security monitoring tools have become essential for monitoring the attack surface in cloud environments. These tools provide visibility into cloud infrastructure, applications, and data, helping to identify potential vulnerabilities and misconfigurations.

With the proliferation of IoT devices in supply chains, IoT security solutions are necessary to monitor and secure these devices, which can often be overlooked and represent potential entry points for cyber attacks.

Third-party risk management platforms help organisations assess and manage the cyber risks posed by their suppliers, partners, and other third-party vendors. They provide visibility into the security posture of these third parties and enable continuous monitoring of their attack surface.

It's important to note that no single tool or technology can provide complete protection against cyber threats. A comprehensive approach that combines multiple tools and technologies, along with robust processes and skilled personnel, is essential for effective continuous attack surface monitoring.

Case Studies

As an experienced CISO I have helped countless organisations to successfully implement continuous attack surface monitoring in their supply chains, resulting in improved cybersecurity and reduced risks. While keeping them anonymous here are a few case studies that highlight the benefits of this approach:

Global automotive manufacturer: A leading automotive manufacturer implemented a continuous attack surface monitoring programme to gain visibility into the cyber risks posed by its vast network of suppliers and third-party vendors. By continuously monitoring and assessing the security posture of these partners, the company was able to identify and address numerous vulnerabilities, preventing potential cyber attacks and data breaches. This proactive approach not only strengthened the company's cybersecurity but also helped maintain compliance with industry regulations and standards.

Healthcare supply chain: A major health organisation recognised the importance of securing its supply chain, which involved sensitive patient data and critical medical devices. By implementing continuous attack surface monitoring, the organisation was able to identify and mitigate vulnerabilities in its network infrastructure, medical devices, and third-party software applications. This proactive approach helped protect patient data and ensure the integrity and availability of critical healthcare systems.

Retail supply chain: A large retail company with a complex global supply chain implemented continuous attack surface monitoring to gain visibility

into the cyber risks posed by its suppliers, logistics partners, and e-commerce platforms. By continuously monitoring and assessing the security posture of these interconnected systems, the company was able to identify and address potential vulnerabilities before they could be exploited by cyber criminals. This proactive approach helped protect customer data, maintain business continuity, and preserve the company's reputation.

These case studies demonstrate the real-world benefits of continuous attack surface monitoring in the supply chain, including improved cybersecurity, reduced risk of cyber attacks and data breaches, and enhanced compliance with industry regulations and standards.

As the threat landscape continues to evolve and supply chains become increasingly complex, continuous attack surface monitoring will remain a critical aspect of cybersecurity.

Advances in automation and machine learning technologies will enable more efficient and effective continuous monitoring processes. Machine learning algorithms can analyse vast amounts of data to identify patterns and anomalies, helping organisations prioritise and respond to potential threats more effectively.

Continuous attack surface monitoring will become more tightly integrated with DevOps and Agile methodologies, ensuring that cybersecurity is considered throughout the entire software development lifecycle and supply chain.

As organisations embrace the principles of the Zero Trust security model, continuous attack surface monitoring will play a crucial role in verifying and continuously monitoring the security posture of all systems, users, and devices, regardless of their location or ownership.

With the growing recognition of supply chain risks, continuous attack surface monitoring will become an integral part of broader supply chain risk management strategies, helping organisations assess and mitigate risks posed by third-party vendors and partners.

As the boundaries between physical and cyber domains continue to blur, continuous attack surface monitoring will need to consider both physical and cyber threats, leading to the integration of physical security measures and cyber threat intelligence.

The integration of emerging technologies, such as blockchain, IoT, and 5G networks, will introduce new attack surfaces and challenges for continuous monitoring, requiring organisations to adapt and evolve their approaches.

Effective continuous attack surface monitoring will rely on increased collaboration and information sharing among organisations, industry groups, and government agencies, fostering a collective approach to identifying and mitigating cyber threats.

As these trends unfold, organisations will need to stay vigilant and adapt their continuous attack surface monitoring strategies to keep pace with the ever-changing threat landscape and the evolving complexities of supply chains.

In the dynamic and interconnected world of supply chains, continuous attack surface monitoring has become an essential component of cybersecurity. By continuously identifying, assessing, and mitigating potential vulnerabilities and exposures, organisations can proactively address cyber risks and strengthen their overall security posture.

The benefits of continuous attack surface monitoring in the supply chain are numerous, including improved visibility, enhanced security, supplier risk management, incident response and recovery, regulatory compliance, and potential cost savings. However, organisations must also navigate challenges such as complexity, data management, false positives, skilled personnel requirements, integration challenges, and vendor cooperation.

To maximise the effectiveness of continuous attack surface monitoring, organisations should adopt best practices such as establishing a comprehensive strategy, leveraging automation, prioritising vulnerabilities, fostering collaboration and information sharing, continuous improvement, integrating with incident response and recovery plans, and providing ongoing training and awareness.

A range of tools and technologies, including vulnerability scanners, penetration testing tools, SIEM solutions, threat intelligence platforms, cloud security monitoring tools, IoT security solutions, and third-party risk management platforms, can support effective continuous attack surface monitoring.

As the threat landscape evolves and supply chains become increasingly complex, continuous attack surface monitoring will remain a critical aspect of cybersecurity. Future trends, such as increased automation and machine learning, integration with DevOps and Agile methodologies, adoption of Zero Trust architectures, increased focus on supply chain risk management, convergence of physical and cyber security, adoption of emerging technologies, and increased collaboration and information sharing, will shape the future of this domain.

By embracing continuous attack surface monitoring and adopting a proactive and collaborative approach to cybersecurity, organisations can fortify their defences, protect their supply chains, and maintain the trust and confidence of their customers and stakeholders.

Notes

1 Oyedokun, G.E., and Campbell, O., 2023. Imperatives of Risk Analysis and Asset Management on Cyber Security in a Technology-Driven Economy. In *Effective Cybersecurity Operations for Enterprise-Wide Systems* (pp.147–168). IGI Global.
2 Faulk Jr., T.J., 2024. Senior Executives' Strategic Edicts for Consistent Information Technology Metrics over Asset Management (Doctoral dissertation, Walden University).
3 Olivero, G., 2022. Asset Discovery Tools Supporting Cybersecurity Inventory (Doctoral dissertation, Politecnico di Torino).

4 Kotenko, I., Doynikova, E., Fedorchenko, A., and Desnitsky, V., 2022. Automation of Asset Inventory for Cyber Security: Investigation of Event Correlation-Based Technique. *Electronics*, 11(15), p.2368.
5 Yaseen, A., 2024. Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures. *Quarterly Journal of Emerging Technologies and Innovations*, 9(1), pp.38–60.
6 https://www.axonius.com/resources/khaleeji-bank-case-study.
7 https://www.idoxgroup.com/case-studies/health-case-studies/gloucestershire-hospitals-nhs-foundation-trust.
8 https://www.axonius.com/resources/wacom-case-study?channel=rc.
9 Rasel, M., Salam, M.A., and Shovon, R.B., 2024. Synergizing Cyber Threat Intelligence Sharing and Risk Assessment for Enhanced Government Cybersecurity: A Holistic Approach. *Journal Environmental Sciences And Technology*, 3 (1), pp.649–673.
10 Sarker, I.H., 2024. *AI-driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-making and Explainability*. Springer Nature.
11 Ampel, B.M., Samtani, S., Zhu, H., and Chen, H., 2024. Creating Proactive Cyber Threat Intelligence with Hacker Exploit Labels: A Deep Transfer Learning Approach. *MIS Quarterly*, 48(1).
12 Zacharis, A., Katos, V., and Patsakis, C., 2024. Integrating AI-driven Threat Intelligence and Forecasting in the Cyber Security Exercise Content Generation Lifecycle. *International Journal of Information Security*, pp.1–20.
13 https://www.crowdstrike.co.uk/resources/case-studies/lasselsberger.
14 https://www.crowdstrike.co.uk/resources/case-studies/gorillas.
15 https://www.crowdstrike.com/resources/case-studies/mercury-financial-consolidating-with-crowdstrike/?_gl=1*1txsnfd*_gcl_au*NTgzODQ4OTExLjE3MTk2NDk4Njg.*_ga*MTQwODI3NDU1Ny4xNzE5NjQ5ODc0*_ga_ZKTET1D58V*MTcxOTY0OTg3NC4xLjEuMTcxOTY1MDM1MS4wLjAuMA.
16 Amoo, O.O., Osasona, F., Atadoga, A., Ayinla, B.S., Farayola, O.A., and Abrahams, T.O., 2024. Cybersecurity Threats in the Age of IoT: A Review of Protective Measures. *International Journal of Science and Research Archive*, 11(1), pp.1304–1310.
17 Osazuwa, O-M. C., and Musa, M.O., 2024. The Expanding Attack Surface: Securing AI and Machine Learning Systems in Security Operations. *International Journal of Innovative Science and Research Technology (IJISRT)*, 9(5). https://doi.org/10.38124/ijisrt/IJISRT24MAY1613.

12

SECURITY TESTING, VULNERABILITY SCANNING AND INCIDENT RESPONSE (IR)

Security Testing

In the intricate web of global trade and commerce, the supply chain stands as a critical lifeline, connecting businesses, manufacturers, and consumers across continents. However, with the ever-increasing reliance on digital technologies and interconnected systems, this intricate network has become a prime target for malicious actors seeking to exploit vulnerabilities for personal gain or disruptive purposes.

Kaur et al. (2024) argue that as we navigate the complexities of the modern supply chain, it is imperative to recognise the paramount importance of cybersecurity testing. By proactively identifying and mitigating potential risks, we can fortify the resilience of our supply chains, safeguarding not only the flow of goods and services but also the integrity of sensitive data and the trust of our stakeholders.[1]

Rane and Qureshi (2024) argue that automated scanning and penetration testing are vital components of a cybersecurity strategy. To improve understanding, we must conduct supply chain cybersecurity testing, advocating for best practices in an era where cyber threats loom large. Cybersecurity testing has a pivotal role in securing the supply chain and ensuring partners are not unwittingly opening up new vulnerabilities.[2]

The growing threat of cyberattacks must be taken seriously. The supply chain, once perceived as a relatively secure domain, has increasingly become a prime target for cybercriminals. The interconnectivity and complexity of modern supply chains, coupled with the proliferation of digital technologies, have inadvertently created vulnerabilities that malicious actors are all too eager to exploit.

Cyberattacks on the supply chain can manifest in various forms, each with devastating consequences. From data breaches compromising sensitive

DOI: 10.4324/9781003604969-12

information to ransomware attacks threatening operations, the repercussions can ripple across the entire supply chain ecosystem, disrupting operations, eroding consumer trust, and inflicting substantial financial losses.

Moreover, the rise of advanced persistent threats (APTs) and state-sponsored cyber activities has added a new layer of complexity to the threat landscape. These sophisticated actors possess the resources and motivation to infiltrate supply chains, often with the intent of stealing intellectual property, disrupting critical infrastructure, or gaining a strategic advantage.

Ignoring the growing threat of cyberattacks on the supply chain is no longer an option. Proactive measures, including robust cybersecurity testing, are paramount to safeguarding the integrity and continuity of our supply chains in the face of an ever-evolving cyber threat landscape.

Common vulnerabilities in the supply chain must be considered. To effectively secure the supply chain, it is crucial to understand the various vulnerabilities that can be exploited by malicious actors. These vulnerabilities can stem from a range of sources.

Lax security protocols, outdated software, and insufficient access controls can create entry points for cybercriminals to breach systems and compromise data. The supply chain often involves multiple third-party vendors and partners, each with their own security posture. A weak link in this chain can potentially expose the entire ecosystem to cyber threats.

Disgruntled employees, contractors, or individuals with malicious intent can exploit their privileged access to systems and data, posing a significant risk to the supply chain's integrity. Outdated and legacy systems, which may still be in use due to compatibility or cost concerns, can present vulnerabilities that are difficult to patch or mitigate.

The complex nature of supply chains can create gaps in awareness, making it challenging to monitor and detect potential threats or anomalies across the entire ecosystem.

By identifying and addressing these common vulnerabilities, organisations can take proactive steps to enhance the cybersecurity posture of their supply chains, reducing the risk of costly breaches and disruptions.

Cybersecurity testing plays a pivotal role in enhancing the resilience of the supply chain by proactively identifying and mitigating potential vulnerabilities before they can be exploited. By conducting rigorous testing, organisations can evaluate the effectiveness of their security measures, identify gaps, and implement necessary improvements to fortify their defences.

Cybersecurity testing techniques, such as penetration testing and vulnerability assessments, can uncover weaknesses in systems, applications, and processes, allowing organisations to take corrective actions before malicious actors can exploit them. By simulating real-world attack scenarios, cybersecurity testing can help organisations refine their threat detection and incident response capabilities, ensuring they are better prepared to respond swiftly and effectively to potential cyber incidents.

Engaging in regular cybersecurity testing promotes a heightened awareness of security risks and challenges within the organisation, fostering a culture of vigilance and proactive risk management. Many industries and sectors have stringent cybersecurity regulations and standards in place. Cybersecurity testing can help organisations demonstrate compliance and mitigate the risk of hefty fines or legal consequences.

By leveraging the power of cybersecurity testing, organisations can fortify the resilience of their supply chains, safeguarding against potential disruptions, data breaches, and reputational damage, while fostering trust and confidence among stakeholders.

Cybersecurity testing encompasses a wide range of techniques and methodologies designed to assess and validate the security posture of systems, applications, and processes. In the context of supply chain security, several types of cybersecurity testing are relevant.

Vulnerability scanning assessments involve scanning and analysing systems, networks, and applications to identify known vulnerabilities that could be exploited by malicious actors. Vulnerability assessments provide a comprehensive view of potential weaknesses and enable organisations to prioritise remediation efforts. External vulnerability scans aim to identify vulnerabilities that attackers could exploit from outside the organisation's network. Internal vulnerability scans help to identify vulnerabilities that could potentially be exploited by attackers who have already gained internal access, such as employees or contractors.

Penetration testing simulates real-world cyber attacks to evaluate the effectiveness of an organisation's security controls and incident response capabilities. Penetration testers employ various techniques, such as network reconnaissance, exploitation, and post-exploitation activities, to identify and exploit vulnerabilities. Examples include External Infrastructure Pen Tests, Internal Pen Tests, and Wi-Fi Tests.

As supply chains increasingly rely on web-based applications and platforms, it is crucial to assess the security of these applications. Web application security testing involves identifying and mitigating vulnerabilities such as cross-site scripting (XSS), SQL injection, and insecure authentication mechanisms.

In the context of software development and integration within the supply chain, secure code review involves analysing source code to identify potential security vulnerabilities, coding flaws, and non-compliance with secure coding practices.

Supply chains often involve human interactions, making them susceptible to social engineering attacks. Social engineering testing evaluates the effectiveness of security awareness training and the ability of employees to identify and respond to phishing attempts, pretexting, and other forms of deception.

Given the reliance on third-party vendors and partners within the supply chain, it is essential to assess their security posture and practices. Third-party

risk assessments help organisations identify and mitigate potential risks introduced by external entities.

By employing a combination of these cybersecurity testing techniques, organisations can gain a comprehensive understanding of their supply chain's security posture, identify vulnerabilities, and implement effective mitigation strategies to enhance overall resilience. Let's explore a few in more detail:

Penetration testing simulates a real-time cyber attack against an app/software, system, or network under secure conditions. It is performed manually by a certified security expert to understand the strength of the security measures against attacks in real time. Unknown vulnerabilities, including zero-day threats and business logic flaws, are uncovered.

The typical process involves defining the scope of the test, including the systems, applications, and networks to be tested. Gather information about the target systems, such as IP addresses, domain names, and publicly available information. Scan the target systems using automated vulnerability scanning tools to identify known vulnerabilities.

Develop attack scenarios and threat models based on the identified vulnerabilities. Attempt to exploit the identified vulnerabilities to gain unauthorised access or manipulate the target systems.

Collect data on the vulnerabilities exploited and any sensitive information accessed. Document the findings, including the vulnerabilities exploited, methods used, and potential impact. Provide recommendations for remediation.

Red team exercises involve the act of systematically and rigorously (but ethically) identifying an attack path that breaches the organisation's security defence through real-world attack techniques. In adopting this adversarial approach, the organisation's defences are based not on the theoretical capabilities of security tools and systems, but their actual performance in the presence of real-world threats. Red teaming is a critical component in accurately assessing the company's prevention, detection, and remediation capabilities and maturity.

