Hype Cycle for Cyber Risk Management, 2023

Published 25 July 2023 - ID G00793179 - 90 min read

By Analyst(s): Deepti Gopal, Sema Yuce, Michael Kranawetter

Initiatives: Cyber Risk; Meet Daily Cybersecurity Needs

Adopting cyber risk management technologies and concepts helps uncover the impacts of cyber risk and supports business and compliance goals. Security and risk management leaders should use this research to evaluate the impact of new and evolving solutions to inform appropriate adoption decisions.

Analysis

What You Need to Know

The disruptive impact of armed conflicts and climate change continues in 2023, and organizations continue to strive to find their “normal.” Geopolitical divide, misinformation, talent risk and inflation are all too familiar in nature. These challenges are compounded by the new, rapid and unconstrained development in and adoption of technology such as generative AI. Security and risk management leaders must focus on challenging the status quo and prepare to lead their organizations to a more resilient state. Cybercrime is not just a critical infrastructure challenge; it continues to gain momentum as a societal challenge as technology is intertwined in the lives of all people.

Organizations are evolving their cyber risk management programs by:

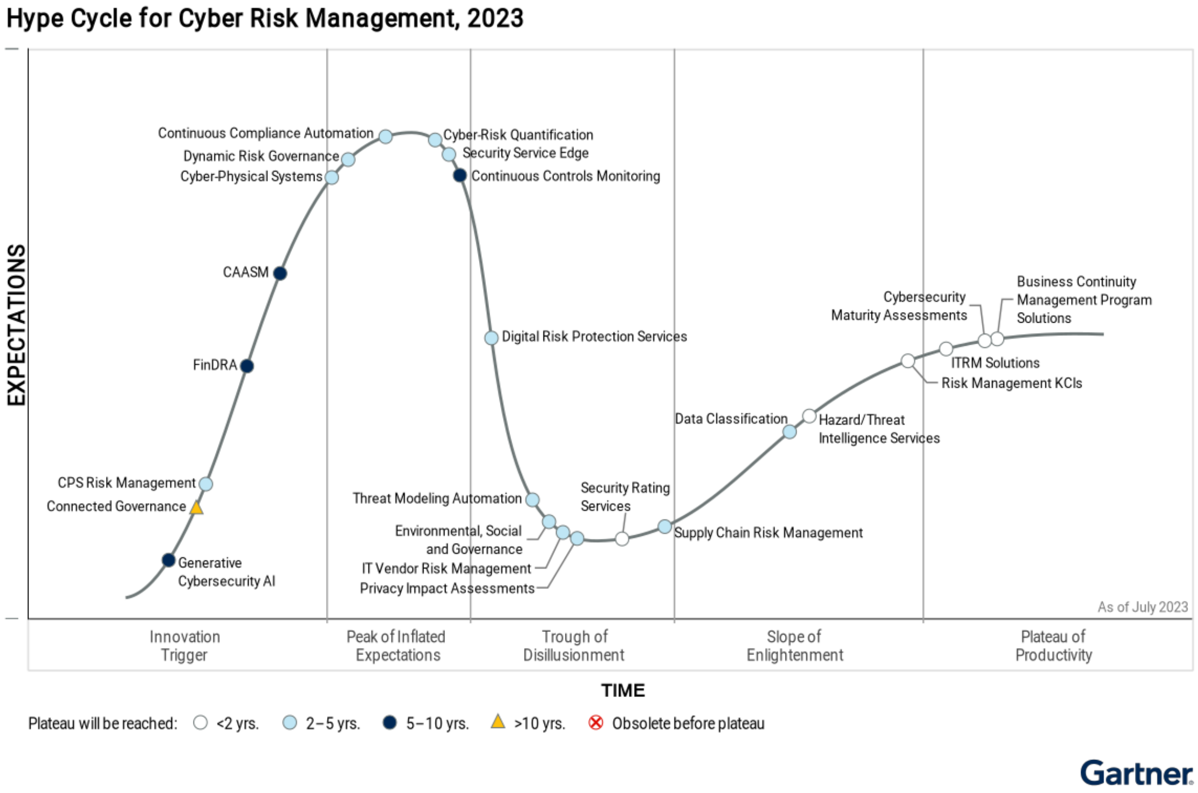
- Adapting risk identification and evaluation efforts to match the changing ways in which cyber risk is manifested due to rapid changes in technology, business and threat landscapes.
- Adopting agile exposure management and risk management techniques to support the digitization of business processes.
- Bringing balance to technology adoption and a cybersecurity-related friction reduction.

The Hype Cycle

This Hype Cycle for Cyber Risk Management describes the related concepts, methods, processes and technology solutions that organizations can use to develop programs to withstand risk events or seek risk-related opportunities. The impacts of rapidly evolving regulatory environments, ransomware, cyber attacks, and critical infrastructure and data breaches have changed the way cyber risk is manifesting in organizations.

This Hype Cycle demonstrates the need for organizations, including critical infrastructure operators, to respond, restructure and rebalance their approach to cyber risk management. The topics covered in this Hype Cycle provide risk insights that are required to support successful digital business outcomes.

Figure 1: Hype Cycle for Cyber Risk Management, 2023



The Priority Matrix

The average time required for the concepts and technologies included in this Hype Cycle to achieve mainstream adoption is less than five years. This is indicative of an evolving set of relevant concepts and technologies that are becoming best practices in their applicable areas.