Red team exercises allow organisations to actively test their existing cyber defences and capabilities in a low-risk environment. This allows them to continuously evolve the organisation's security strategy based on the company's unique weaknesses and vulnerabilities, and the latest real-world attack techniques.

This enables organisations to identify misconfigurations and coverage gaps in existing security products, improve network security to detect targeted attacks and improve breakout time and increase healthy competition among security personnel and foster cooperation among IT and security teams. Generating security awareness among staff over the risk of human vulnerabilities which may compromise the organisation's security is crucial. Develop skills and maturity in security capabilities within a safe training environment.

Van Buggenhout (2024) argues *purple team exercises* work better than red team exercises as they are run in a more collaborative way so both defenders

and attackers work together more cohesively to identify routes in and improve runbooks and response mechanisms.[3]

Security code review is vital in secure software development. This aims to identify and rectify vulnerabilities in an application's source code, reducing the risk of security breaches.

A security analyst examines the source code to identify potential security flaws and coding errors. Security code reviews should be integrated into the software development life cycle, conducted regularly, and tailored to the application's specific technology stack and threat landscape.

Static application security testing (SAST) or code scanning automates the analysis of an application's source code, bytecode, or binary code for security vulnerabilities and coding errors without executing the application. SAST tools break down your code, enabling them to probe deep into functions and subroutines for hidden vulnerabilities. They occasionally produce false positives, but these tools are adept at uncovering a wide array of potential threats, such as memory leaks, infinite loops, and unhandled errors.

Dynamic application security testing (DAST), or black-box testing, is a method for evaluating the security of an application while it's running without any knowledge of its internal code or structure. This simulates real-world attack scenarios with valuable insights into potential vulnerabilities from an external perspective.

Key capabilities include runtime testing: DAST scanners interact with the application in real time, sending various inputs and requests to assess how the application responds. DAST scanners examine the application from an outsider's perspective, just like a malicious attacker would.

DAST tools simulate various attack vectors, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), to identify vulnerabilities that could compromise the application's security. DAST tools are particularly efficient when scanning large and complex applications because they do not require access to the source code. DAST tools can assess how well authentication and access controls are implemented by trying to bypass them through various means.

Ethical hacking involves security professionals attempting to breach a system's defences in an authorised manner. This allows organisations to identify vulnerabilities and weak points from the perspective of an attacker. Ethical hackers use the techniques malicious hackers use to improve security.

Web application hacking: Ethical hackers focus on identifying weaknesses in web applications.

System hacking: Ethical hackers attempt to identify vulnerabilities within operating systems, software, and hardware components of computer systems.

Web server hacking: Ethical hackers assess web server configurations, access controls, and vulnerabilities that might allow attackers to compromise the server's functionality or gain unauthorised access.

Database hacking: This involves identifying vulnerabilities within databases and their management systems. Ethical hackers aim to uncover issues

such as SQL injection, insecure database configurations, and unauthorised data access.

Implementing effective cybersecurity testing within the supply chain requires a strategic and well-coordinated approach. To maximise the benefits of cybersecurity testing and ensure its successful integration, organisations should consider best practices.

Establish a comprehensive cybersecurity testing programme. Develop a structured programme that outlines the objectives, scope, methodologies, and frequency of cybersecurity testing activities. This programme should align with the organisation's overall risk management strategy and be tailored to the specific needs and complexities of the supply chain.

Involve stakeholders and subject matter experts. Engage relevant stakeholders, including supply chain partners, security professionals, and subject matter experts, throughout the cybersecurity testing process. Their input and collaboration can provide valuable insights and ensure a comprehensive assessment of potential risks and vulnerabilities.

Integrate cybersecurity testing into the software development life cycle (SDLC). For organisations developing or integrating software within the supply chain, it is crucial to incorporate cybersecurity testing practices into the SDLC. This includes conducting secure code reviews, static and dynamic application security testing (SAST/DAST), and ensuring adherence to secure coding standards.

Adopt a risk-based approach to cybersecurity testing, focusing efforts on critical systems, applications, and processes that pose the highest risk to the supply chain. This approach ensures efficient allocation of resources and maximises the impact of testing activities.

Establish well-defined processes for identifying, prioritising, and remediating vulnerabilities discovered during cybersecurity testing. This includes developing and maintaining a centralised vulnerability management system, assigning responsible parties, and establishing timelines for remediation.

Encourage collaboration and information sharing among supply chain partners, industry associations, and relevant stakeholders. This can facilitate the exchange of threat intelligence, best practices, and lessons learned, enhancing the overall cybersecurity posture of the supply chain ecosystem.

Cybersecurity threats are constantly evolving, necessitating continuous monitoring and adaptation of cybersecurity testing strategies. Regularly review and update testing methodologies, tools, and processes to ensure they remain effective and aligned with the latest threat landscape and industry best practices.

By adhering to these best practices, organisations can effectively integrate cybersecurity testing into their supply chain operations, fostering a proactive and resilient approach to cybersecurity and mitigating the risks posed by malicious actors.

Investing in supply chain cybersecurity testing may require dedicated resources and commitment, but the benefits it offers are invaluable in today's

threat-laden landscape. By prioritising cybersecurity testing, organisations can reap advantages.

Cybersecurity testing provides organisations with a comprehensive understanding of their supply chain's risk landscape, enabling them to identify and mitigate potential vulnerabilities proactively. This proactive approach to risk management can prevent costly data breaches, operational disruptions, and reputational damage.

By identifying and addressing vulnerabilities, cybersecurity testing strengthens the overall resilience of the supply chain. This increased resilience ensures continuity of operations, minimises disruptions, and fosters trust among stakeholders, including customers, partners, and regulatory bodies.

Many industries and sectors have stringent cybersecurity regulations and standards in place. Implementing robust cybersecurity testing practices can help organisations demonstrate compliance, avoid hefty fines, and maintain their reputation as responsible and trustworthy entities.

In an increasingly competitive business landscape, organisations that prioritise cybersecurity testing and supply chain resilience can gain a significant competitive advantage. Customers and partners are more likely to trust and prefer working with organisations that demonstrate a strong commitment to cybersecurity and risk management.

Supply chains often involve the exchange of sensitive information, including trade secrets, proprietary data, and customer information. Cybersecurity testing helps organisations safeguard this valuable intellectual property and data, preventing unauthorised access, theft, or misuse.

While cybersecurity testing requires an initial investment, the long-term benefits can outweigh the costs. By preventing costly data breaches, operational disruptions, and reputational damage, organisations can realise significant cost savings and maintain operational efficiency throughout the supply chain.

Investing in supply chain cybersecurity testing is not merely a defensive measure; it is a strategic investment in the long-term viability, resilience, and competitiveness of an organisation. By prioritising cybersecurity testing, organisations can navigate the complex threat landscape with confidence, safeguarding their supply chains and fostering trust among stakeholders.

Despite the numerous benefits of cybersecurity testing for supply chain resilience, organisations may encounter various challenges and obstacles during implementation. Acknowledging and addressing these challenges is crucial for the successful integration of cybersecurity testing practices.

Implementing comprehensive cybersecurity testing programmes can be resource-intensive, requiring dedicated personnel, specialised tools, and infrastructure. Organisations may face budgetary constraints or limitations in skilled cybersecurity professionals, hindering their ability to execute effective testing initiatives.

Supply chains often involve multiple stakeholders, diverse systems, and intricate interconnections. This complexity can make it challenging to gain a

comprehensive understanding of potential vulnerabilities and attack vectors, complicating the cybersecurity testing process.

Many organisations within the supply chain rely on legacy systems and applications that may not be compatible with modern cybersecurity testing tools and methodologies. Integrating these systems into the testing process can be a significant challenge, requiring specialised expertise and customised approaches.

Effective cybersecurity testing requires collaboration and buy-in from all stakeholders within the supply chain ecosystem. Overcoming resistance to change, addressing concerns about potential disruptions, and fostering a culture of cybersecurity awareness can be daunting tasks.

Different industries and regions may have varying cybersecurity regulations and compliance requirements. Navigating this complex landscape and ensuring compliance during cybersecurity testing can be a significant obstacle, particularly for organisations operating across multiple jurisdictions.

The cyber threat landscape is constantly evolving, with new attack vectors and sophisticated techniques emerging regularly. Keeping cybersecurity testing practices up to date and effective in the face of this rapid evolution can be a continuous challenge.

To overcome these challenges, organisations must adopt a proactive and strategic approach. This may involve investing in skilled cybersecurity professionals, leveraging automation and advanced testing tools, fostering collaboration and information sharing within the supply chain ecosystem, and continuously updating testing methodologies to align with emerging threats and best practices.

As the supply chain landscape continues to evolve, so too must the approaches and technologies employed for cybersecurity testing. Embracing emerging trends and innovations in this field will be crucial for organisations to stay ahead of the curve and maintain a robust cybersecurity posture. Some of the key trends and innovations shaping the future of supply chain cybersecurity testing include:

AI and ML technologies are increasingly being leveraged to enhance cybersecurity testing capabilities. These technologies can automate vulnerability detection, analyse vast amounts of data for potential threats, and even simulate advanced cyber attacks for testing purposes.

As software development practices shift towards more agile and iterative approaches, integrating cybersecurity testing into the Continuous Integration and Continuous Delivery (CI/CD) pipeline becomes essential. This ensures that security vulnerabilities are identified and addressed early in the development cycle, reducing the risk of introducing vulnerabilities into the supply chain.

Blockchain and distributed ledger technologies offer promising solutions for enhancing supply chain transparency and traceability. By leveraging these technologies, organisations can create immutable audit trails, enabling more effective cybersecurity testing and verification of supply chain integrity.

With the proliferation of IoT devices and their integration into supply chain operations, dedicated IoT security testing methodologies are gaining prominence. These methodologies address the unique vulnerabilities and attack vectors associated with IoT devices, ensuring comprehensive cybersecurity testing across the entire supply chain ecosystem.

As organisations increasingly adopt cloud-based technologies and services within their supply chains, cloud-based cybersecurity testing solutions are emerging. These solutions offer scalability, cost-effectiveness, and the ability to conduct testing from remote locations, enhancing the accessibility and flexibility of cybersecurity testing initiatives.

Fostering collaboration and information sharing among supply chain partners, industry associations, and government agencies will become increasingly crucial. By pooling threat intelligence and sharing best practices, organisations can collectively enhance their cybersecurity testing capabilities and stay ahead of emerging threats.

Embracing these trends and innovations will not only strengthen the cybersecurity posture of individual organisations but also contribute to the overall resilience of the global supply chain ecosystem. By staying at the forefront of technological advancements and embracing a proactive approach to cybersecurity testing, organisations can navigate the ever-evolving threat landscape with confidence and ensure the continuity of their supply chain operations.

Securing the supply chain through effective cybersecurity testing is not merely a defensive measure but a strategic imperative in today's interconnected and threat-laden landscape. By proactively identifying and mitigating vulnerabilities, organisations can fortify the resilience of their supply chains, safeguarding the flow of goods, services, and sensitive data while fostering trust among stakeholders.

While the journey towards robust supply chain cybersecurity testing may present challenges, the benefits it yields are invaluable. From improved risk management and enhanced operational continuity to compliance with industry standards and competitive advantages, investing in cybersecurity testing is an investment in the long-term viability and success of an organisation.

The integration of emerging technologies such as AI, blockchain, and cloud-based solutions will revolutionise the cybersecurity testing landscape. Embracing these innovations and fostering collaboration within the supply chain ecosystem will be crucial for organisations to stay ahead of the ever-evolving cyber threat landscape.

Ultimately, securing the supply chain is a shared responsibility that requires a proactive and collaborative approach from all stakeholders. By prioritising cybersecurity testing and adopting best practices, we can collectively fortify the resilience of our supply chains, ensuring the seamless flow of goods and services while safeguarding the integrity of our digital ecosystems.

In the ever-evolving landscape of cybersecurity, vulnerability scanning is a critical component of any comprehensive security strategy. As the digital world continues to expand, organisations face an increasing number of threats, making it imperative to identify and address potential vulnerabilities before they can be exploited by malicious actors.

Vulnerability Scanning

Vulnerability scanning is a process that involves systematically analysing systems, networks, and applications to detect and report on any weaknesses or flaws that could be leveraged by cybercriminals. These vulnerabilities can range from software bugs and misconfigurations to outdated or unpatched systems, all of which can leave an organisation exposed to various types of cyber attacks.

Sontan and Samuel (2024) argue the case for the use of AI-powered vulnerability scanners. By using AI to conducting regular vulnerability scans, organisations can gain valuable insights into their security posture, enabling them to prioritise and address the most critical vulnerabilities promptly. They argue that we can better prioritise critical vulnerabilities by applying machine learning algorithms to analyse extensive datasets. This proactive approach not only helps mitigate risks but also ensures compliance with industry regulations and standards.[4]

Mohaidat and Al-Helali (2024) contend that vulnerability scanning is vital in supply chain security. Supply chain security has become a paramount concern for organisations across various industries. With the increasing interconnectivity and complexity of modern supply chains, a single vulnerability in any part of the chain can have far-reaching consequences, potentially compromising the entire ecosystem.[5]

Jimmy (2024) argues vulnerability scanning plays a crucial role in securing the supply chain by identifying and addressing vulnerabilities at every stage. They argue the case for use of AI and cloud security tooling for conducting thorough scans of all systems, networks, and applications involved in the supply chain process so that organisations can detect and remediate vulnerabilities more quickly before they can be exploited by threat actors.[6]

Moreover, vulnerability scanning helps organisations maintain visibility and control over their supply chain partners' security posture. By requiring supply chain partners to undergo regular vulnerability assessments and provide reports, organisations can ensure that their partners adhere to the same high security standards, minimising the risk of a breach originating from a third-party vendor or supplier.

Implementing a robust vulnerability scanning programme can provide numerous benefits in securing your supply chain. By identifying and addressing vulnerabilities proactively, organisations can significantly reduce the risk of cyber attacks, data breaches, and other security incidents that could disrupt the supply chain operations.[7]

Many industry regulations and standards, such as PCI DSS, HIPAA, and ISO 27001, mandate regular vulnerability assessments. Vulnerability scanning helps organisations demonstrate compliance and avoid costly penalties or legal ramifications.

Proactively addressing vulnerabilities is often more cost-effective than dealing with the consequences of a successful cyber attack, which can include remediation costs, reputational damage, and potential legal liabilities.

Vulnerability scanning provides organisations with a comprehensive view of their security posture, enabling them to make informed decisions and prioritise remediation efforts based on the criticality of the identified vulnerabilities.[8]

By implementing robust security measures, including vulnerability scanning, organisations can differentiate themselves from competitors and demonstrate their commitment to supply chain security, which can be a key factor in attracting and retaining customers.

Common vulnerabilities in supply chain systems must be constantly assessed. Supply chain systems are vulnerable to a wide range of threats. Outdated or unpatched software can introduce vulnerabilities that can be exploited by cybercriminals. Common software vulnerabilities include buffer overflows, cross-site scripting (XSS), and SQL injection.

Improperly configured systems, such as web servers, databases, or firewalls, can expose sensitive information or provide entry points for unauthorised access. Inadequate authentication and authorisation mechanisms, such as weak passwords or lack of multi-factor authentication, can allow unauthorised access to critical systems and data.

Unencrypted or poorly secured communication channels between supply chain partners can expose sensitive data in transit, making it vulnerable to interception and manipulation. Supply chain partners, such as vendors or suppliers, may have inadequate security measures in place, increasing the risk of vulnerabilities being introduced into the supply chain ecosystem.

Develop a comprehensive vulnerability management policy that outlines the scope, frequency, and procedures for conducting vulnerability scans, as well as the roles and responsibilities of various stakeholders.

Maintain an up-to-date inventory of all systems, networks, and applications involved in the supply chain process. This inventory will serve as the foundation for your vulnerability scanning efforts.

Choose vulnerability scanning tools that are suitable for your organisation's specific needs and infrastructure. Consider factors such as ease of use, scalability, and compatibility with existing systems.

Establish a schedule for conducting regular vulnerability scans across all identified assets. The frequency of scans should be based on the criticality of the assets and the organisation's risk tolerance.

Develop a systematic approach to prioritising and remediating identified vulnerabilities. Consider factors such as the severity of the vulnerability, the

potential impact on the supply chain, and the resources required for remediation.

Implement continuous monitoring and reporting mechanisms to ensure that vulnerabilities are promptly identified and addressed. Regular reporting to stakeholders and management can help maintain visibility and accountability.

Engage with supply chain partners and establish clear expectations for vulnerability management. Consider requiring partners to undergo regular vulnerability assessments and provide reports to ensure a consistent level of security across the entire supply chain ecosystem.

It is important to maximise the effectiveness of your vulnerability scanning efforts in securing your supply chain. Ensure that your vulnerability scanning programme covers all relevant assets, including systems, networks, applications, and devices involved in the supply chain process. Regularly update your asset inventory to account for changes and additions.

Implement automated and scheduled vulnerability scans to ensure consistent and timely assessments. This approach minimises the risk of overlooking vulnerabilities due to manual processes or resource constraints.

Conduct both credentialled (authenticated) and non-credentialled (unauthenticated) vulnerability scans to gain a comprehensive understanding of your security posture. Credentialled scans provide deeper insights into system configurations and vulnerabilities, while non-credentialled scans simulate external attacks.

Prioritise the remediation of vulnerabilities based on their risk level, considering factors such as the severity of the vulnerability, the criticality of the affected assets, and the potential impact on the supply chain operations.

Implement continuous monitoring and alerting mechanisms to promptly detect and respond to newly discovered vulnerabilities or changes in the security landscape.

Integrate your vulnerability scanning programme with other security tools and processes, such as patch management, incident response, and security information and event management (SIEM) systems, for a more comprehensive and coordinated approach to security.

Establish secure and controlled processes for remediating identified vulnerabilities. This may include testing patches or updates in a secure environment before deploying them to production systems.

Provide regular training and awareness programmes for employees and supply chain partners to ensure a consistent understanding of vulnerability management best practices and the importance of supply chain security.

Selecting the appropriate vulnerability scanning tools is crucial for the success of your vulnerability management programme. Ensure that the chosen tools are compatible with your organisation's existing systems, networks, and applications. This includes support for various operating systems, databases, and web applications.

Select tools that are scalable to accommodate the size and complexity of your supply chain ecosystem, including the ability to scan a large number of assets simultaneously. Evaluate the accuracy of the vulnerability scanning tools and their ability to minimise false positives, which can lead to wasted resources and unnecessary remediation efforts.

Look for tools that provide comprehensive reporting and intuitive dashboards, enabling you to easily visualise and analyse vulnerability data, track remediation efforts, and communicate findings to stakeholders.

Consider tools that offer automation capabilities and seamless integration with other security tools, such as patch management systems, SIEM solutions, and ticketing systems, to streamline vulnerability management processes. Evaluate the vendor's reputation, support offerings, and commitment to regular updates and improvements to ensure that the tools remain effective and up to date with the latest vulnerabilities and threats.

Ensure that the chosen tools comply with relevant industry regulations and standards, such as PCI DSS, HIPAA, or ISO 27001, if applicable to your organisation. Vulnerability scanning plays a crucial role in helping organisations achieve and maintain compliance with various industry regulations and standards. Many regulatory bodies and frameworks, such as PCI DSS, HIPAA, and NIST, mandate regular vulnerability assessments and the implementation of robust vulnerability management processes.

PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) requires organisations that handle credit card transactions to conduct regular vulnerability scans and remediate identified vulnerabilities to protect cardholder data.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) requires health organisations and their business associates to implement measures to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI), which includes conducting vulnerability assessments and addressing identified vulnerabilities.

NIST: The National Institute of Standards and Technology (NIST) provides guidelines and best practices for vulnerability management, including the NIST Cybersecurity Framework and the NIST Special Publication 800–53, which outline requirements for vulnerability scanning and remediation.

ISO 27001: The International Organization for Standardization (ISO) 27001 standard for information security management systems requires organisations to implement vulnerability management processes, including regular vulnerability assessments and remediation activities.

By implementing a robust vulnerability scanning programme and adhering to industry-specific regulations and standards, organisations can demonstrate their commitment to security and compliance, avoid costly penalties and legal ramifications, and maintain the trust of customers and stakeholders.

In the ever-evolving landscape of cybersecurity, securing your supply chain has become an imperative for organisations across various industries.

Vulnerability scanning plays a crucial role in identifying and addressing potential weaknesses and flaws that could be exploited by malicious actors, compromising the integrity and resilience of your supply chain operations.

By implementing a comprehensive vulnerability scanning programme and following best practices, organisations can proactively mitigate risks, maintain visibility into their security posture, and ensure compliance with industry regulations and standards. Collaboration with supply chain partners, continuous monitoring, and the integration of vulnerability scanning with other security tools and processes are essential components of a robust supply chain security strategy.

Incident Response

Organisations face an ever-increasing array of potential incidents that can disrupt operations, compromise data integrity, and tarnish reputations. From cyber attacks and natural disasters to supply chain disruptions and regulatory breaches, the need for a comprehensive and well-orchestrated incident response plan has never been more paramount.

Aldabjan et al. (2024) insist that *incident response planning* is a proactive approach to mitigating risks and minimising the impact of disruptive events. It involves developing strategies, protocols, and procedures that enable organisations to respond swiftly and effectively to a wide range of incidents.[9]

Naseer et al. (2024) contend that streamlining incident response planning is a critical endeavour, one that necessitates close collaboration with suppliers and unwavering preparedness. By fostering a culture of preparedness and establishing clear lines of communication and responsibility, incident response planning empowers organisations to safeguard their operations, protect their stakeholders, and maintain business continuity in the face of adversity.[10]

Haber and Rolls (2024) argue that in an era marked by rapid technological advancements, globalised supply chains, and heightened regulatory scrutiny, the significance of streamlining incident response planning cannot be overstated.[11]

A well-crafted and meticulously executed plan can mean the difference between a swift resolution and a prolonged, costly crisis. By optimising incident response processes, organisations can minimise downtime and operational disruptions, protect sensitive data and intellectual property, and maintain customer trust and loyalty. They can comply with industry regulations and avoid penalties. It is important to preserve brand reputation and stakeholder confidence.

Streamlining incident response planning is not merely a risk mitigation strategy; it is a strategic imperative that underpins organisational resilience and long-term success.

Effective incident response planning encompasses a multitude of critical components, each playing a vital role in ensuring a comprehensive and

coordinated approach. Risk assessment is crucial in identifying potential threats, vulnerabilities, and their associated impacts. Incident detection and reporting helps with establishing robust mechanisms for early detection and clear communication channels. Response procedures ensure there are detailed action plans and protocols for various incident scenarios. Crisis communication plans ensure strategies are agreed for transparent and timely communication with stakeholders. Resource allocation should be agreed in advance, ensuring the availability of necessary resources, including personnel, equipment, and funding. Training and testing ensure we are conducting regular drills and exercises to validate and refine the incident response plan. Continuous improvement ensures we are incorporating lessons learned and best practices to enhance the plan's effectiveness.

By addressing these components holistically, organisations can cultivate a proactive and adaptable incident response posture, positioning themselves to navigate even the most challenging situations with confidence and agility.

In the intricate tapestry of modern supply chains, organisations are inextricably linked to a vast network of suppliers and partners. A disruption or incident affecting any one of these entities can reverberate throughout the entire ecosystem, underscoring the critical importance of *supplier collaboration* in incident response planning.

Effective supplier collaboration involves identifying critical suppliers. Assess the criticality of each supplier based on their impact on operations and potential risks. Establishing robust communication channels and protocols helps to facilitate real-time information sharing and coordination. Collaborating with suppliers helps to ensure alignment between respective incident response plans and procedures. Conducting joint exercises proves helpful by organising simulations and drills that involve suppliers, testing collective readiness and identifying areas for improvement. Fostering trust and transparency is important. Cultivating an environment of mutual trust and open communication, enabling a proactive approach to incident management.

By fostering strong supplier collaboration, organisations can enhance their incident response capabilities, mitigate supply chain disruptions, and safeguard the continuity of their operations.

While supplier collaboration is paramount, it is equally crucial to ensure that suppliers themselves are adequately prepared to respond to incidents effectively. To help organisations assess and enhance supplier preparedness we can conduct supplier risk assessments to evaluate suppliers' incident response capabilities, infrastructure, and overall resilience. We can establish clear performance expectations by defining specific requirements and standards for supplier incident response preparedness. It is important to provide training and resources. Offer training opportunities, guidance, and resources to support suppliers in developing robust incident response plans. Monitor and audit supplier readiness through regular review and audit of suppliers'

incident response plans and preparedness levels. Encourage continuous improvement by collaborating with suppliers to identify areas for improvement and implement best practices. By fostering a culture of preparedness among suppliers, organisations can strengthen the collective resilience of their supply chain and mitigate the potential impact of incidents.

Case Studies

To illustrate the tangible benefits of streamlining incident response planning and fostering supplier collaboration, let's explore two real-world case studies:

Case Study 1: Cyber Attack on a Global Retailer

In 2019, a major global retailer fell victim to a sophisticated cyber attack that compromised customer data and disrupted online operations. Thanks to their well-orchestrated incident response plan and close collaboration with key technology suppliers, the retailer was able to:

- Rapidly isolate and contain the breach.
- Restore critical systems and resume online operations within 48 hours.
- Implement enhanced security measures and data protection protocols.
- Maintain customer trust and minimise reputational damage.

The retailer's proactive approach to incident response planning, coupled with their strong partnerships with cybersecurity providers and cloud service suppliers, proved invaluable in mitigating the impact of the attack and ensuring business continuity.

Case Study 2: Natural Disaster and Supply Chain Disruption

In 2021, a major automotive manufacturer faced significant supply chain disruptions due to a catastrophic natural disaster that impacted several key suppliers. However, their comprehensive incident response plan and collaborative efforts with suppliers enabled them to:

- Quickly identify alternative sourcing options and reroute shipments.
- Leverage contingency production facilities and inventory buffers.
- Maintain open communication with customers and stakeholders.
- Minimise production delays and meet customer demand.

The manufacturer's commitment to supplier collaboration, including joint incident response exercises and risk mitigation strategies, proved instrumental in navigating the crisis and minimising the impact on their operations and customer relationships.

These case studies demonstrate the invaluable role of streamlining incident response planning and fostering supplier collaboration in mitigating risks, ensuring business continuity, and preserving stakeholder trust.

Supplier Collaboration

While the benefits of streamlining incident response planning and supplier collaboration are evident, organisations often encounter various *challenges* along the way. We can consider some common hurdles and *strategies* to overcome them. Lack of executive buy-in is very common. Educate leadership on the importance of incident response planning and its direct impact on organisational resilience and profitability.

Siloed operations and communication barriers are prevalent. Foster a culture of cross-functional collaboration and implement robust communication channels across departments and with suppliers. Resource constraints can hinder progress. Prioritise incident response planning as a strategic investment and explore cost-effective solutions, such as leveraging cloud-based tools and shared resources with suppliers.

Resistance to change and complacency are some of the biggest obstacles to driving a change of culture. Continuously reinforce the value of preparedness and highlight the potential consequences of inaction through simulations and real-world examples. The complexity of supplier relationships can hamper progress. Establish clear roles, responsibilities, and performance expectations for suppliers, and leverage technology to streamline collaboration and information sharing.

By proactively addressing these challenges, organisations can overcome obstacles and cultivate a robust incident response posture that integrates supplier collaboration and preparedness.

To ensure the successful streamlining of incident response planning and effective supplier collaboration, organisations should adopt best practices. Establish a dedicated incident response team. Assemble a cross-functional team with clearly defined roles and responsibilities, including representatives from key suppliers.

Develop comprehensive incident response policies and procedures. Document detailed protocols for various incident scenarios, covering detection, response, communication, and recovery. Implement robust communication and collaboration tools. Leverage modern communication platforms, project management tools, and secure data-sharing solutions to facilitate real-time collaboration with suppliers. Conducting regular training and simulations are essential. Organise periodic training sessions and realistic simulations to test the effectiveness of the incident response plan and identify areas for improvement. Foster a culture of continuous improvement by encouraging open feedback, lessons learned sessions, and the incorporation of best practices to continuously enhance the incident response plan and supplier collaboration efforts.

By adhering to these best practices, organisations can streamline their incident response planning processes, foster stronger supplier relationships, and cultivate a culture of preparedness and resilience.

In today's digital age, a plethora of tools and technologies are available to support efficient incident response planning and supplier collaboration. These include incident response management platforms, which are centralised platforms that facilitate incident tracking, response coordination, and real-time communication with stakeholders, including suppliers. Threat intelligence and monitoring solutions are effective as advanced tools that provide real-time threat detection, analysis, and actionable intelligence, enabling proactive incident response.

Secure collaboration and data-sharing tools are useful as cloud-based platforms that enable secure file sharing, document collaboration, and communication with suppliers, ensuring data protection and compliance. Incident simulation and training platforms are effective as immersive simulation environments that enable realistic incident response drills and training exercises, involving suppliers and partners. Automated incident response workflows using intelligent automation tools help to streamline incident response processes, reducing manual effort and improving response times.

By leveraging these cutting-edge tools and technologies, organisations can enhance their incident response capabilities, foster seamless supplier collaboration, and stay ahead of emerging threats and challenges.

As we navigate an increasingly complex and interconnected business landscape, the importance of streamlining incident response planning and fostering supplier collaboration cannot be overstated. By embracing a proactive and collaborative approach, organisations can cultivate a culture of preparedness, mitigate risks, and safeguard their operations, data, and reputation.

The future of incident response planning lies in the seamless integration of advanced technologies, intelligent automation, and real-time collaboration platforms. These innovations will empower organisations to respond swiftly and effectively to a wide range of incidents, while fostering closer partnerships with suppliers and ensuring business continuity.

Moreover, the ongoing evolution of regulatory frameworks and industry standards will further emphasise the criticality of robust incident response planning and supplier collaboration. Organisations that proactively align their strategies with these evolving requirements will gain a competitive advantage and enhance their resilience in the face of disruptions.

As we look ahead, the successful streamlining of incident response planning and supplier collaboration will be a hallmark of organisational agility, resilience, and long-term success. By embracing this strategic imperative, organisations can navigate the complexities of the modern business landscape with confidence and emerge stronger, more prepared, and better positioned to thrive in an ever-changing world.

Notes

1 Kaur, G., Bharathiraja, N., Singh, K.D., Veeramanickam, M.R.M., Rodriguez, C. R., and Pradeepa, K., 2024. Emerging Trends in Cybersecurity Challenges with Reference to Pen Testing Tools in Society 5.0. *Artificial Intelligence and Society 5.0*, pp.196–212.

2 Rane, N., and Qureshi, A., 2024, April. Comparative Analysis of Automated Scanning and Manual Penetration Testing for Enhanced Cybersecurity. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–6). IEEE.

3 Van Buggenhout, E., 2024. Purple Teaming: A Comprehensive and Collaborative Approach to Cyber Security. *Cyber Security: A Peer-Reviewed Journal*, 7(3), pp.207–216.

4 Sontan, A.D., and Samuel, S.V., 2024. The Intersection of Artificial Intelligence and Cybersecurity: Challenges and Opportunities. *World Journal of Advanced Research and Reviews*, 21(2), pp.1720–1736.

5 Mohaidat, A.I., and Al-Helali, A., 2024. Web Vulnerability Scanning Tools: A Comprehensive Overview, Selection Guidance, and Cyber Security Recommendations. *International Journal of Research*, 10(1), pp.8–15.

6 Jimmy, F.N.U., 2024. Cyber Security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General Science (JAIGS)*, 2 (1), pp.129–171.

7 Seara, J.P., and Serrão, C., 2024. Automation of System Security Vulnerabilities Detection Using Open-Source Software. *Electronics*, 13(5), p.873.

8 Chand, P., 2024. Vulnerability Scanner Build a Tool that Scans a System For Potential Vulnerability. *International Journal for Modern Trends in Science and Technology*, 10(2), pp.143–150.

9 Aldabjan, A., Furnell, S., Carpent, X., and Papadaki, M., 2024. Cybersecurity Incident Response Readiness in Organisations. In *ICISSP* (pp.262–269).

10 Naseer, H., Desouza, K., Maynard, S.B., and Ahmad, A., 2024. Enabling Cybersecurity Incident Response Agility through Dynamic Capabilities: The Role of Real-time Analytics. *European Journal of Information Systems*, 33(2), pp.200–220.

11 Haber, M.J., and Rolls, D., 2024. Identity Threat Detection and Response (ITDR). In *Identity Attack Vectors: Strategically Designing and Implementing Identity Security*, Second Edition (pp.81–86). Berkeley, CA: Apress.