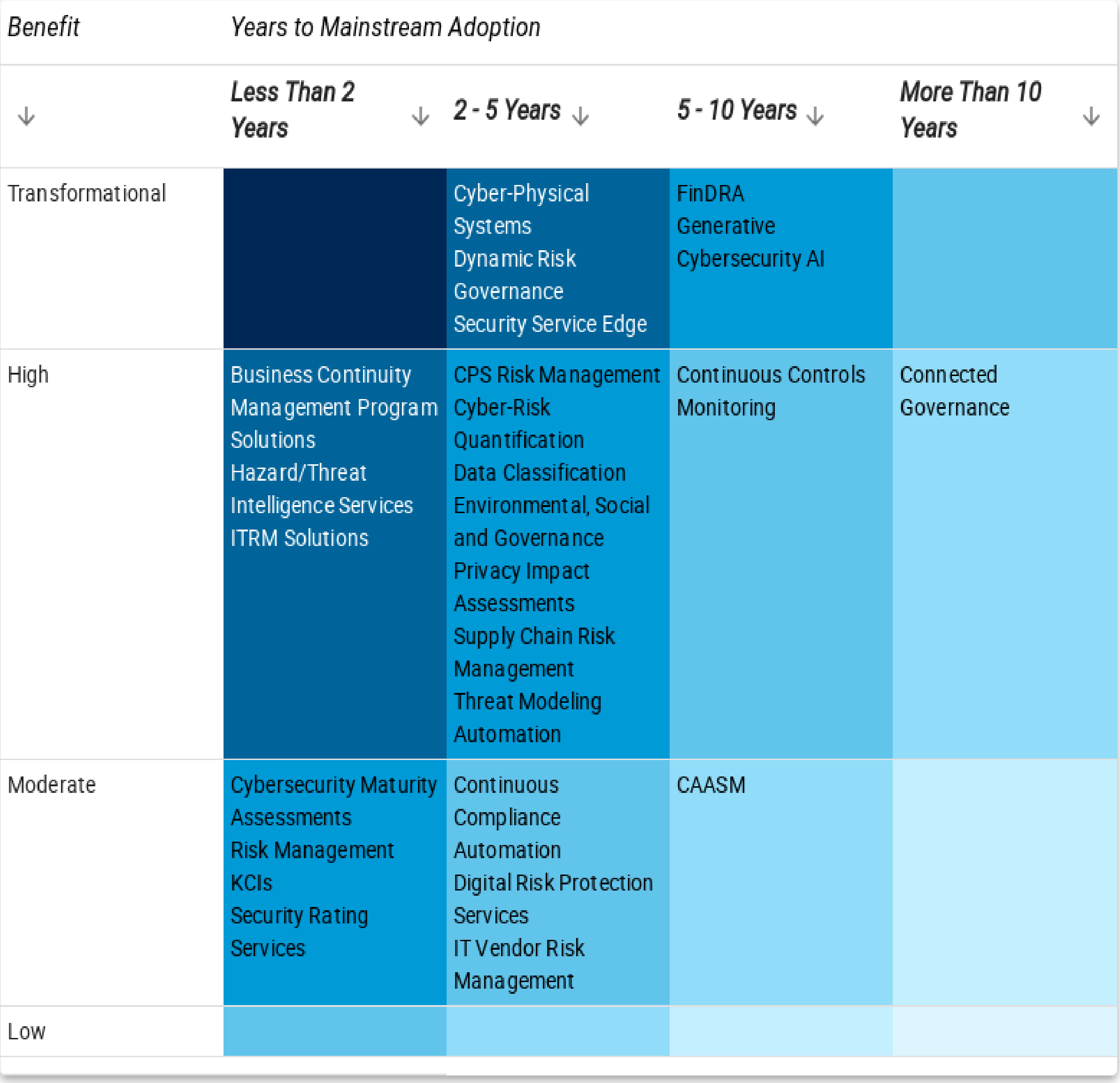
However, investments in risk management seldom provide immediate transformational benefits, and are designed to reduce risk and respond to changing threat landscape. As such, there is no easily quantifiable "return on investment."

Concepts and technologies such as dynamic risk governance could help scale decision making. Others, such as risk quantification and end-to-end supply chain management, offer additional insights into business impact and operational resilience and compliance. Based on Gartner customer inquiry trends and statistics and the further focus on cyber risk within the scope of this Hype Cycle, the changes from the 2022 version are:

- Two innovations have been removed due to fluctuations in mainstream adoption: IT risk appetite statements and cybersecurity performance management.
- Ethics and compliance management has reached the Plateau of Productivity and is no longer included.
- The innovation profile for application security requirements and threat modeling (ASRTM) has been simplified; it has been recast as "threat modeling automation" to reflect its evolution as a top practice in application development.
- CASB has reached the Plateau of Productivity and is replaced by secure service edge.
- Generative cybersecurity AI has been added to reflect the impact of GenAI.
- Continuous controls monitoring has been added to reflect new approaches for security controls management.

Table 1: Priority Matrix for Cyber Risk Management, 2023

(Enlarged table in Appendix)



Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		Cyber-Physical Systems Dynamic Risk Governance Security Service Edge	FinDRA Generative Cybersecurity AI	
High	Business Continuity Management Program Solutions Hazard/Threat Intelligence Services ITRM Solutions	CPS Risk Management Cyber-Risk Quantification Data Classification Environmental, Social and Governance Privacy Impact Assessments Supply Chain Risk Management Threat Modeling Automation	Continuous Controls Monitoring	Connected Governance
Moderate	Cybersecurity Maturity Assessments Risk Management KCIs Security Rating Services	Continuous Compliance Automation Digital Risk Protection Services IT Vendor Risk Management	CAASM	
Low				

Source: Gartner (July 2023)

On the Rise

Generative Cybersecurity AI

Analysis By: Jeremy D'Hoinne, Avivah Litan, Mark Horvath, Wilco van Ginkel

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Generative cybersecurity AI technologies generate new derived versions of security-related and other relevant content, strategies, designs and methods by learning from large repositories of original source data. Generative cybersecurity AI can be delivered as a public or privately hosted cloud service or embedded with security management interfaces. It can also integrate with software agents to take action.

Why This Is Important

Enterprises witness many applications leveraging foundation models that can read multimodal objects (such as sensory data and images), following the first applications based on large language models (LLMs).

Cybersecurity technology providers can exploit generative cybersecurity AI to improve existing workflows, be a proxy of existing analytics, and generate security configuration or realistic attack data. Soon, applications will include autonomous agents, which can work using high-level guidance without a need for frequent prompting.

Business Impact

Existing vendors and new startups will add generative cybersecurity AI, expanding or replacing features. They will start implementing it with resource-intensive tasks, such as incident response, exposure or risk management, or code analysis.

Organizations will benefit from generative cybersecurity AI as it can improve efficiency and shorten response times to cybersecurity risks and threats. The pace of adoption will vary across industries and geographies due to security and privacy concerns.

Drivers

- ChatGPT is one of the most hyped and fastest-adopted AI technologies ever. It relies on generative AI foundation models, which are largely trained on massive internet datasets.

- Security operations center (SOC) teams cannot keep up with the deluge of security alerts they must constantly review, and are missing key threat indicators in the data.

- Risk analysts need to speed up risk assessments, and be more agile and adaptable through increased automation and prepopulation of risk data in context.

- Organizations continue to experience skill shortages and look for opportunities to automate resource-intensive cybersecurity tasks. Use cases for the application of generative AI include: synthesizing and analyzing threat intelligence; generating remediation suggestions for application security, cloud misconfigurations and configuration changes to adjust to threats; generating scripts and codes generation; implementing secure code agents; identifying and graphing key security events in logging systems; conducting risk and compliance identification and analysis; automating the first steps in incident response; tuning of security configuration adjustment; creating general best practice guidance.

- Generative cybersecurity AI augments existing continuous threat exposure management (CTEM) programs by better aggregating, analyzing and prioritizing inputs. It also generates realistic scenarios for validation.

- Generative AI offerings include the ability to fine-tune models, develop applications using prompt engineering and integrate with prepackaged tools and plugins through APIs. These possibilities open up a path for providers to add generative cybersecurity AI.

- Microsoft has already demonstrated a preview version of its security co-pilot feature, which is expected to drive competitors to embed similar approaches.

- Security program performance solutions and activities can solve their increasing demand for business alignment. Further, they can perform scenario planning for budget (re)allocation, and efficiency and effectiveness indicators and corrections.

Obstacles

- The cybersecurity industry is already plagued with false positives. Early examples of “hallucinations” and inaccurate responses will cause organizations to be cautious about adoption or limit the scope of their usage.

- Best practices and tooling to implement responsible AI, privacy, trust, security and safety for generative AI applications do not fully exist yet.
- Privacy and intellectual property concerns could prevent sharing and usage of business- and threat-related data, reducing the accuracy of generative cybersecurity AI outputs.
- As generative AI is still emerging, establishing the trust required for its wider adoption will take time. This is especially true for the skill augmentation use cases, as you would need the skills you are supposed to augment, in order to ensure the recommendations are good.
- Uncertainty on laws and regulations related to generative AI may slow down adoption in some industries, for example regulated industries in EU countries subject to GDPR compliance.

User Recommendations

- Pick initial use cases carefully. First implementations might have a higher error rate than more mature techniques already in place.
- Monitor the addition of generative AI features from your existing providers and beware of “generative AI washing.” Don’t pay a premium before obtaining measurable results.
- Choose fine-tuned models that align with the relevant security use case or fine-tune in-house models from base models offered by the providers.
- Refrain from sharing sensitive and confidential data with hosted models until verifiable privacy assurances are provided by the host.
- Apply AI security frameworks, such as AI TRiSM. Work with your legal team on data privacy and copyright issues.
- Implement a documented approval workflow for allowing new generative cybersecurity AI experiments.
- Make it mandatory from a policy standpoint that any content (that is, configuration or code) generated by an AI is fully documented, peer-reviewed by humans and tested before it is implemented. If not possible, consider any AI-generated content as “Draft Only” when used for critical use cases.