13

CYBERSECURITY TOOLING

SIEM, SOAR, and XDR

Security Information and Event Management (SIEM)

In today's digital landscape, where cyber threats are ever-evolving and becoming increasingly sophisticated, organisations must stay vigilant and proactive in safeguarding their critical assets.

Măcăneaă (2024) contends that *security information and event management (SIEM)* and *security orchestration, automation, and response (SOAR)* have emerged as powerful tools in the realm of cybersecurity, offering comprehensive defence mechanisms against potential breaches and attacks.[1]

To improve awareness, we will delve into the intricacies of SIEM and SOAR, exploring their key features and benefits, and the synergistic relationship between them in strengthening our cybersecurity defences.

Milson and Basit (2024) argue traditional security measures are often insufficient in keeping pace with the rapidly evolving threat landscape. This is where defence mechanisms like SIEM and SOAR come into play, offering a comprehensive and proactive approach to cybersecurity.[2]

The digital age has ushered in unprecedented opportunities for businesses and individuals alike, but it has also introduced a myriad of cybersecurity risks. From malware infections and phishing attempts to sophisticated advanced persistent threats (APTs) and data breaches, the potential consequences of a successful cyber attack can be devastating.

Manzoor et al. (2024) argue many organisations have tight budgets but there is always hope. Many open-source SIEM solutions are available to help in navigating the complexities of the cyber world. Whatever the budget is of your organisation, these technologies can help to fortify your cybersecurity posture.[3]

Security information and event management (SIEM) is a powerful technology that collects, analyses, and correlates security-related data from

DOI: 10.4324/9781003604969-13

various sources within an organisation. By aggregating and processing this data, SIEM solutions provide a centralised view of an organisation's security posture, enabling real-time monitoring, threat detection, and incident response.

Benefits of SIEM for cybersecurity include centralised log management. SIEM solutions collect and consolidate log data from diverse sources, such as firewalls, intrusion detection systems (IDS), antivirus software, and other security devices. This centralised log management streamlines the security monitoring process and ensures that no critical information is overlooked.

SIEM solutions employ advanced analytics and correlation techniques to identify patterns, anomalies, and potential threats within the collected data. By correlating events across multiple sources, SIEM can detect complex attack scenarios that might go unnoticed by individual security tools.

Real-time monitoring is essential. SIEM solutions continuously monitor the security environment, providing real-time alerts and notifications when potential threats or suspicious activities are detected. This enables organisations to respond promptly and mitigate risks before they escalate into full-blown incidents.

Many industries are subject to various regulatory requirements and compliance standards. SIEM solutions can assist organisations in meeting these obligations by generating comprehensive reports and audit trails, demonstrating adherence to security policies and regulations.

Incident investigation and forensics are a key priority. In the event of a security breach or incident, SIEM solutions can facilitate efficient investigation and forensic analysis. By providing a comprehensive view of security events and logs, SIEM can help organisations identify the root cause, scope, and impact of an incident, enabling more effective incident response and remediation efforts.

Security Orchestration, Automation, and Response (SOAR)

Security orchestration, automation, and response (SOAR) is a powerful cybersecurity solution that complements and enhances the capabilities of SIEM. SOAR solutions are designed to streamline and automate various security operations, enabling organisations to respond to threats more efficiently and effectively.

How SIEM and SOAR work together to strengthen cybersecurity defences is a key factor. While SIEM provides the foundation for collecting, analysing, and correlating security data, SOAR takes this a step further by automating and orchestrating the response to identified threats and incidents. The integration of SIEM and SOAR creates a powerful synergy, enhancing an organisation's overall cybersecurity posture.

SIEM solutions identify potential threats and prioritise them based on their severity and impact. This information is then seamlessly fed into the SOAR solution, which can initiate appropriate response actions.

SOAR solutions leverage predefined playbooks and workflows to automate various incident response tasks, such as containment, investigation, and remediation. This automation reduces the time and effort required for manual interventions, enabling faster and more efficient incident handling. SOAR solutions facilitate the orchestration of security operations by integrating with various security tools and platforms. This integration enables seamless collaboration and information sharing among different security teams, ensuring a coordinated and effective response to threats.

Case management is important. SOAR solutions provide comprehensive case management capabilities, allowing security teams to track and document the entire lifecycle of an incident, from detection to resolution. This streamlines the incident response process and improves overall efficiency and accountability. By capturing and analysing data from past incidents, SOAR solutions can identify areas for improvement and refine existing playbooks and workflows. This continuous learning and adaptation process enhances the effectiveness of an organisation's cybersecurity defences over time.

Implementing SIEM and SOAR solutions within an organisation requires careful planning and execution. Conduct a thorough assessment of your organisation's security requirements, risk profile, and existing security infrastructure. This will help you identify the specific capabilities and features you need from SIEM and SOAR solutions. Evaluate and select SIEM and SOAR solutions that align with your organisation's needs, budget, and existing IT infrastructure. Consider factors such as scalability, integration capabilities, and vendor support.

Ensure that your SIEM solution can effectively collect and normalise data from various sources within your organisation, including security devices, network infrastructure, and applications. Work closely with your security teams to develop and refine playbooks and workflows for incident response and automation within the SOAR solution. These playbooks should align with your organisation's security policies and best practices.

Provide comprehensive training to your security teams on the effective use of SIEM and SOAR solutions. Ensure that they understand the capabilities, workflows, and best practices for leveraging these technologies. Regularly review and optimise your SIEM and SOAR implementations to ensure they remain effective and aligned with your evolving security needs and the ever-changing threat landscape.

Best practices for optimising SIEM and SOAR solutions should be incorporated. To maximise the benefits of SIEM and SOAR solutions, it is essential to follow best practices and adopt a proactive approach to cybersecurity. Develop and implement well-defined security policies and procedures that govern the use of SIEM and SOAR solutions, as well as the overall incident response process.

Leverage threat intelligence feeds and integrate them with your SIEM and SOAR solutions. This will help you stay informed about the latest threats

and adjust your security posture accordingly. Identify and automate routine security tasks, such as patching, vulnerability scanning, and user account management, using the automation capabilities of your SOAR solution. This will free up valuable resources and reduce the risk of human error.

Foster collaboration and information sharing among different security teams and stakeholders within your organisation. This will ensure a coordinated and effective response to security incidents. Regularly assess and audit your SIEM and SOAR implementations, as well as your overall security posture. This will help identify areas for improvement and ensure compliance with industry standards and regulations.

Treat cybersecurity as an ongoing journey. Continuously refine and adapt your SIEM and SOAR solutions, playbooks, and workflows based on lessons learned, evolving threats, and changing business requirements.

The cybersecurity landscape is constantly evolving, and SIEM and SOAR technologies are continuously adapting to keep pace with emerging threats and technological advancements. The integration of artificial intelligence (AI) and machine learning (ML) capabilities into SIEM and SOAR solutions is expected to enhance their ability to detect and respond to threats more effectively. These technologies can help identify complex patterns, learn from historical data, and adapt to new threat scenarios.

As organisations increasingly adopt cloud computing and hybrid IT environments, SIEM and SOAR solutions will need to adapt to these deployment models. Cloud-based and hybrid SIEM and SOAR offerings will become more prevalent, providing scalability, flexibility, and cost-effectiveness.

The trend towards greater automation and orchestration in cybersecurity operations will continue. SOAR solutions will become more sophisticated, enabling seamless integration with a wider range of security tools and platforms, and facilitating more complex and adaptive incident response workflows.

User and entity behaviour analytics (UEBA) technology, which analyses user and entity behaviour patterns to detect anomalies and potential threats, is expected to be increasingly integrated into SIEM and SOAR solutions. This will enhance their ability to detect insider threats and advanced persistent threats (APTs).

As regulatory requirements and compliance standards evolve, SIEM and SOAR solutions will need to provide more comprehensive and automated compliance reporting capabilities. This will help organisations demonstrate adherence to various security and privacy regulations.

The sharing of threat intelligence among organisations and security communities is expected to become more prevalent. SIEM and SOAR solutions will need to facilitate seamless integration with threat intelligence platforms and enable efficient sharing of threat data and indicators of compromise (IoCs).

In the ever-evolving landscape of cybersecurity threats, organisations must adopt a proactive and comprehensive approach to safeguarding their critical

assets. SIEM and SOAR are powerful tools that can significantly enhance an organisation's cybersecurity posture.

By leveraging the capabilities of SIEM for centralised log management, advanced analytics, and real-time monitoring, organisations can gain a comprehensive view of their security environment and detect potential threats more effectively. SOAR solutions, on the other hand, enable organisations to automate and orchestrate their incident response efforts, streamlining the process and ensuring a more efficient and coordinated response to security incidents.

The synergistic relationship between SIEM and SOAR creates a formidable defence against cyber threats. By implementing these technologies and following best practices, organisations can stay ahead of the curve, mitigate risks, and protect their valuable assets from the ever-evolving threat landscape.

Extended Detection and Response (XDR)

In the ever-evolving landscape of cybersecurity, organisations face an array of advanced threats that can wreak havoc on their digital assets and operations. Conventional security measures often fall short in detecting and mitigating these sophisticated attacks, leaving businesses vulnerable to data breaches, financial losses, and reputational damage. Enter *extended detection and response (XDR),* an approach that promises to improve the way we defend against cyber threats.

Katulić at al. (2024) argue XDR is a comprehensive security solution that unifies and correlates data from multiple security products, providing a holistic view of an organisation's security posture. By integrating various security tools, such as endpoint protection, network security, cloud security, and threat intelligence, XDR enables seamless collaboration and information sharing, empowering security teams to detect, investigate, and respond to threats more effectively.[4]

Bassey et al. (2024) contend that organisations that do not allocate sufficient security budgets have no excuse. As the digital landscape continues to expand and threats become more sophisticated, the need for robust cybersecurity solutions like XDR has never been more crucial. They argue there are open-source tools available so organisations must understand the intricacies of XDR, its key features and benefits, and how it can fortify an organisation's defence against advanced threats.[5]

Advanced threats are highly sophisticated and targeted attacks designed to evade traditional security measures. These threats can take various forms, including APTs, zero-day exploits, ransomware, and supply chain attacks. They often leverage cutting-edge techniques, such as social engineering, malware obfuscation, and lateral movement within networks, making them challenging to detect and mitigate.

Traditional security solutions, while effective in addressing known threats, often struggle to keep pace with the ever-evolving landscape of advanced threats. Siloed security tools and lack of integration can lead to gaps in visibility, making it difficult to detect and respond to complex attacks effectively.

To combat these advanced threats, organisations require a holistic and integrated approach to cybersecurity. This is where XDR comes into play, offering a comprehensive solution that leverages the power of multiple security tools and provides a unified view of an organisation's security posture.

The journey towards XDR began with the advent of endpoint detection and response (EDR) solutions, which focused on monitoring and responding to threats at the endpoint level. While EDR provided enhanced visibility and response capabilities, it lacked the ability to correlate data from other security tools, limiting its effectiveness against advanced threats that span multiple attack vectors.

Next came the emergence of SIEM systems, which aggregated and analysed security logs from various sources. However, SIEM solutions often faced challenges in handling the vast volume of data and providing actionable insights, leading to alert fatigue and missed threats.

Recognising the limitations of siloed security solutions, the industry evolved towards a more integrated approach, giving rise to SOAR platforms. SOAR solutions aimed to streamline security operations by automating repetitive tasks and facilitating coordination between security tools. However, these solutions still lacked the comprehensive visibility and advanced analytics capabilities required to effectively combat advanced threats.

XDR emerged as the next logical step in this evolution, combining the strengths of EDR, SIEM, and SOAR while addressing their limitations. By integrating and correlating data from multiple security products, XDR provides a unified view of an organisation's security posture, enabling advanced threat detection, investigation, and response capabilities.

XDR offers a comprehensive set of features and capabilities that empower organisations to defend against advanced threats effectively. XDR collects and correlates data from various security tools, including endpoint protection, network security, cloud security, and threat intelligence feeds. This integrated approach provides a holistic view of an organisation's security posture, enabling the detection of threats that span multiple attack vectors.

XDR leverages advanced analytics and machine learning algorithms to identify patterns and anomalies in security data. This enables the detection of sophisticated threats that may evade traditional signature-based detection methods. XDR solutions often incorporate automation capabilities that streamline the investigation and response processes. This includes automated triage, threat hunting, and incident response workflows, reducing the time and effort required to mitigate threats.

XDR solutions integrate with various threat intelligence sources, providing security teams with up-to-date information on the latest threats, attack

vectors, and indicators of compromise (IoCs). This intelligence helps organisations stay ahead of emerging threats and proactively enhance their security posture.

XDR offers a centralised management console that provides a unified view of an organisation's security posture. This enables security teams to monitor and manage security events, investigations, and responses from a single pane of glass, improving efficiency and reducing the risk of missed threats. Many XDR solutions offer open integration capabilities, allowing organisations to incorporate additional security tools and data sources as needed. This extensibility ensures that the XDR solution can adapt to an organisation's evolving security requirements and technology stack.

Adopting XDR as part of an organisation's cybersecurity strategy offers numerous benefits. By integrating and correlating data from multiple security tools, XDR enhances an organisation's ability to detect and respond to advanced threats more effectively. This comprehensive approach reduces the risk of missed threats and enables faster incident response times.

XDR provides a unified view of an organisation's security posture, offering greater visibility and context into potential threats. This contextual awareness enables security teams to make better-informed decisions and prioritise their response efforts. XDR solutions automate various security tasks, such as triage, investigation, and response workflows. This automation reduces the workload on security teams, allowing them to focus on more strategic and high-impact activities.

By integrating data from multiple security tools, XDR facilitates better collaboration and information sharing among security teams. This cross-functional collaboration enhances threat intelligence and enables more effective threat mitigation strategies. By consolidating multiple security tools into a unified platform, XDR can help organisations reduce the complexity and costs associated with managing and maintaining separate security solutions.

XDR solutions are designed to be scalable and adaptable, allowing organisations to easily incorporate new security tools and data sources as their security requirements evolve.

Case Studies

To illustrate the effectiveness of XDR in defending against advanced threats, let's explore some real-world case studies.

A multinational corporation faced a sophisticated ransomware attack that targeted its critical systems and data. By leveraging the XDR solution's advanced analytics and threat intelligence integration, the security team was able to detect the initial intrusion, analyse the attack vector, and quickly isolate the affected systems. The XDR solution's automated response capabilities enabled the rapid deployment of countermeasures, minimising the impact of the attack and ensuring business continuity.

A US government agency was targeted by an APT group known for its stealthy tactics and advanced malware. The agency's XDR solution integrated data from multiple security tools, including endpoint protection, network security, and threat intelligence feeds. This comprehensive visibility enabled the security team to detect and track the APT group's lateral movement within the network, identify compromised systems, and effectively contain the threat.

A software development company fell victim to a supply chain attack, where malicious code was injected into one of their software components. The XDR solution's integration with the company's DevOps tools and continuous monitoring capabilities enabled the early detection of the compromised component. The security team was able to quickly investigate the incident, identify the root cause, and mitigate the threat before it could cause further damage.

XDR is powerful in defending against advanced threats, demonstrating its ability to provide comprehensive visibility, advanced analytics, and automated response capabilities.

Selection and Implementation

Selecting the appropriate XDR solution for your organisation is crucial to ensure effective defence against advanced threats. There are some factors to consider when choosing an XDR solution. Evaluate the XDR solution's ability to integrate with your existing security tools and data sources. Look for solutions that offer open integration and extensibility, allowing you to incorporate new security tools as your requirements evolve. Assess the XDR solution's advanced analytics and machine learning capabilities. Look for solutions that can effectively analyse and correlate data from multiple sources, identify patterns and anomalies, and provide actionable insights. Consider the XDR solution's automation and orchestration capabilities. Evaluate its ability to streamline investigation and response workflows, automate repetitive tasks, and facilitate seamless coordination between security teams and tools. Ensure that the XDR solution can scale to meet your organisation's growing security needs and handle large volumes of security data without compromising performance. Evaluate the vendor's expertise, reputation, and commitment to ongoing product development and support. A reliable vendor with a strong track record and dedicated support team can be invaluable in ensuring the successful implementation and management of the XDR solution. Consider your organisation's compliance and regulatory requirements, and ensure that the XDR solution can support and facilitate adherence to relevant standards and regulations.

By carefully evaluating these factors, you can select an XDR solution that aligns with your organisation's specific security requirements, infrastructure, and operational processes.