Gartner Recommended Reading

4 Ways Generative AI Will Impact CISOs and Their Teams

Innovation Insight for Generative AI

Market Guide for AI Trust, Risk and Security Management

Connected Governance

Analysis By: Saul Judah, Malcolm Murray, Andrew White

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Connected governance is a framework for establishing a virtual governance layer across organizations and business functions, or legal entities, in multiple geographies to achieve cross-enterprise business outcomes. By connecting existing governance bodies within and across enterprises, its component-based approach enables complex business challenges to be addressed without adding further layers of bureaucracy.

Why This Is Important

Governance bodies for enterprise functions such as HR, risk, and data and analytics are typically adequate for addressing their individual domain areas. However, cross-enterprise and interenterprise governance challenges are increasingly difficult to overcome. Rather than creating yet another permanent governance body, connected governance leverages existing governance bodies through a virtual framework, providing strategic oversight and accountability management across them with minimum additional overhead.

Business Impact

Senior business executives and board members spanning multiple organizations, legal entities and geographies will find value in exploring connected governance to address cross-enterprise strategic issues and opportunities. Organizations anticipating mergers and acquisitions (M&As) will find value in connected governance, enabling both value and risk management to be addressed earlier and allowing experimentation with governance bodies prior to their formal adoption.

Drivers

- The fast pace of deglobalization and digitalization is putting pressure on senior leaders across multiple business functions to respond to business and regulatory demands at greater effectiveness and speed than they are able to with their existing capabilities. Existing governance bodies are designed to address their functional areas, but understanding accountability and decision rights across these proves very difficult. This is especially relevant when some of the functional areas exist in different legal entities and different countries, and the same business asset is subject to potentially conflicting governance policies.

- A key driver for adoption of connected governance stems from the limitations of existing approaches. Traditional approaches to cross-enterprise governance challenges have been to establish another layer of governance, which adds a greater overhead cost, creates another layer of bureaucracy and is often inflexible. Furthermore, some strategic challenges (such as M&A and business model changes) require a one-off response for governance, and creation of additional governance layers in these circumstances is an excessive drain on executives' time without accrued benefit. Consequently, adoption of connected governance becomes an attractive option.

Obstacles

- Connected governance leverages existing governance bodies, but some of these bodies may operate poorly. As a result, the value that connected governance offers may be depleted in organizations that are not already mature in their governance.

- Siloed governance efforts might reinforce those silos and prevent the benefits of connected governance without disruptive organizational change. Either way, inertia and local success of siloed governance will slow down the adoption of connected governance.

- Once the board of directors or executive committee has approved the cross-governance initiative, an executive leader is expected to shape the cross-governance response. However, this needs support and facilitation from a strategic governance office, which requires skills that are currently in short supply.

User Recommendations

- Evaluate whether connected governance would benefit your organization. If you operate in a complex environment, across multiple legal entities and geographies, there may be challenges that are difficult to address now. In such situations, put on the agenda of your executive committee meeting to initiate a cost-benefit assessment and report its findings. If this does not apply at your organization, connected governance may not be for you.

- Connected governance needs the support of strategic, cross-enterprise governance. Analyze whether this needs a dedicated governance office or if operating as a virtual governance office will be sufficient. If your strategic challenge is a one-off situation, or if you are trialing this as a new initiative, a virtual office may be sufficient for now. However, large enterprises in diverse, complex ecosystems and expecting to address many strategic scenarios may necessitate a dedicated strategic governance office to support connected governance.

Gartner Recommended Reading

Connected Governance Orchestrates Complex Cross-Enterprise Decisions

Connected Governance Drives Adoption of Data and Analytics Governance Platforms

Quick Answer: What Kind of Governance Does Healthcare Data Interoperability Need?

Choose the Optimal Corporate Structure to Cope With Geopolitical Risks

Trends 2023: Rise and Risks From EU, U.S., China and Other Sovereign Data Strategies and Policies

CPS Risk Management

Analysis By: Katell Thielemann

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Cyber-physical systems (CPS) risk management ensures that the unique security and safety risks of CPS are effectively managed. As they connect the cyber and physical worlds, CPS greatly enlarge the threat landscape and consequences for organizations, whether they come into existence out of information technology/operational technology (IT/OT) connectivity, Internet of Things (IoT), industrial IoT, or smart “X” programs. As a result, they require special focus when it comes to risk management.

Why This Is Important

Deployed in critical infrastructure, smart grids, smart buildings or autonomous vehicles, CPS are also core to manufacturing, OT, IoT and industrial IoT technologies. They represent the confluence of physical and digital systems to connect people, data and processes, but also blur the lines between cyber and physical risks. Unfortunately, “first to market” has historically taken precedence over “security by design,” as CPS are full of vulnerabilities and attackers are increasingly targeting it.

Business Impact

Unlike enterprise IT systems that mainly transact data, CPS connect both the cyber and physical worlds, and are usually deployed in operational or mission-critical environments. This means that CPS risk management efforts need to focus on human safety and operational resilience, above and beyond traditional information risk management efforts. This is because an incident could impact both the real world and an organization’s bottom line or mission.

Drivers

- CPS are transforming every industry, whether by orchestrating data flows between previously disconnected systems, automating processes, shortening production cycle times, improving product and service quality, or promoting real-time information gathering and processing.
- Because CPS connect both cyber and physical worlds, risk management is particularly critical in production- and mission-critical industries. As the risk lens expands to the physical plane, beyond cybersecurity, concerns over physical perimeter breaches, jamming, hacking, spoofing, tampering, command intrusion or malware implanted in physical assets, must be addressed.
- The last few years have seen a marked increase in attacks moving from enterprise IT systems, impact operations, and production environments in manufacturing and critical infrastructure organizations. Because these areas are where value is usually created, CPS will continue to be targeted.
- The last few years have also seen a marked increase in vulnerabilities being disclosed in CPS components, such as real-time operating systems (RTOS). As more security researchers focus on CPS, more vulnerabilities will be disclosed, which will provide more attack vectors.
- This increase in the attack surface has driven an increase in regulations, directives, frameworks and standards.
- The consequences of a successful attack on CPS can go way beyond cybersecurity-centric data loss to include operational shutdowns, environmental impacts, damage and destruction of property and equipment, or even health and personal safety risks.
- A growing list of vendors are coming to market with CPS cyber risk quantification platforms.
- The use of simpler platforms like Raspberry Pi in CPS has lowered the barrier for attackers compared to proprietary platforms in traditional OT.

Obstacles

- Many CPS are still not designed and deployed with strong security in mind.

- Legacy systems often reach end of support with no way to update them.

- CPS are routinely deployed by business units without consultation with IT or security teams.

- Security disciplines (e.g., cybersecurity, supply chain security) are usually functionally siloed, whereas effective CPS risk management mandates their convergence around an asset-centric view of security (as opposed to traditional network-centric OT security focusing on segmentation and firewalls).

- Most organizations still focus mainly on IT-security-centric risk management.

- There is a shortage of skills for risk assessments and mitigation efforts in operations or mission-critical environments.

- Purchasing decision makers may not be aware of cyber-physical risks or may prioritize cost and speed over risk, especially when physical risks seem theoretical.

- Vendors who provide comprehensive CPS security posture risk scoring of critical assets are still emerging.

User Recommendations

- Use asset discovery platforms to discover all connected assets in the organization's environment, whether born out of IT/OT convergence or new IoT, IIoT or smart "X" programs. Prioritize those with risk quantification features.

- Define the risk profiles for these systems and update risk registries accordingly, prioritizing CPS assets deemed to be of high value.

- Identify specific CPS security controls already in place, and determine what gaps need to be prioritized based on potential impact.

- Collaborate with cross-functional peers to help develop a vision, strategy and training for the organization's CPS risk management program.

Sample Vendors

Cytellix; DeNexus; OTORIO; Radiflow; SecurityGate.io

Gartner Recommended Reading

3 Initial Steps to Address Unsecure Cyber-Physical Systems

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

CPS Security Governance — Best Practices From the Front Lines

Innovation Insight for Cyber-Physical Systems Protection Platforms

FinDRA

Analysis By: Brian Lowans

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A financial data risk assessment (FinDRA) prioritizes financial investment decisions in data security and privacy. The aim of a FinDRA assessment is to mitigate business risks to a level that is acceptable to balance business outcomes. FinDRA achieves this prioritization by analyzing the financial impacts of business risks identified through data security governance (DSG) and data security and privacy risk assessments.

Why This Is Important

FinDRA enables organizations to translate the language of data security and privacy risks into the language of business risks and business outcomes.

Business Impact

FinDRA creates the basis for establishing a budget for investment in data security, by focusing on how data security and privacy risks affect business outcomes in financial terms.

Drivers

- Organizations are exploiting a variety of data and analytics assets, leading to prolific growth of data and business risks. However, they rarely analyze the financial impacts of data security or privacy risks that can result from investment decisions.
- FinDRA is creating an opportunity to understand how financial impacts may emerge from the opportunity costs, waste and risks associated with each dataset.
- Organizations need the ability to assess how data security and privacy risks associated with security incidents can create financial impacts to a business. Examples of data security and privacy risks associated with security incidents include data breaches, privacy enforcement, noncompliance and even accidental processing. This assessment capability requires a process to translate the issues of data risks into the language of business and financial impacts.

Obstacles

- Most organizations continue to separate the decision processes and responsibilities for data monetization investments from the investment decisions associated with data security and privacy.
- Security perspectives are normally not included in business decisions to create, collect, use or share data. Therefore, they do not have the opportunity to translate the impacts of disparate security and privacy risks into business outcomes.
- Business leaders do not understand the language of data security and privacy risks and will frequently prioritize business access to data over data-security-led controls.

User Recommendations

- Establish a DSG framework to identify all essential datasets and associated data owners, and identify and prioritize the mitigation of business risks through a set of data security policies.
- Conduct a data risk assessment (DRA) to identify how data security or privacy technologies apply security controls to each dataset. Use the DRA to analyze gaps and inconsistencies in data security policy implementation, and to gauge policy effectiveness when mitigating business risks.
- Work with business and financial leaders to evaluate how the business risks for each dataset affect business outcomes that may be measured in financial terms. Examples of these metrics can be revenue, ROI and opportunity cost.
- Use FinDRA to establish business support and to identify which business risks should be prioritized for data security investment.
- Use FinDRA to help reprioritize the data security budget as the risk assessments and IT architecture evolve.