To maximise the benefits of XDR and ensure its effective implementation and management, organisations should develop a comprehensive security strategy that aligns with the organisation's goals, risk appetite, and regulatory requirements. Integrate XDR as a key component of this strategy, ensuring that it complements and enhances your existing security measures.

Perform a thorough assessment of your organisation's current security posture, identify gaps and vulnerabilities, and determine the specific requirements for an XDR solution. This assessment will guide the selection and implementation process. Engage cross-functional teams, including security operations, IT, and business stakeholders, throughout the implementation process. This collaborative approach ensures that the XDR solution aligns with the organisation's broader security and operational needs.

Invest in comprehensive training for your security teams to ensure they understand the XDR solution's capabilities, functionality, and best practices for effective utilisation. Define clear processes and workflows for incident detection, investigation, and response. Leverage the XDR solution's automation and orchestration capabilities to streamline these processes and improve operational efficiency.

Regularly monitor the XDR solution's performance, analyse security data and metrics, and optimise configurations and processes as needed. This continuous improvement approach ensures that the XDR solution remains effective and aligned with evolving security requirements. Foster strong partnerships with the XDR solution vendor and leverage their expertise, support, and product updates to stay ahead of emerging threats and maximise the value of the investment.

By following these best practices, organisations can effectively implement and manage their XDR solution, ensuring a robust defence against advanced threats while optimising operational efficiency and security effectiveness.

The field of XDR technology is rapidly evolving, and several exciting trends and advancements are on the horizon. As organisations increasingly adopt cloud computing and cloud-based services, the demand for cloud-native XDR solutions is growing. These solutions are designed to seamlessly integrate with cloud environments, providing comprehensive visibility and security across on-premises and cloud infrastructures.

Managed security service providers (MSSPs) and managed detection and response (MDR) providers are increasingly adopting XDR solutions to enhance their security offerings. This trend enables organisations to leverage the expertise and resources of these providers while benefitting from the advanced threat detection and response capabilities of XDR.

XDR solutions are expected to integrate with emerging technologies, such as artificial intelligence (AI), machine learning (ML), and blockchain. These integrations will further enhance threat detection, investigation, and response capabilities, leveraging advanced analytics and decentralised security models.

As XDR solutions continue to evolve, we can expect to see increased automation and orchestration capabilities. This will further streamline security operations, reduce manual intervention, and enable faster and more efficient threat mitigation. XDR solutions will continue to expand their integration with various threat intelligence sources, providing security teams with real-time insights into emerging threats and attack vectors. This will enable proactive threat hunting and enhance an organisation's overall security posture.

XDR vendors are focusing on enhancing the user experience and data visualisation capabilities of their solutions. This will enable security teams to better understand and interpret security data, facilitating more informed decision-making and effective threat management.

As the cybersecurity landscape continues to evolve, XDR technology will play a pivotal role in empowering organisations to defend against advanced threats effectively. By staying ahead of these trends and advancements, organisations can future-proof their security strategies and maintain a robust defence against emerging cyber threats.

In the ever-evolving landscape of cybersecurity, the threat of advanced attacks looms large, challenging organisations to stay vigilant and adopt cutting-edge security solutions. XDR emerges as a game-changer, offering a comprehensive and integrated approach to detecting and responding to advanced threats.

By unifying and correlating data from multiple security tools, XDR provides a holistic view of an organisation's security posture, enabling advanced threat detection, investigation, and response capabilities. With features like advanced analytics, automation, and threat intelligence integration, XDR empowers security teams to stay ahead of sophisticated adversaries and mitigate risks effectively.

Implementing XDR as part of a comprehensive cybersecurity strategy offers numerous benefits, including improved threat detection and response, enhanced visibility and context, increased operational efficiency, and reduced complexity and costs. Real-world case studies have demonstrated the effectiveness of XDR in defending against sophisticated threats, such as ransomware attacks, advanced persistent threats, and supply chain attacks.

As organisations navigate the complex cybersecurity landscape, choosing the right XDR solution and following best practices for implementation and management are crucial. By carefully evaluating integration capabilities, advanced analytics, automation, scalability, and vendor expertise, organisations can select an XDR solution that aligns with their specific requirements and infrastructure.

Looking ahead, the future of XDR technology is promising, with advancements in areas such as cloud-native solutions, managed services integration, emerging technology integration, increased automation, and expanded threat intelligence. Embracing these trends and advancements will

enable organisations to future-proof their security strategies and maintain a robust defence against emerging cyber threats.

Notes

1 Măcăneață, C., 2024. Overview of Security Information and Event Management Systems. *Informatica Economica*, 28(1).
2 Milson, S., and Basit, S., 2024. *Security Operations and Incident Response in Cybersecurity* (No. 11710). EasyChair.
3 Manzoor, J., Waleed, A., Jamali, A.F., and Masood, A., 2024. Cybersecurity on a Budget: Evaluating Security and Performance of Open-source SIEM Solutions for SMEs. *Plos One*, 19(3), p.e0301183.
4 Katulić, F., Groš, S., Sumina, D., and Erceg, I., 2024, March. Enhancing Industrial Automation and Control Systems Cybersecurity Using Endpoint Detection and Response Tools. In *International Conference on Science and Technology Education* (pp. 186–197). Cham: Springer Nature Switzerland.
5 Bassey, C., Chinda, E.T., and Idowu, S., 2024. Building a Scalable Security Operations Center: A Focus on Open-source Tools. *Journal of Engineering Research and Reports*, 26(7), pp.196–209.

14

EMERGING TECHNOLOGIES

AI, ML, Robotics, and Automation

Artificial Intelligence (AI)

Supply chain management has undergone a profound revolution, with organisations leveraging advanced technologies to streamline operations and enhance efficiency. However, this increased reliance on digital systems has also exposed supply chains to a myriad of cyber threats, making cybersecurity an indispensable component of modern supply chain management.

Shahani and Sehgal (2024) argue that cybersecurity breaches can have far-reaching consequences for supply chains, ranging from data breaches and intellectual property theft to operational disruptions and financial losses. A compromised supply chain can lead to a ripple effect, impacting multiple stakeholders, including suppliers, manufacturers, distributors, and customers. Consequently, ensuring the integrity and resilience of supply chain systems has become a top priority for organisations across various industries.[1]

Diaz et al. (2024) contend that as supply chains become increasingly interconnected and data-driven, the need for robust cybersecurity measures is paramount. Traditional approaches to cybersecurity may no longer be sufficient to address the complexities and ever-evolving threats in the digital landscape. This is where artificial intelligence (AI) and machine learning (ML) emerge as powerful tools, offering innovative solutions to enhance supply chain cybersecurity.[2]

Supply chain cybersecurity is a multifaceted challenge. Supply chains involve intricate networks of suppliers, vendors, and partners, each with their own systems and security protocols. Ensuring end-to-end security across this complex ecosystem is a daunting task. Supply chains rely heavily on the exchange of sensitive data, such as product specifications, inventory levels, and financial information. Protecting this data from unauthorised access, theft, or manipulation is crucial.

DOI: 10.4324/9781003604969-14

While external cyber threats are a significant concern, insider threats posed by disgruntled employees or compromised accounts can be equally devastating for supply chain security. Many supply chain operations still rely on legacy systems and outdated software, which can be more susceptible to cyber attacks due to unpatched vulnerabilities and limited security features.

Implementing robust cybersecurity measures can be resource-intensive, both in terms of financial investment and skilled personnel. Smaller organisations may face challenges in allocating adequate resources for supply chain cybersecurity.

To address these challenges effectively, organisations must adopt innovative approaches that leverage the power of AI and ML technologies.

AI has emerged as a game-changer in the realm of cybersecurity, offering advanced capabilities to detect, prevent, and respond to cyber threats. In the context of supply chain cybersecurity, AI plays a pivotal role. AI algorithms can analyse vast amounts of data from various sources, such as network traffic, user behaviour, and system logs, to identify potential cyber threats in real time. By recognising patterns and anomalies, AI can detect sophisticated attacks that might go unnoticed by traditional security measures.

Predictive analytics mean that AI models can be trained on historical data to predict future cyber threats and vulnerabilities. By anticipating potential risks, organisations can proactively implement mitigation strategies and strengthen their defences. AI-powered security systems can automate the response to cyber threats, taking immediate actions to contain and mitigate the impact of an attack. This rapid response capability is crucial in minimising the potential damage and ensuring business continuity.

AI can continuously monitor supply chain systems, networks, and endpoints, providing real-time visibility into potential security risks. This proactive monitoring approach enables organisations to stay ahead of emerging threats and take appropriate actions. AI algorithms can help with vulnerability assessment by analysing supply chain systems, identify vulnerabilities, and recommend remediation measures. This proactive approach helps organisations strengthen their security posture and reduce the risk of cyber attacks.

By leveraging AI capabilities, organisations can enhance their supply chain cybersecurity efforts, enabling more effective threat detection, proactive risk mitigation, and rapid response to cyber incidents.

Machine Learning (ML)

Machine learning (ML), a subset of AI, plays a crucial role in enhancing supply chain cybersecurity by enabling systems to learn and adapt from data without being explicitly programmed. ML algorithms can analyse vast amounts of data, identify patterns, and make intelligent decisions based on learned behaviours.

ML models can be trained to recognise normal patterns of behaviour within supply chain systems. By continuously monitoring system activity, these models can detect deviations from expected patterns, indicating potential cyber threats or anomalous activities.

ML algorithms can be used for user behaviour analytics to analyse user behaviour patterns, such as login attempts, data access patterns, and network activity. By establishing baselines for normal user behaviour, ML models can identify suspicious activities that may indicate compromised accounts or insider threats.

ML techniques can be employed to analyse code, executables, and network traffic to identify malware signatures or suspicious patterns that may indicate the presence of malicious software within the supply chain ecosystem. ML models can analyse financial transactions, purchase orders, and invoices to detect anomalies that may indicate fraudulent activities, such as unauthorised purchases or payments.

ML algorithms can continuously learn from new data and adapt their detection and response strategies accordingly. This adaptive capability enables supply chain security systems to stay ahead of evolving cyber threats and adjust their defences in real time.

With ML, organisations can enhance their supply chain cybersecurity posture, enabling proactive threat detection, automated response, and continuous learning and adaptation to emerging risks.

The adoption of AI and ML in supply chain cybersecurity is gaining momentum, with organisations across various industries recognising the benefits of these technologies. Pharmaceutical companies are using ML algorithms to monitor their supply chain networks for potential counterfeit products or deviations from established quality standards. These algorithms analyse data from various sources, such as product tracking systems, shipping logs, and customer feedback, to identify anomalies that may indicate counterfeit or substandard products.

Major retailers are employing AI-powered security systems to detect and prevent cyber threats targeting their supply chain operations. These systems leverage ML algorithms to analyse vast amounts of data, including customer transactions, inventory movements, and supplier interactions, to identify potential security risks or fraudulent activities.

Automotive manufacturers are leveraging AI and ML technologies to secure their connected vehicle supply chains. ML models are used to monitor and analyse data from various sources, such as vehicle telematics, component suppliers, and software updates, to detect potential cyber threats or vulnerabilities that could compromise vehicle safety and security.

Companies in the food and beverage industry are using ML-based systems to monitor their supply chain processes for potential food safety risks. These systems analyse data from sources like temperature sensors, transportation logs, and supplier certifications to identify deviations from established food safety protocols or potential contamination risks.

Defence contractors and military organisations are employing AI and ML technologies to secure their supply chains and protect sensitive information from cyber threats. These systems leverage ML algorithms to analyse data from various sources, including supplier networks, logistics operations, and personnel activities, to detect potential security breaches or insider threats.

These examples demonstrate the growing adoption of AI and ML in supply chain cybersecurity across diverse industries, highlighting the versatility and effectiveness of these technologies in addressing complex security challenges.

Implementation

Integrating AI and ML into supply chain cybersecurity requires a strategic approach that considers various factors, including data availability, infrastructure readiness, and organisational culture. AI and ML algorithms rely heavily on data to learn and make accurate predictions. Organisations must ensure that they have access to relevant and high-quality data sources, such as system logs, network traffic, user behaviour patterns, and supply chain transactions. Data cleansing and normalisation processes may be required to prepare the data for effective analysis.

Implementing AI and ML solutions often requires significant computational resources, including powerful hardware (e.g., GPUs, TPUs) and scalable cloud infrastructure. Organisations should assess their existing infrastructure and consider upgrading or adopting cloud-based solutions to support AI and ML workloads effectively.

Leveraging AI and ML for supply chain cybersecurity requires a skilled workforce with expertise in areas such as data science, machine learning, and cybersecurity. Organisations should invest in training and upskilling their existing workforce or consider hiring specialised talent to support the implementation and ongoing management of AI and ML solutions.

The deployment of AI and ML systems in supply chain cybersecurity must adhere to relevant regulations and industry standards. Organisations should establish robust governance frameworks, ensuring transparency, accountability, and ethical considerations in the development and use of these technologies.

AI and ML solutions should be seamlessly integrated with existing supply chain systems and cybersecurity tools. Automation capabilities can streamline processes, enabling real-time threat detection, automated response, and continuous monitoring of supply chain activities.

Continuous improvement: AI and ML models require ongoing training and optimisation to maintain their effectiveness and adapt to evolving cyber threats. Organisations should establish processes for continuous data collection, model retraining, and performance evaluation to ensure the long-term success of their AI and ML initiatives.

By following a structured approach and addressing these key considerations, organisations can effectively leverage AI and ML to enhance their supply chain cybersecurity posture and stay ahead of emerging cyber threats.

To maximise the benefits of AI and ML in supply chain cybersecurity, organisations should follow best practices that promote effective implementation, governance, and continuous improvement. Define a clear strategy for integrating AI and ML into supply chain cybersecurity, aligning it with the organisation's overall cybersecurity objectives and risk management framework.

Ensure the quality, completeness, and accuracy of the data used for training AI and ML models. Invest in data governance processes and tools to maintain data integrity throughout the supply chain. Engage with key stakeholders, including supply chain partners, cybersecurity experts, and data science teams, to foster collaboration and ensure the effective deployment of AI and ML solutions.

Establish rigorous testing and validation processes to ensure the reliability and accuracy of AI and ML models before deployment. Continuously monitor and evaluate model performance to identify and address potential biases or errors. Ensure transparency and explainability in the decision-making processes of AI and ML systems. This will facilitate trust, accountability, and compliance with relevant regulations and industry standards.

AI and ML models require continuous learning and adaptation to remain effective against evolving cyber threats. Establish processes for regular model retraining, incorporating new data and feedback from security incidents.

Prioritise security and privacy by implementing robust security measures to protect the AI and ML systems, as well as the data used for training and inference. Ensure compliance with data privacy regulations and best practices. Encourage a culture of innovation within the organisation, promoting the exploration and adoption of emerging AI and ML technologies in supply chain cybersecurity.

By adhering to these best practices, organisations can effectively integrate AI and ML into their supply chain cybersecurity strategies, enhancing their ability to detect and respond to cyber threats while promoting transparency, accountability, and continuous improvement.

As the adoption of AI and ML technologies in supply chain cybersecurity continues to grow, we can expect to see several exciting developments and advancements in the near future. AI and ML systems will become increasingly autonomous, capable of detecting, responding to, and mitigating cyber threats with minimal human intervention. This will enable faster response times and more effective threat containment, reducing the potential impact of cyber attacks on supply chain operations.

Predictive and proactive security is crucial. AI and ML models will become more sophisticated in predicting and identifying potential cyber

threats before they occur. This proactive approach will allow organisations to implement preventive measures and strengthen their defences against emerging threats.

Organisations will leverage federated learning techniques to collaboratively train AI and ML models on distributed data sets, without compromising data privacy or security. This collaborative approach will enable the development of more robust and effective cybersecurity models, benefitting the entire supply chain ecosystem.

AI and ML will be integrated with other emerging technologies, such as blockchain, Internet of Things (IoT), and 5G networks, to create comprehensive and secure supply chain solutions. This convergence will enable enhanced visibility, traceability, and security across the entire supply chain lifecycle.

As AI and ML systems become more prevalent in supply chain cybersecurity, there will be a growing emphasis on explainable AI (XAI) techniques. XAI will provide transparency and interpretability, enabling stakeholders to understand and trust the decision-making processes of these systems.

Organisations will prioritise the ethical development and deployment of AI and ML technologies in supply chain cybersecurity. Robust governance frameworks and ethical guidelines will be established to ensure fairness, accountability, and respect for privacy and human rights.

The demand for skilled professionals in AI, ML, and cybersecurity will continue to rise. Organisations will invest in continuous skills development programmes, fostering a workforce capable of leveraging these technologies effectively and adapting to the ever-evolving cybersecurity landscape.