Gartner Recommended Reading

Use the Data Security Governance Framework to Balance Business Needs and Risks

4 Critical Steps to Accelerate the Adoption of Data Security Governance

A Data Risk Assessment Is the Foundation of Data Security Governance

Develop a Financial Risk Assessment for Data Using Infonomics

Select the Best Approach for Capturing and Communicating the Value of Cybersecurity

CAASM

Analysis By: John Watts, Mitchell Schneider, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cyber asset attack surface management (CAASM) is focused on enabling security teams to overcome asset visibility and exposure challenges. It enables organizations to see all assets (internal and external), primarily through API integrations with existing tools, query consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues.

Why This Is Important

CAASM aggregates asset visibility from other products that collect a subset of assets, such as endpoints, servers and devices. By consolidating internal and external cyberassets, users can query to find coverage gaps and misconfigurations for security tools such as vulnerability assessment and endpoint detection and response (EDR) tools. CAASM provides mostly passive data collection via API integrations, replacing time-consuming manual processes to collect and reconcile asset information.

Business Impact

CAASM enables security teams to improve basic security hygiene by finding security controls gaps, security posture, and asset exposures across all digital assets. Organizations that deploy CAASM reduce dependencies on homegrown systems and manual collection processes, and remediate gaps either manually or via automated workflows. Organizations visualize security tool coverage, support attack surface management (ASM) processes, and correct systems of record that may have stale or missing data.

Drivers

- Full visibility into any asset owned by the organization collected through existing tools to improve the understanding of an organization’s potential attack surface and existing security control gaps.

- Quicker audit compliance reporting through more accurate, current, and comprehensive asset and security control reports.

- Consolidation of existing products that collect asset and exposure information into a single normalized view, to reduce operational overhead of manual processes and dependencies on homegrown applications.

- Access to consolidated asset views for multiple individuals and teams across an organization and integrations with other systems of record for current state visibility.

- Lower resistance to data collection from, and better security visibility into, “shadow IT” organizations, installed third-party systems and line-of-business applications over which the IT department lacks governance and control. Security teams need visibility in these places, whereas the IT department may not.

- Help IT teams improve the accuracy of their existing CMDB through periodic updates of assets and attributes missed by CMDB reconciliation processes.

Obstacles

- Resistance to “yet another” tool — there are increasing overlaps with CAASM vendors and adjacent tools that provide some asset inventory and reporting.

- Not all vendors have capabilities to identify and integrate with every required system for visibility and vulnerability information.

- Vendor response actions to prioritized issues may be limited to opening tickets or invoking a script.

- Products licensed per asset consumed become cost-prohibitive for very large organizations.

- The scalability of a single instance may be limited for extremely large environments, in terms of both data collection and usability.

- Tools that can be integrated with a CAASM product either do not exist (due, for example, to the lack of an API) or may be prevented from integrating by the teams that own them.

- Reconciliation processes that conflict with source systems may not be resolved easily within CAASM vendor tooling.

User Recommendations

- Take advantage of proof-of-concept opportunities, and free versions of products and subscriptions, in order to “try before you buy,” as CAASM products are nondisruptive and easy to deploy.
- Given the immaturity of the market, sign no more than a one year contract.
- Favor vendors that can combine inside-out and outside-in asset visibility capabilities or partner with EASM providers.
- Favor vendors that understand all asset types beyond traditional asset categories such as granular software assets, users, and IoT/OT systems to extend to more use cases.
- Inventory all available APIs that can be integrated with the CAASM product you are considering, and ensure you have read-only or low-privilege user accounts available to integrate.
- Ask your incumbent security vendors if they have a roadmap to provide CAASM functionality in future.

Sample Vendors

Armis; Axonius; Brinqa; Encore; JupiterOne; Noetic Cyber; Northstar.io; Ordr; Panaseer; Sevco Security

Gartner Recommended Reading

Innovation Insight for Attack Surface Management

Implement a Continuous Threat Exposure Management (CTEM) Program

Competitive Landscape: External Attack Surface Management

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

At the Peak

Cyber-Physical Systems

Analysis By: Katell Thielemann

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Cyber-physical systems (CPS) are engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). They control production and mission-critical assets, and underpin all critical infrastructure-related industries.

Why This Is Important

Whether deployed in smart grids, smart buildings or autonomous vehicles, CPS are core to manufacturing, industrial control systems (ICS)/supervisory control and data acquisition (SCADA), operational technology (OT), Internet of Things (IoT), and industrial IoT deployments. They represent the confluence of physical and digital systems to connect people, products, data and processes. Deployments can use sensors, robotics, cloud services, analytics, machine learning and high-speed networks, to orchestrate data and physical processes in real time.

Business Impact

CPS orchestrate data flows and physical processes between previously disconnected systems, automate unstructured processes, shorten cycle times, and improve product and service quality. In industrial environments, CPS replace stand-alone production process control and automation, materials handling systems, and transactional workflow systems to process real-time information. They improve productivity, reduce costs, and enable value creation for all asset-intensive industries.

Drivers

- Customer or citizen demand for faster, cheaper, better and more products/services.
- New digital business models.
- Productivity and maintenance improvements.

- Labor cost reduction made possible by automation provided by robotic CPS.
- CPS-enabled operational excellence and enhanced operational data gathering.
- Improved situational awareness in operations or mission-critical environments.
- The need to keep up with the competitive landscape by automating as many processes as possible.

Obstacles

- Concerns over physical perimeter breaches, jamming, hacking, spoofing, tampering, or command intrusion must be addressed above and beyond cybersecurity considerations.
- Deployment-related obstacles include scale (potentially billions of devices are in scope), complex architectural requirements and design approaches from many disciplines involved, sense and control loops that must be designed to evolve with business needs, the need for significant computational resources, and a variety of sensory input/output devices.
- Many organizations increasingly have a mix of legacy and new systems with proprietary protocols, which creates interoperability challenges. While end users have been seeking better interoperability, common standards are still under development in many industries.
- Many devices lack storage and compute power to facilitate security mechanisms.
- Because CPS are usually highly automated, new skills are needed for operations, security and maintenance.

User Recommendations

- Determine the business value of CPS deployment by weighing benefits against cost, complexity and security.
- Promote the use of standards and interoperability recommendations to manage complexity, enable scalability and extensibility, and ensure focus on security and safety imperatives.
- Make sure that any deployment is negotiated with CPS OEMs to ensure upgrades can be easily incorporated. Emerging technologies, such as cloud computing and 5G, will greatly impact these systems.

Sample Vendors

Honeywell International; Johnson Controls; Medtronic; Siemens; Yokogawa

Gartner Recommended Reading

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

CPS Security Governance — Best Practices From the Front Lines

Innovation Insight for Cyber-Physical Systems Protection Platforms

Dynamic Risk Governance

Analysis By: Malcolm Murray

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Dynamic risk governance (DRG) is a new approach to risk governance, which is the critical task of defining the roles and responsibilities for risk management. As opposed to traditional risk governance models, such as the three lines of defense (3LOD), DRG makes risk management more tightly connected to strategy and more meaningful for the business. By customizing risk governance appropriately to each risk, organizations can better manage risks and lower their cost of assurance.

Why This Is Important

The world in which organizations are operating is getting more complex and uncertain, making strategic risk management more important than ever. However, it is also more difficult than ever. Risks are more interconnected and volatile, and can no longer be managed through antiquated risk governance frameworks. DRG offers an approach to rethink the organization's risk management, and manage risk as a strategic asset and liability.

Business Impact

DRG is quantitatively proven to lead to better risk management than traditional risk governance, such as 3LOD. It benefits risk and assurance functions (such as information security and compliance) by improving their collaboration, and benefits the business by reducing the "assurance fatigue" it often experiences from disconnected assurance efforts. DRG makes it easier for the organization to make risk aligned with strategy by applying risk appetite and tolerance to risk governance decisions.

Drivers

- While the risk landscape has evolved dramatically in the last few years, risk governance models have not. While risks have become dynamic and digital, risk management remains too inflexible and uniform. This makes DRG necessary to make risk management more meaningful for the business.
- As organizations have become more complex, risks have become more interconnected. Today's top organizational risks, such as supply chain, cybersecurity and third-party risk, all cut across large parts of the organization.
- The increased digitalization of organizations has led to the creation of new, fully digital risks such as ransomware, as well as an increase in the speed and volatility of other risks such as third-party risks. Risks now change in their nature more often and quickly.
- The rapid adoption of generative AI looks likely to lead to rapid changes in organizations, thereby adding increased uncertainty to many of the key risks in an organization. This includes cybersecurity risk, fraud risk and competitor risk.

Obstacles

- The lack of shared technology platforms and tools, where risk information and analytics are shared between all relevant functions, is an obstacle to DRG implementation. These platforms, such as GRC (governance, risk and compliance) and IRM (integrated risk management) systems are evolving, but there is still a lack of adoption and full implementation.

- A lack of maturity in terms of the collaboration between risk and assurance functions also obstructs the adoption of DRG. Due to organizational history, artificial lines of separation and regulatory pressure, the level of alignment of assurance efforts is still limited and has remained static over the last few years. Adopting DRG aids collaboration, but a higher initial level of risk management agility in the collaboration between functions would be helpful.

User Recommendations

- Apply differing levels of risk governance intensity to different risks, depending on the organization's strategic needs and tolerance for the specific risk.

- Assign accountable parties for risk management activities, based on their actual suitability for the task and not their theoretical function in the organization (e.g., first-, second- or third-line). Use risk-responsible, accountable, consulted and informed (RACI) charts to map this, in order to limit risk management activities to only the essential ones.

- Put digital risk management considerations first when designing and refining risk governance models to streamline risk governance with automation, and more centralized and coordinated data analytics usage.

- Make the board and senior management more involved in risk discussions by framing risk governance discussions around risk tolerance and risk appetite.

Gartner Recommended Reading

The "Risk Balance Sheet" — What It Is and Why You Need One

Use Dynamic Risk Governance to Align Risk Management to Strategy

Dynamic Risk Governance Is the New Risk Mandate

Ignition Guide to Piloting Dynamic Risk Governance

Continuous Compliance Automation

Analysis By: Daniel Betts, Hassan Ennaciri

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Continuous compliance automation (CCA) integrates compliance and security policy enforcement into DevOps delivery pipelines. CCA codifies and continuously applies compliance policies and controls, while monitoring, reporting on correcting and protecting against vulnerabilities resulting from coding defects and misconfiguration. It reduces the number of manual execution steps involved in adhering to regulatory requirements, enhancing consistency, traceability and auditability.