As the future unfolds, the integration of AI and ML into supply chain cybersecurity will become increasingly crucial for organisations to stay ahead of cyber threats, maintain operational resilience, and protect their supply chain ecosystems.

Supply chains face an array of cybersecurity threats that can disrupt operations, compromise sensitive data, and inflict substantial financial losses. As we embrace the digital transformation, the integration of robotics and automation has emerged as a powerful solution to fortify supply chain cybersecurity. These cutting-edge technologies offer a multitude of advantages, revolutionising the way we approach supply chain security.

Podile et al. (2024) argue that *robotics and automation* have become indispensable tools in streamlining supply chain processes, enhancing efficiency, and minimising human error. By automating repetitive tasks and leveraging advanced sensors and algorithms, these technologies reduce the risk of cyber threats originating from human error or malicious intent. Furthermore, robotic systems can operate in environments that are hazardous or inaccessible to human workers, mitigating potential security vulnerabilities.[3]

Robotics and Automation

As we delve deeper into the realm of robotics and automation, it becomes evident that their impact extends far beyond operational optimisation. These technologies play a pivotal role in fortifying supply chain cybersecurity, safeguarding critical infrastructure, and ensuring the seamless flow of goods and services.

The benefits of incorporating robotics and automation are vast. The integration of robotics and automation in supply chain cybersecurity offers numerous advantages that transcend traditional security measures. By leveraging these cutting-edge technologies, organisations can bolster their defences against cyber threats, enhancing resilience and ensuring business continuity.

Increased accuracy and consistency are crucial. Robotic systems and automated processes minimise the potential for human error, which is often a significant vulnerability in cybersecurity. These technologies operate with precision and consistency, reducing the risk of accidental data breaches or security lapses. Advanced sensors and algorithms employed in robotics and automation enable real-time monitoring of supply chain operations. Anomalies or suspicious activities can be detected promptly, allowing for swift response and mitigation measures.

Robotic systems can be deployed to secure physical assets, such as warehouses, distribution centres, and transportation hubs. Automated surveillance, access control, and intrusion detection mechanisms fortify the physical security of supply chain infrastructure. Automated processes and robotic systems can encrypt sensitive data, ensuring its integrity and confidentiality throughout the supply chain. This safeguards against unauthorised access, data tampering, or theft.

As supply chain operations evolve and expand, robotics and automation can seamlessly scale and adapt to changing security requirements. This flexibility ensures that cybersecurity measures remain robust and effective, even in dynamic environments.

By harnessing the power of robotics and automation, organisations can proactively address cybersecurity challenges, mitigate risks, and foster a secure and resilient supply chain ecosystem.

Supply chains are inherently complex and interconnected, making them vulnerable to a wide range of cybersecurity threats. Understanding these threats is crucial for developing effective mitigation strategies and implementing robust security measures.

Supply chains are susceptible to various cyber attacks, such as malware infections, Distributed Denial of Service (DDoS) attacks, and advanced persistent threats (APTs). These attacks can disrupt operations, compromise sensitive data, and cause significant financial losses.

The vast amount of data exchanged within supply chains, including sensitive information like customer details, financial records, and intellectual

property, makes them prime targets for data breaches. Unauthorised access or theft of this data can have severe consequences.

Malicious insiders pose a significant risk to supply chain cybersecurity. Disgruntled employees, contractors, or third-party vendors with access to critical systems and data can exploit vulnerabilities or engage in sabotage.

Supply chains often involve numerous third-party vendors, suppliers, and service providers. A security breach or vulnerability in any of these entities can potentially compromise the entire supply chain ecosystem.

The proliferation of counterfeit products within the supply chain not only poses financial risks but also raises concerns about product safety and security. Counterfeit components or products may contain malicious code or backdoors, jeopardising the integrity of the supply chain.

By understanding these common cybersecurity threats, organisations can prioritise their security efforts, allocate resources effectively, and implement targeted measures to mitigate risks and protect their supply chain operations.

Robotics and automation offer a powerful arsenal of tools and techniques to address the cybersecurity risks faced by supply chains. By leveraging these technologies, organisations can proactively identify and mitigate potential vulnerabilities, enhancing the overall security posture of their supply chain operations.

Robotic systems and automated processes can continuously scan for vulnerabilities within the supply chain infrastructure, including hardware, software, and network components. Once vulnerabilities are identified, automated patching and remediation processes can be initiated, reducing the risk of exploitation.

Robotic process automation (RPA) for repetitive security tasks, such as log analysis, incident response, and compliance monitoring can improve speed. This not only improves efficiency but also minimises the risk of human error, ensuring consistent and reliable security operations.

Robotic intrusion detection and response can improve security. Advanced robotic systems equipped with sensors and intelligent algorithms can detect and respond to potential intrusions or security breaches in real time. These systems can autonomously initiate countermeasures, such as isolating compromised components or deploying virtual patches, minimising the impact of cyber attacks.

Automated processes and robotic systems can ensure secure data transfer and encryption throughout the supply chain. Sensitive information can be encrypted at rest and in transit, reducing the risk of data breaches and unauthorised access.

Robotics and automation can facilitate the creation and maintenance of comprehensive audit trails, enabling organisations to track and monitor supply chain activities for compliance purposes. Automated compliance monitoring ensures adherence to industry regulations and security best practices.

Case Studies

By integrating robotics and automation into their cybersecurity strategies, organisations can proactively identify and mitigate risks, respond swiftly to threats, and maintain a secure and resilient supply chain ecosystem.

Case Study 1: Automated Vulnerability Management in a Global Logistics Company

A leading global logistics company faced challenges in managing vulnerabilities across its vast network of warehouses, distribution centres, and transportation fleets. Manual vulnerability scanning and patching processes were time-consuming and prone to human error, leaving the company vulnerable to cyber threats.

To address this issue, the company implemented an automated vulnerability management solution powered by robotics and automation. Robotic systems continuously scanned the company's IT infrastructure, identifying vulnerabilities in real time. Once detected, automated patching processes were initiated, ensuring that vulnerabilities were promptly remediated without disrupting operations.

The implementation of this automated solution resulted in a significant reduction in the company's risk exposure, as well as improved operational efficiency and cost savings. The company experienced a 60% decrease in the time required for vulnerability remediation and a 75% reduction in security-related incidents.

Case Study 2: Robotic Intrusion Detection and Response in a Manufacturing Supply Chain

A multinational manufacturing company with a complex supply chain faced challenges in detecting and responding to cyber threats in a timely manner. Traditional security measures were reactive and often failed to keep pace with the evolving threat landscape.

To address this challenge, the company implemented a robotic intrusion detection and response system (IDRS) across its supply chain infrastructure. This system utilised advanced sensors, machine learning algorithms, and robotic response mechanisms to monitor and analyse network traffic, system logs, and user activities.

When a potential threat was detected, the IDRS automatically initiated countermeasures, such as isolating compromised systems, deploying virtual patches, and alerting security teams for further investigation and remediation.

The implementation of the robotic IDRS significantly enhanced the company's ability to detect and respond to cyber threats in real time, minimising

the impact of security incidents. The company reported a 90% reduction in the time required to detect and contain security breaches, and a substantial decrease in the overall cost of incident response.

These case studies demonstrate the transformative potential of robotics and automation in fortifying supply chain cybersecurity. By leveraging these cutting-edge technologies, organisations can stay ahead of evolving cyber threats, protect critical assets, and maintain business continuity.

Implementation

While the benefits of incorporating robotics and automation in supply chain cybersecurity are compelling, organisations must carefully consider several key factors to ensure successful implementation and maximise the potential of these technologies.

Cybersecurity by design is essential. When deploying robotic systems and automated processes, it is crucial to prioritise cybersecurity from the outset. Cybersecurity should be an integral part of the design and development process, ensuring that security measures are built-in and not treated as an afterthought.

Robotic systems and automated processes often handle sensitive data and perform critical operations. Implementing robust access controls, such as multi-factor authentication, role-based access, and encryption, is essential to prevent unauthorised access and ensure data integrity.

Robotics and automation introduce new attack vectors and potential vulnerabilities. Continuous monitoring and auditing of these systems are necessary to detect anomalies, identify security gaps, and ensure compliance with industry regulations and best practices.

Successful implementation and maintenance of robotics and automation in supply chain cybersecurity require a skilled and well-trained workforce. Organisations must invest in training programmes to develop the necessary expertise and ensure that personnel are equipped to manage and secure these advanced technologies.

Many robotics and automation solutions involve third-party vendors and service providers. It is crucial to conduct thorough risk assessments and implement robust vendor management processes to mitigate potential vulnerabilities introduced by external parties.

Despite the best security measures, cyber incidents can still occur. Organisations must develop comprehensive incident response and business continuity plans that incorporate robotics and automation, ensuring resilience and minimising disruptions in the event of a security breach.

By carefully considering these key factors and adopting a holistic approach, organisations can effectively leverage the power of robotics and automation to enhance supply chain cybersecurity, while mitigating potential risks and challenges.

The integration of robotics and automation in supply chain cybersecurity is just the beginning of a transformative journey. As technology continues to evolve, new trends and innovations are shaping the future of supply chain security.

AI and ML algorithms are becoming increasingly sophisticated, enabling robotic systems and automated processes to adapt and learn from data patterns, anomalies, and cyber threats. These technologies can enhance threat detection, predictive analytics, and autonomous decision-making capabilities, further bolstering supply chain cybersecurity. Blockchain and distributed ledger technologies offer immutable and transparent record-keeping, enabling secure and tamper-proof tracking of supply chain transactions and data. These technologies can enhance supply chain visibility, traceability, and integrity, mitigating the risk of counterfeit products and data tampering.

The proliferation of connected devices and sensors in supply chain operations, known as the IoT and IIoT, presents both opportunities and challenges. While these technologies enable real-time monitoring and automation, they also introduce new attack vectors and vulnerabilities. Robust security measures, including secure device onboarding, encryption, and access controls, are essential to mitigate IoT or related risks. Quantum computing promises to revolutionise various fields, including cybersecurity. Quantum-resistant cryptographic algorithms and quantum key distribution systems can enhance data security and protect against future quantum computing-based attacks on traditional encryption methods.

AR and VR technologies can be leveraged for enhanced situational awareness, training, and simulation in supply chain cybersecurity. These technologies can provide immersive environments for personnel to practise incident response, identify vulnerabilities, and develop skills in a controlled and safe environment.

As these emerging trends and technologies continue to evolve, organisations must stay vigilant, adapt their cybersecurity strategies, and embrace innovation to maintain a secure and resilient supply chain ecosystem.

While the benefits of incorporating robotics and automation in supply chain cybersecurity are significant, it is essential to acknowledge and address the potential challenges and limitations associated with these technologies.

Robotic systems and automated processes can themselves become targets for cyber attacks. Vulnerabilities in software, firmware, or communication protocols can be exploited by malicious actors, potentially leading to system compromise, data breaches, or disruption of operations.

Integrating robotics and automation into existing supply chain infrastructure can be complex and challenging. Compatibility issues, legacy systems, and disparate technologies may hinder seamless integration, requiring significant resources and expertise.

Robotic systems and automated processes rely heavily on the quality and accuracy of the data they process. Inaccurate or incomplete data can lead to

flawed decision-making, compromising the effectiveness of cybersecurity measures.

Implementing and maintaining advanced robotics and automation solutions can be capital-intensive and resource-intensive. Organisations may face financial constraints, particularly for small and medium-sized enterprises, limiting their ability to adopt these technologies.

The use of robotics and automation in supply chain cybersecurity may be subject to various regulatory requirements and industry standards. Organisations must ensure compliance with data privacy laws, cybersecurity regulations, and ethical guidelines to avoid legal and reputational risks.

The introduction of robotics and automation can disrupt existing workflows and processes, potentially leading to resistance from employees and stakeholders. Effective change management, training, and communication are crucial to overcome these challenges and foster a culture of innovation and adaptation.

To mitigate these challenges and limitations, organisations must adopt a strategic and holistic approach. This includes conducting thorough risk assessments, implementing robust security measures, investing in workforce training, and collaborating with industry partners and regulatory bodies to ensure compliance and best practices.

Notes

1 Shahani, N., and Sehgal, A., 2024. Impact of Cybersecurity and AI on Global Supply Chain and Economy. *International Journal of Marketing and Technology*, 14(6).

2 Diaz, R., Ungo, R., Smith, K., Haghnegahdar, L., Singh, B., and Phuong, T., 2024. Applications of AI/ML in Maritime Cyber Supply Chains. *Procedia Computer Science*, 232, pp.3247–3257.

3 Podile, V., Rameshkumar, P.M., and Divya, S., 2024. Assessing Cybersecurity Risks in the Age of Robotics and Automation: Frameworks and Strategies for Risk Management. In *Robotics and Automation in Industry 4.0* (pp. 215–228). CRC Press.

15

CONCLUSION

Enable Digital Resilience in Your Organisation

A Comprehensive Strategy

Cyber threats pose a significant risk to businesses, particularly those with complex supply chains. As organisations increasingly rely on digital technologies to streamline operations and enhance efficiency, the potential for cyber attacks has escalated. Malicious actors can exploit vulnerabilities in the supply chain, leading to data breaches, operational disruptions, financial losses, and reputational damage.

Cyber threats can manifest in various forms, including malware, phishing attacks, Distributed Denial of Service (DDoS) attacks, and advanced persistent threats (APTs). These threats can target any aspect of the supply chain, from raw material sourcing to manufacturing, distribution, and customer delivery. A single breach in the supply chain can have far-reaching consequences, affecting multiple stakeholders and potentially disrupting entire operations.

The impact of cyber threats on supply chain security cannot be overstated. A successful attack can result in the theft of sensitive data, such as intellectual property, trade secrets, or customer information. It can also disrupt production lines, delay shipments, and undermine customer trust. In some cases, cyber attacks can even lead to physical harm or environmental damage, particularly in industries that rely on critical infrastructure.

We have discussed how the importance of operational resilience in securing your supply chain is immeasurable. Operational resilience is a crucial component of supply chain security, enabling organisations to withstand and recover from disruptions, including cyber attacks. By fostering operational resilience, companies can minimise the impact of cyber threats and ensure business continuity, even in the face of adverse events.

DOI: 10.4324/9781003604969-15

Achieving operational resilience requires a holistic approach that encompasses people, processes, and technologies. It involves identifying critical assets and processes, implementing robust risk management strategies, and establishing contingency plans to maintain essential operations during and after a cyber incident.

Organisations with strong operational resilience are better equipped to respond swiftly and effectively to cyber threats, minimising downtime and reducing the potential for long-term consequences. They can quickly adapt to changing circumstances, leveraging redundancies and alternative suppliers or distribution channels to maintain supply chain operations.

Digital resilience is a multifaceted concept that encompasses various aspects of cybersecurity, risk management, and business continuity. It involves implementing a comprehensive strategy to protect digital assets, detect and respond to cyber threats, and recover from incidents while maintaining critical operations.

Ensuring the integrity, availability, and confidentiality of sensitive data through backup and recovery strategies, data governance policies, and secure data handling practices. Digital resilience relies on aspects including implementing robust cybersecurity measures to protect against cyber threats, such as firewalls, antivirus software, encryption, and access controls.

Maintaining the resilience of critical infrastructure, including networks, servers, and cloud environments, through redundancy, failover mechanisms, and disaster recovery planning. Developing and deploying resilient applications that can withstand cyber attacks, recover from failures, and maintain functionality during incidents.

Establishing resilient business processes that can adapt to disruptions, incorporating risk management practices, and leveraging automation and digitisation to enhance efficiency and agility. By addressing these components holistically, organisations can build a comprehensive digital resilience strategy that safeguards their supply chain operations from cyber threats and ensures business continuity.

Assessing and managing cyber risks in the supply chain is a critical step in building digital resilience. This process involves identifying potential vulnerabilities, evaluating the likelihood and impact of cyber threats, and implementing appropriate risk mitigation strategies.

We discussed how to effectively assess and manage cyber risks: organisations should consider developing a comprehensive understanding of the entire supply chain, including all stakeholders, processes, and dependencies. This mapping exercise helps identify potential entry points for cyber threats and areas of heightened risk.

Conduct regular risk assessments to identify and prioritise cyber risks within the supply chain. This assessment should consider factors such as the criticality of assets, the likelihood of threats, and the potential impact on operations. Implement a robust vendor risk management programme to assess and monitor the cybersecurity posture of third-party suppliers and

partners. This includes evaluating their security practices, conducting audits, and establishing contractual obligations for cybersecurity compliance.

Develop comprehensive incident response and recovery plans to address cyber incidents within the supply chain. These plans should outline roles and responsibilities, communication protocols, and step-by-step procedures for containment, eradication, and recovery. Regularly monitor and assess the effectiveness of risk mitigation strategies, and continuously improve security measures based on evolving cyber threats and industry best practices.

By proactively assessing and managing cyber risks, organisations can identify potential vulnerabilities, implement appropriate safeguards, and enhance the overall resilience of their supply chain operations.

We considered best practices for building digital resilience in your organisation. Building digital resilience requires a comprehensive approach that involves people, processes, and technologies.

Foster a culture of cybersecurity awareness and vigilance throughout the organisation. Provide regular training and education to employees, emphasising the importance of secure practices and their role in protecting digital assets.

Implement robust cybersecurity measures by deploying a multi-layered cybersecurity strategy that includes firewalls, intrusion detection and prevention systems, antivirus software, and encryption technologies. Regularly update and patch systems to address known vulnerabilities.

Develop detailed incident response and recovery plans that outline steps to detect, contain, and recover from cyber incidents. Regularly test and update these plans to ensure their effectiveness. Explore the use of cloud computing and automation technologies to enhance resilience and agility. Cloud services can provide scalability, redundancy, and disaster recovery capabilities, while automation can streamline processes and reduce human error.

Establish robust access controls and identity management practices to ensure that only authorised individuals have access to critical systems and data. Implement multi-factor authentication and regularly review and update access privileges. Perform periodic risk assessments and audits to identify vulnerabilities, evaluate the effectiveness of existing security measures, and prioritise areas for improvement.

Collaborate with industry partners, government agencies, and cybersecurity experts to share threat intelligence, best practices, and lessons learned. Participate in information-sharing platforms and initiatives to stay informed about emerging threats and mitigation strategies.

Regularly review and update your digital resilience strategy to align with evolving cyber threats, technological advancements, and industry best practices. Embrace a culture of continuous improvement and adaptation to maintain a strong cybersecurity posture.

By implementing these best practices, organisations can enhance their digital resilience, better protect their supply chain operations, and ensure business continuity in the face of cyber threats.

Case Studies

To illustrate the importance and effectiveness of digital resilience strategies, let's consider two final case studies of organisations that successfully implemented robust measures to secure their supply chain operations against cyber threats.

Case Study 1: Global Pharmaceutical Company: Pfizer[1]

Pfizer, a leading global pharmaceutical company, recognised the critical importance of supply chain security in ensuring the safe and timely delivery of life-saving medications to patients worldwide. To enhance digital resilience, the company implemented cross-institutional collaboration. Collaboration between CISOs across the pharma industry enabled an agreed supply chain security framework.

The company launched a comprehensive cybersecurity awareness programme, educating employees at all levels about potential threats, secure practices, and their role in maintaining a strong cybersecurity posture. A thorough risk assessment was conducted to identify vulnerabilities and potential entry points for cyber threats across the entire supply chain, from raw material sourcing to manufacturing and distribution.

A robust vendor risk management programme was established, requiring all third-party suppliers and partners to undergo rigorous cybersecurity assessments and adhere to stringent security standards. Detailed incident response and recovery plans were developed, outlining step-by-step procedures for detecting, containing, and recovering from cyber incidents. Regular tabletop exercises and simulations were conducted to test and refine these plans.

The company leveraged cloud computing and automation technologies to enhance resilience, scalability, and agility. Critical systems and data were migrated to secure cloud environments, and automated processes were implemented to streamline operations and reduce human error.

By implementing these digital resilience measures, Pfizer successfully mitigated cyber risks, maintained the integrity of its supply chain, and ensured the uninterrupted delivery of essential medications to patients worldwide.

Case Study 2: Automotive Manufacturer: Hyundai[2]

Hyundai, an automotive manufacturer, recognised the potential impact of cyber threats on its complex global supply chain, which involved numerous suppliers, manufacturing facilities, and distribution channels. To bolster digital resilience, the company took up cross-institutional information sharing. The Automotive Information Sharing and Analysis Center (Auto-ISAC) is an industry-driven community. They share and analyse intelligence about

emerging cybersecurity risks to the vehicle, and collectively enhance vehicle cybersecurity capabilities across the global automotive industry, including light- and heavy-duty vehicle OEMs, suppliers, and the commercial vehicle sector.

A dedicated cybersecurity governance structure was established, with clear roles and responsibilities defined for managing cyber risks across the organisation and supply chain. The company conducted a comprehensive mapping exercise to understand the intricate dependencies and vulnerabilities within its supply chain. This information was used to perform detailed risk assessments and prioritise risk mitigation efforts.

Significant investments were made in securing critical infrastructure, including networks, servers, and manufacturing systems. Additionally, a "secure by design" approach was adopted for developing resilient applications and software systems.

The automotive manufacturer actively participated in industry-wide collaboration and information-sharing initiatives, leveraging collective intelligence and best practices to enhance its cybersecurity posture. A robust cybersecurity monitoring and improvement programme was implemented, involving regular vulnerability assessments, penetration testing, and the continuous adaptation of security measures based on emerging threats and industry best practices.

Through these comprehensive digital resilience efforts, the automotive manufacturer significantly reduced the risk of cyber threats disrupting its supply chain operations, ensuring the timely delivery of vehicles and maintaining customer trust and satisfaction.

Training

We discussed how cybersecurity awareness and training plays a crucial role in ensuring the security of supply chain operations. Human error and lack of awareness can often be the weakest link in an organisation's cybersecurity defences, making it essential to cultivate a culture of security vigilance among employees.

Effective cybersecurity awareness and training programmes should be targeted. Educate employees about the various types of cyber threats, such as phishing attacks, malware, and social engineering tactics, and how they can impact supply chain operations.

Provide guidance on secure practices, including strong password management, identifying and reporting suspicious emails or activities, and handling sensitive data securely. Train employees on the appropriate steps to take in the event of a suspected or confirmed cyber incident, including reporting protocols and escalation procedures.

Tailor training programmes to address the specific cybersecurity risks and responsibilities associated with different roles within the supply chain, such as

procurement, logistics, and manufacturing. Implement ongoing awareness campaigns and refresher training sessions to reinforce cybersecurity best practices and ensure that employees remain vigilant against evolving threats.

Conduct simulated phishing exercises, tabletop exercises, and other interactive scenarios to test employees' ability to identify and respond to cyber threats in a controlled environment. By fostering a strong cybersecurity culture through comprehensive awareness and training programmes, organisations can empower their employees to become active participants in securing the supply chain against cyber threats.

Collaboration

We considered how collaborating with partners and suppliers to strengthen digital resilience is vital. Building digital resilience in the supply chain requires coordination among all stakeholders, including partners and suppliers. By working together and sharing information, organisations can collectively enhance their cybersecurity posture and better protect the entire supply chain ecosystem.

Effective collaboration with partners and suppliers is necessary. Establish clear cybersecurity requirements and standards that partners and suppliers must adhere to. These standards should cover areas such as data protection, incident response, access controls, and regular security assessments. Participate in industry-wide information-sharing platforms and initiatives to exchange threat intelligence, best practices, and lessons learned. This collaborative approach helps identify and mitigate emerging cyber threats more effectively. Conduct joint risk assessments and audits with partners and suppliers to identify potential vulnerabilities and areas for improvement within the shared supply chain ecosystem. Develop coordinated incident response plans and communication protocols to ensure a swift and effective response in the event of a cyber incident affecting multiple stakeholders within the supply chain. Collaborate on developing and delivering cybersecurity awareness and training programmes tailored to the specific needs and risks of the supply chain ecosystem. Foster an environment of continuous improvement and innovation by exploring new technologies, processes, and strategies to enhance digital resilience within the supply chain.

By fostering collaboration and leveraging the collective expertise and resources of partners and suppliers, organisations can create a more resilient and secure supply chain ecosystem, better equipped to withstand and recover from cyber threats.

Emerging Trends

As digital technologies continue to evolve and cyber threats become increasingly sophisticated, the importance of digital resilience in supply chain

management will only grow. Organisations must stay ahead of the curve by anticipating and adapting to emerging trends and challenges.

The future of digital resilience will be based on the adoption of emerging technologies such as artificial intelligence (AI), machine learning, blockchain, and the Internet of Things (IoT). These will reshape supply chain operations. These technologies can enhance visibility, automation, and security, but they also introduce new vulnerabilities that must be addressed through robust digital resilience strategies.

As the demand for cybersecurity professionals continues to rise, organisations will need to invest in developing and retaining skilled talent to support their digital resilience efforts within the supply chain.

Evolving regulations and industry standards related to cybersecurity, data privacy, and supply chain transparency will drive the need for enhanced digital resilience measures and compliance frameworks. The increasing digitisation and automation of supply chain processes will necessitate stronger cybersecurity measures and resilient systems to protect against potential disruptions and cyber threats.

Collaborative efforts and information sharing among industry partners, government agencies, and cybersecurity experts will become even more critical in addressing the global nature of cyber threats and maintaining supply chain resilience. As cyber threats evolve, organisations must embrace a mindset of continuous adaptation and innovation, regularly reviewing and updating their digital resilience strategies to stay ahead of emerging risks.

By anticipating and proactively addressing these future trends and challenges, organisations can position themselves to maintain a competitive advantage and ensure the long-term resilience and security of their supply chain operations in an increasingly digital and interconnected world.

Notes

1 https://kpmg.com/us/en/insights-by-industry/insights-healthcare-life-sciences/pharma-leaders-supply-chain-security-framework.html.
2 https://www.isao.org/group/automotive-isac.

APPENDICES

Appendix A – Example SCM Policy (SMEs)

Purpose

This policy describes the minimum requirements for managing information risks resulting from the utilisation of a supplier's services and/or products.

All new supplier relationships must comply with these requirements by [*Insert Date*].

All existing supplier relationships must comply with these requirements by [*Insert Date*].

Scope

All supplier relationships (including IT and non-IT relationships) are in scope for this policy and its supporting documentation.

Due to the unique requirements of contracting with government and regulatory agencies, exceptions may be made to the scope of this policy.

Definitions

- Commercial off-the-shelf or commercially available off-the-shelf (COTS) products: Packaged solutions which are adapted to satisfy the needs of the organisation making the purchase, rather than the commissioning of custom-made solutions.
- Contractual Documents: Legally binding and appropriately signed legal documents between Organisation and the Supplier. They can take

multiple forms such as Master Service Agreements, Amendment, Addendum, Task Order, Statement of Work, etc.

- Cybersecurity: The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
- Executive Sponsor: Organisational leader with the accountability for the business risks that originate from the utilisation of a Supplier's services and/or products and is able to influence and obtain organisational resources to address those risks.
- Relationship Owner: Organisation employee who is accountable for the relationship with the Supplier. Relationship Owners can delegate their responsibilities but not their accountability. A Relationship Owner:

  a Is the primary Organisation point of contact for the Supplier.
  b Consults with the Global Sourcing and Procurement function and collaborates with other relationship owners, where a Supplier has multiple engagements with Organisation, to provide comprehensive oversite to the relationship.
  c Understands and stays updated about the services and/or products provided by the Supplier.

- Collaborates with appropriate IT functions to manage Supplier information risks.
- Supplier(s): Broadly interpreted to include any individual or entity that provides any type of service and/or product to Organisation. Also, commonly referred to as "vendor", "service provider", "consultant", "external partner", "third party", or "business partner".
- Supplier Information Risk Management: Risk Management practices employed to identify, manage, and mitigate the level of information risk resulting from the utilisation of a Supplier's services and/or products.
- Supplier Relationship: Any engagement with a Supplier responsible for handling Company information, paid or unpaid, resulting from a legally binding contract. One or more contracts can constitute a single supplier relationship.

Requirements

This policy follows the Supplier relationship through four different phases. These phases include: Pre-contracting Due Diligence, Contracting, Supplier Governance and Ongoing Monitoring, Expiration/termination of Supplier Contract and Relationship. These phases account for the overall life cycle of a supplier relationship.

Since this policy is taking the life cycle approach to managing Supplier risks, the role of Relationship Owner becomes critically important to manage

Supplier risks. This role's responsibilities are discussed in the following sections and are spread across all the phases of the relationship.

Pre-contracting Due Diligence

1. Prior to signing off on a contract, the following requirements must be met. Government or regulatory agencies are exempt from this requirement when the type of engagement does not permit it.

1.1 The Supplier must demonstrate a current, valid, and appropriate certification of cybersecurity posture.
1.2 If the Supplier does not demonstrate a current, valid, and appropriate certification, a risk assessment must be performed.
1.3 Relationship Owners must plan for and complete the remediation of identified gaps uncovered by the risk assessment in a satisfactory timeframe after signing off on the contract, or as agreed by the executive sponsor.

Supplier Contracting

2. Relationship Owners must ensure the following security requirements are met or as needed defined in contracts or service agreements:

2.1 Suppliers must hold and maintain current, relevant, and appropriate certifications and/or attestations when the services and/or products provided need to comply with laws or regulations requiring such certifications (e.g., PCI-DSS).
2.2 Ensure contracts incorporate a right to audit the Supplier or the right to obtain evidence of an independent audit (e.g., Statement on Standards for Attestation Engagements (SSAE) No. 16 type SOC2, or International Standard on Assurance Engagements (ISAE) 3402).
2.3 Where relevant (e.g., externally hosted systems or applications, SaaS, Cloud, etc.), ensure the contract incorporates a right to perform or request evidence of vulnerability scans of Supplier information systems that host or process company information.
2.4 Changes in Supplier personnel with access to Organisation information including changes in role must be communicated to affected Relationship Owners as soon as possible.
2.5 When Suppliers providing services to Organisation engage with additional suppliers (e.g., 4^{th} or 5^{th} party suppliers/aggregators, subcontractors, etc.), the information risk management terms and conditions of our contract are applicable to their lower-tier agreements as well.
2.6 Supplier access to internal systems and data must require use of credentials that meet minimum criteria established by Organisation and Relationship Owners must ensure access by authorised supplier personnel only.

Supplier Governance and Ongoing Monitoring

1. Managers of Relationship Owners must ensure new Relationship Owners are assigned when there is a change in the Relationship Owner for a given Supplier.
2. When a Supplier has multiple relationships with the organisation, all associated Relationship Owners must participate in the governance of the Supplier.
3. When modifications are made to an existing Supplier relationship that result in changes to our Organisation's information systems or changes in the access to Organisation information, the Supplier risk assessment must be refreshed.
4. Relationship Owners must ensure that the Supplier's access to Organisation information assets is appropriately updated when personnel change notifications are received from the Supplier. Access changes must be implemented in line with the Organisation's own information security policy.
5. Ensure information exchanges occur over connections that are secure, authorised, maintained, and terminated when the engagement ends or the scope of the Supplier relationship changes.

7.1 The Organisation must conduct an annual review of established information exchange connections between the Organisation and Suppliers and take appropriate action.

Expiration/termination of Supplier Contracts and Relationship

Suppliers may have one or more contracts with the Organisation. In a single-contract relationship, the expiration or termination of the contract results in the termination of the entire relationship with the Supplier. In multiple-contract relationships where additional contracts are still in effect, the expiration or termination of a single contract does not necessarily result in the expiration or termination of the entire relationship. In those cases, follow the requirements outlined in the contract that has expired or is being terminated.

1. Where information is not stored on Organisation-managed infrastructure, Relationship Owners must ensure that Organisation information is returned securely to Organisation at the end of the relationship or upon expiration or termination of the relationship, unless agreed upon in the original contract. This includes both electronic and non-electronic information.
2. When the Supplier hosts or processes Organisation information using its own information systems, Relationship Owners must ensure that after the required information has been returned to Organisation, the

Supplier securely erases or destroys Organisation information from its information systems including backup and archival media and provides evidence that the information was securely erased or destroyed, unless agreed upon in the original contract.

3. Access by Supplier personnel to Organisation information and information systems must be removed as part of the expiration or termination of Supplier relationships. Any physical connections (e.g., site-to-site VPN) and system-to-system integrations must also be disconnected as part of the expiration or termination of the relationship.
4. Where applicable, Relationship Owners must also ensure that the Organisation's information assets (e.g., laptops or mobile devices etc.) are securely returned to the Organisation at the end of the relationship without erasing the contents, unless agreed upon in the original contract. The proper disposition of Organisation's software licences must also be addressed as part of this process.

Document Content Approvals

Approval:	
Individual Role	{Signature/Date}
Any signature qualification/caveat	

Version History

Version:	*Date:*	*Author:*	*Description:*
1.0	01-JAN-2025	Name	Description of version/change

Appendix B – Supply Chain Risk & Security Templates

These can be viewed at: https://www.smartsheet.com/content/supply-chain-risk-assessment-templates.

Supplemental files include:

- Supplier Risk Assessment Checklist Template.
- Supplier Risk Assessment Template with Scorecard.
- Supply Chain Risk Assessment Template.
- Supplier Security Risk Assessment Template.

Appendix C – Example Contractual Clauses

Instructions

The following cover-page section and the clauses are to be properly numbered and inserted where appropriate in the agreement being negotiated. All paragraph styles, formatting, numbering, definitions, etc. must be conformed to the agreement into which this is being inserted.

The Requirements for Information Security are divided in two separate sections.

- ***Core requirements*** are applicable to all relationship types and are, in my opinion, an essential baseline for any cybersecurity contractual language – the controls implemented to achieve compliance with NIST CSF.
- ***Supplemental requirements*** are based on the type of supplier relationship and are additive in nature. This means if your supplier falls in multiple categories, you should add requirements from all the applicable categories.

Contract Template

Core (Mandatory) Requirements

Cybersecurity Policy, Training, and Awareness

1. The Supplier shall have documented information security policies in place, refreshed annually, to ensure the confidentiality, integrity, and availability of Supplier and Company Information. These policies shall cover all business geographies and business functions of the Supplier, including their own subcontractors/suppliers. These policies shall address the following core and supplemental requirements detailed in the agreed contract and shall ensure that enforcement mechanisms including training and awareness exist.

Asset and Change Management

2. The Supplier shall maintain inventory of its information system assets, refreshed annually, that documents the identification, ownership, usage, location, and configuration for each item. The Supplier shall ensure that changes to assets follow a documented change management procedure.

Access Control

3. The Supplier shall be accountable for providing appropriate identity management for authentication and authorisation according to the principle of least privilege. The supplier shall have a documented process for provisioning and deprovisioning of access (including elevated privileges) to their physical facilities and information system assets which must include independent approval, a formal periodic review of access (at least annually) and timely removal of access.
4. The Supplier shall limit elevated privileges to the minimum number of users needed for effective operations and shall actively manage such privileges by reviewing periodically at a reasonable frequency higher than the general user access review and revoking immediately when no longer needed.

Network Security

5. The Supplier shall allow inbound access into their organisation's network with explicit approach, the default rule being to deny all inbound traffic. The Supplier shall restrict access to assets with potentially high impact by use of further internal network segmentation.
6. The Supplier shall restrict physical access to information system assets to authorised personnel.
7. The Supplier shall implement controls to protect information system assets from potential malicious activities which penetrate the first line of a layered defence as established by firewalls and other such controls. The Supplier shall implement intrusion prevention and intrusion detection controls and configure them to update automatically.

Endpoint Protection

8. The Supplier shall implement an anti-malware solution which shall include a local firewall capability on their workstations, servers, and mobile devices. The solution shall prevent disabling by end users and shall automatically receive updates on a regular basis. The solution shall perform both real-time and periodic scans.
9. The Supplier shall ensure that end users who are not designated administrator do not have system administrator permissions, including permissions to install or modify software on the endpoint.

10. The Supplier shall ensure that security patches are monitored, reviewed, and applied to all end points in line with the guidance given by the software provider.
11. The Supplier shall ensure that use of administrator and elevated privileges requires multifactor authentication.
12. The Supplier shall ensure that all manufacturer default user IDs and passwords in the software and technology devices are changed upon installation of the software or device.

Email Protection

13. Supplier email systems shall support encryption in transit via TLS 1.2 and above and DMARC standards. The Supplier shall conduct awareness and training specific to phishing.

Vulnerability and Patch Management

14. The Supplier shall employ a vulnerability scanning solution to detect security vulnerabilities in systems and externally facing websites hosted within their environment and remediate detected gaps in a timely manner. The process must incorporate a defined patch management cycle and controlled changes to configuration.
15. The Supplier shall subscribe to appropriate threat intelligence sources (examples including but not limited to NCSC CISP, US-CERT, not-for-profit ISAC groups).

Incident Response

16. The Supplier shall implement a procedure to respond to security or privacy incidents and shall perform detailed investigation and response activities to assist in identification, containment, eradication, and recovery actions for potential security incidents.

Supplemental Requirements based on Type of Supplier Relationship

1 Suppliers that are mission-critical to Buyer's business with or without data access

Adoption of the core (mandatory) requirements referenced above is recommended to be supplemented with additional guidance (such as legal counsel) for Supplier relationships that fall into this category.

2 Suppliers with direct connectivity and/or access to your organisation's information system assets and/or data

If the Supplier becomes aware that a Cybersecurity Event has or may have occurred, the Supplier and/or service provider designated to act on behalf of the Supplier shall conduct a prompt investigation and notify the Organisation immediately, disclosing all known Indicators of Compromise.

The Supplier shall notify the Organisation immediately when Supplier employees and contractors with access to the Organisation's information system assets no longer require that access to perform their job functions.

3 Suppliers that host/manage applications used by the Organisation, or the Organisation's data on their own infrastructure

a If the Supplier becomes aware that a Cybersecurity Event has or may have occurred, the Supplier and/or service provider designated to act on behalf of the Supplier shall conduct a prompt investigation and notify the Organisation immediately, disclosing all known Indicators of Compromise.

b The Supplier shall encrypt any of the Organisation's data in storage on all media types and when in transit outside of the Supplier's network. Encryption keys shall be periodically rotated and stored separately from the encrypted data. Supplier shall adequately protect the keys from loss/destruction or unauthorised access.

c The Supplier shall employ a Data Loss Prevention solution configured to detect unexpected or unauthorised transference of the Organisation's data within or outside the supplier's network.

d Any software code that the Supplier builds and maintains as part of its services to the Organisation shall undergo peer review by a qualified individual (other than the developer of the code) and code scanning with an automated tool to ensure that malicious or dangerous coding bugs and/or logical design flaws are detected and remediated before they are moved into the production environment.

e Any software that the Supplier builds and maintains as part of its services to the Organisation shall undergo security penetration testing performed by a qualified individual at least annually or with the deployment of any major change, in order to highlight security vulnerabilities in the software that are exploitable by malicious actors. Any exploitable vulnerabilities detected in this process shall be remediated within a reasonable timeframe not to exceed 30 days.

f In the event of termination of the contract, the Supplier shall return the Organisation's data to the Organisation in readable format including any equipment or software necessary to access the data. The Supplier shall destroy all other copies of the Organisation's data following confirmation

from the Organisation that the returned data is readable and accessible unless the contract explicitly permits retention.

4 Suppliers of IoT devices or Software as a Device

a The Supplier shall provide one or more current, available, and supported endpoint protection solutions approved to be installed on the smart device acquired by the Organisation without impact on the terms or duration of the warranty provided by the Supplier over the equipment.
b The Supplier shall integrate cybersecurity risk assessment, security architectural design analysis, security requirements, and security testing into its Quality Management System.
    i The Supplier shall inform the Organisation of the presence of any exploitable security vulnerability which risks or materially impacts the expected function of the acquired device immediately and provide a patch within 30 days of the vulnerability being reported to the Supplier.
c The Supplier shall comply with the regulatory guidance for pre- and post-market management of cybersecurity in smart devices.

5 Suppliers Operating in High-risk Geographies

The Supplier shall employ a Data Loss Prevention solution configured to detect unexpected or unauthorised transference of the Organisation's data within or outside the supplier's network.
The Supplier shall implement segmentation capabilities that enable immediate isolation of operations in the high-risk geography from the rest of the Supplier's operations in the event of a cybersecurity incident.

6 Suppliers of COTS Products Hosted/installed at Buyer

a If the Supplier becomes aware that a Cybersecurity Event has or may have occurred, the Supplier and/or service provider designated to act on behalf of the Supplier shall conduct a prompt investigation and notify the Organisation immediately, disclosing all known Indicators of Compromise.
b Any software code that the Supplier builds and maintains as part of its services to the Organisation shall undergo peer review by a qualified individual (other than the developer of the code) and code scanning with an automated tool to ensure that malicious or dangerous coding bugs and/or logical design flaws are detected and remediated before they are moved into the production environment.

c Any software that the Supplier builds and maintains as part of its services to the Organisation shall undergo security penetration testing performed by a qualified individual at least annually or with the deployment of any major change, in order to highlight security vulnerabilities in the software that are exploitable by malicious actors. Any exploitable vulnerabilities detected in this process shall be remediated within a reasonable timeframe not to exceed 30 days.

Appendix D – Example Supplier Cybersecurity KPIs

The Supplier agrees to track the following cybersecurity indicators on a monthly frequency, and to provide, upon Buyer request, with the data for those indicators for the past 12 months within 10 business days of the Buyer's request to the Supplier up to 4 times per year. These indicators shall also be reviewed at least annually as part of Performance Management Meetings.
1. Month-on-month percentage of its systems which are fully patched and up to date, broken out by the following groupings:

- Workstations.
- Internally facing servers.
- Internet-facing systems to include routers, firewalls, VPN termination points, and servers.

[KPI Targets:

- *Workstations: 95%*
- *Internal servers: 85%*
- *Routers, FW, VPN, Citrix, externally facing: 99%]*

2. Month-on-month percentage of their internet-facing applications scanned by Dynamic Application Security Testing tool within the last 30 days and the Mean Time to Resolve (MTTR) vulnerabilities with a CVSS score of 8 and above.

[KPI Targets:

- *Month-on-Month %: 95%*
- *MTTR: <30 Days]*

3. Month-on-month percentage of their servers scanned for vulnerabilities with an automated vulnerability scanning tool within the last 30 days and the Mean Time to Resolve vulnerabilities with a CVSS score of 8 and above.

[KPI Targets:

- *Month-on-Month %: 95%*
- *MTTR: <30 Days]*

4. Month-on-month percentage of servers and/or workstations running anti-virus and that have had signatures refreshed within at least the last 1 week.

[KPI Targets:

- *Workstations: 95%*
- *Servers: 99%]*

5. Month-on-month percentage of users with administrator privileges at the operating system level to servers and workstations.

[KPI Targets:

- *Less than 5%]*

6. Number of intrusions/attempts detected by Security Operations Centre in the last quarter and the Mean Time to Resolve these incidents.

[KPI Targets:

- *Improving quarter-on-quarter trend]*

7. Percentage of systems critical to operate Buyer's services that have been successfully tested for restore from back-up in the last 12 months.

[KPI Target:

- *>90%]*

8. Month-on-month percentage of inbound email blocked as malicious/grey/spam/low reputation.

[KPI Targets:

- *>90%]*

9. Month-on-month percentage of users with access to its network who have completed basic cybersecurity training within the last 12 months.

[KPI Targets:

- *>90%]*

10. Month-on-month percentage of connected third parties with a vendor security risk assessment updated in the past 24 months and contractual language in their contracts with the Supplier which require cybersecurity controls.

[KPI Targets:

- *>90%]***Appendix E – Example Supplier Privacy and Security Incident Response Guide**

Understanding the details of a supplier's security or privacy incident is important to determine the risk to your organisation's infrastructure as well as the extent to which your data may have been exposed. Quickly gathering information is necessary in order to determine the steps your organisation should take to further mitigate the issue and provide any required notifications to law enforcement, regulatory agencies, clients, and/or customers. Note that this list is not exhaustive as each security incident is different and may require additional research based on unique circumstances.

Supplier Contact Information/Incident Handlers

Name/title of the primary supplier contact:
Name of the supplier's Information Security/Technical team contact(s):
Name of supplier's legal counsel:
Phone numbers:
Email addresses:

Summary of the Security or Privacy Incident: The supplier should submit a summary explaining the incident. The summary, at minimum, should contain:

- Identification of the incident type (breach, unintended disclosure, etc.).
- Date the incident happened or date the incident started.
- Date the incident was discovered by the supplier.
- Date the supplier determined that your organisation's data may be involved.
- How the incident was identified and by whom.

Gather Incident Details: Ask the supplier to provide any details that are available at the time they report the incident to your organisation.

- How did the attacker gain access to the supplier's system(s) or data?

- Was phishing or social engineering used to compromise the system or trick users into providing data?
- What system vulnerabilities or weaknesses did the attacker exploit?
- Has the incident been contained and any affected systems secured?
- At what frequency will the supplier update your organisation as new information becomes available?

Determine the Impact of the Incident: Determine what type of information belonging to your organisation is (or may be) affected.

- What type(s) of data were or may have been compromised?
- How many total records were/may be involved in this incident?
- How many of the impacted records belong to your organisation?
- Was an analysis performed by the supplier's security team and/or did the supplier engage a third party to assist in the investigation (e.g., forensics, legal, or security firm)?
- Has data / system access / service been restored if systems were offline?

Mitigation: Collect information about the controls in place designed to prevent this type of incident. The information should include a description of what control(s) may have failed, the corrective actions taken, and planned control enhancements to prevent a reoccurrence of the incident.

- What controls were in place prior to this incident to prevent such an occurrence?
- What monitoring & alerting mechanisms were in place to detect the incident?
- Have immediate actions been taken to stop the attack and purge the attacker's access? If not, what actions are planned?
- What steps have been taken to address the root cause of the incident?

Notifications: The supplier should provide a list of communications about the incident, including those already sent and any that are planned for future release.

- Has the supplier communicated with affected individuals or organisations about the incident?
- Have any reports been provided to state or federal regulators? If so, please list.
- Has law enforcement (e.g., FBI, state police, other) been contacted?
- Does the supplier plan to initiate a press release?
- Will a notice be posted on the supplier's website?
- Will a copy of statements be provided for your organisation's advance review/feedback?

Post-Incident Assessment and Corrective Actions: The supplier should provide a description of their post-incident review and how lessons learned will be used to ensure proper risk mitigation is applied to the affected systems and processes. The following questions should be answered:

- Has the supplier determined the full extent of sensitive or protected information that was compromised?
- Has the supplier performed a formal risk assessment in response to this incident?
- What corrective actions or additional controls are planned and how long will implementation take?
- Has or will a third party produce a full report on the incident for the supplier's management team? Will the report be shared with your organisation?

Appendix F – NIST BIA & Contingency Planning Templates

NIST SP 800–34, Revision 1, Contingency Planning Guide for Federal Information Systems

These can be viewed at: https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

This publication assists organisations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. The guidance provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organisational resiliency, and the system development life cycle. This document provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities.

Supplemental files include:

- Business Impact Analysis (BIA) Template (docx).
- Contingency Planning: Low Impact System Template (docx).
- Contingency Planning: Moderate Impact System Template (docx).
- Contingency Planning: High Impact System Template (docx).

Appendix G – NIST SP 800-53 Templates

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organisations

This can be viewed at: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

This publication provides a catalogue of security and privacy controls for information systems and organisations to protect organisational operations and assets, individuals, other organisations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

Supplemental files include:

- Control Catalog Spreadsheet.

  The entire security and privacy control catalogue in spreadsheet format. Note: For a spreadsheet of control baselines, see the SP 800-53B details.

- Security and Privacy Control Collaboration Index Template (Excel & Word).

  The collaboration index template supports information security and privacy programme collaboration to help ensure that the objectives of both disciplines are met and that risks are appropriately managed. It is an optional tool for information security and privacy programmes to identify the degree of collaboration needed between security and privacy programmes with respect to the selection and/or implementation of controls in Rev. 5.

Appendix H – ISO 22301 Templates

ISO 22301 Quick Start Guide

These can be viewed at: https://www.smartsheet.com/content/iso-22301-business-continuity-guide

The ISO 22301 standard can provide benefits for your business continuity planning.

Supplemental files include:

- ISO 22301 Audit Checklist Template.
- ISO 22301 Self-Assessment Checklist Template.
- ISO 22301 Implementation Guide.
- ISO 22301 Simplified Cheat-Sheet.
- ISO 22301 Business Continuity Policy Template.
- ISO 22301 Business Continuity Template.
- ISO 22301 Business Continuity Sample.
- Disaster Recovery Plan Templates.
- Business Impact Analysis Template: https://www.smartsheet.com/business-impact-analysis-template
- Risk Management Template: https://www.smartsheet.com/all-risk-assessment-matrix-templates-you-need

INDEX

Page numbers in **bold** indicate Tables.