Why This Is Important

Increased focus on security and compliance improvements drives enterprise investments in compliance automation used to secure code and infrastructure. Traditional compliance practices are incompatible with continuous software delivery processes — leading to slower delivery and unexpected, expensive remediation work. CCA improves release velocity and reliability while simplifying compliance enforcement and reporting via policy-driven, automated controls.

Business Impact

Organizations' evolving DevOps/DevSecOps practices can minimize risks and penalties by embedding automated compliance and reporting into their delivery pipelines. CCA enables organizations to integrate compliance into all phases of the delivery pipeline and consistently enforces compliance policies without sacrificing operational agility. CCA tools can offer benchmarks, assessments and self-service reporting to enable efficiencies in compliance auditing.

Drivers

- As organizations face an increasing number of regulatory obligations and more stringent enforcement, automating compliance will become even more valuable to I&O leaders as they strive to maximize flow.
- Additional compliance requirements continue to be added and require support with limited delay.
- Compliance activities are increasingly executed through automated testing, which delivers increased efficiency for developers and reduces the risk of compliance audit failures.
- As cloud-native application architectures and development models become more pervasive, integrating compliance into the toolchain will become more feasible and common.
- Compliance reporting, benchmarking and assessments are often manual and slow.

Obstacles

- No vendor provides capabilities across all elements of the delivery value stream. DevOps teams must integrate multiple tools into their value streams to provide compliance coverage across development and delivery activities.
- Failure to engage with compliance and security subject matter experts (SMEs) early in the development life cycle can lead to problems.
- A lack of rule set understanding and consistent implementation can be an impediment to CCA. Failure to consistently involve organizational compliance teams in implementation leads to a failure in delivering maximum value.
- Poorly implemented CCA presents a business risk. If it is assumed that by implementing CCA, delivered software becomes compliant without additional effort, organizations will face increased risk of compliance failure.

User Recommendations

- Adhere to compliance, governance and security requirements while creating a leaner operating environment.
- Implement a shift-left approach to ensure compliance controls are understood and applied earlier in the development process. Implement automated compliance checks at every phase of the pipeline, demonstrating a "shift secure" approach.
- Invest in tools that enable CCA at scale and can provide a continuous approach to prevent, detect and correct audit failures, and remove manual reporting activities.
- Select tools that can integrate into DevOps delivery platforms to enable security and compliance checking.
- Enforce security and compliance across all domains, including databases, application code, infrastructure and open-source software. No single vendor tool covers all these domains, so DevOps teams must use multiple tools and integrate across all phases of the delivery pipeline.
- Enable efficient compliance policy checking through compliance automation tools to measure benchmarks, perform assessments and report on compliance policy controls.

Sample Vendors

Anitian; Contrast Security; JFrog; Mend.io; Rapid7; Redgate; RegScale; Snyk; Sonatype; Styra

Gartner Recommended Reading

Market Guide for Continuous Compliance Automation Tools in DevOps

3 Essential Steps to Enable Security in DevOps

How to Build and Evolve Your DevOps Toolchains

Market Guide for Value Stream Delivery Platforms

Cyber-Risk Quantification

Analysis By: Sema Yuce, Michael Kranawetter, Christine Lee, Pedro Pablo Perea de Duenas

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Cyber-risk quantification (CRQ) is a method of expressing risk exposure from interconnected digital environments to an organization in business-relevant terms. Such exposure can be expressed in currency, market share, customer/beneficiary engagement, and disruption to products or services over a chosen period. Defensible exposure value ranges are determined using a combination of business logic, mathematical models, loss event history and current risk assessment.

Why This Is Important

Security and risk management (SRM) leaders struggle to match business expectations with subjective expertise and are increasingly being asked to express cyber risks in monetary terms to enable comparisons with risks across the enterprise (e.g., operational, financial, and health or safety risks). They are also tasked with helping enterprise decision makers manage trade-offs between multiple risks (e.g., cyber, operational, health, safety) and business opportunities.

Business Impact

Cyber-risk quantification is used to enable data-driven decision making and improve communication of cyber risk and mitigation options to business unit (BU) leaders, senior executives and the board. It can:

- Justify investments between competing security priorities
- Optimize spend on modernizing infrastructure and legacy applications
- Aid tactical decision making (e.g., prioritize cybersecurity controls, optimize insurance premiums, add risk transfer options, evaluate risk impact)
- Inform valuation of M&As and divestitures

Drivers

- SRM leaders want their security investment decisions to be objective, data-driven and defensible. Faced with a growing list of priorities, many consider risk quantification a more reliable and rigorous alternative to qualitative assessments for ranking strategic initiatives.

- Increasingly, enterprise leaders also want risk exposure to be expressed in business terms — especially currency value — to enable direct comparisons between cyber and other risks, e.g., financial, health and safety.

- SRM leaders often note that monetary expressions of loss exposure motivate business and IT leaders to remediate risks that they might not otherwise prioritize.

- Although CRQ has less historical data points to draw upon than the domain of finance or insurance, CRQ capabilities can permit near real time analysis of risk exposure — e.g., to ransomware or increasing technical debt — in ways that facilitate operational and tactical decision making, e.g., which systems to upgrade, which penetration test results to remediate first.

- While CRQ remains a work in progress, adopters report executive management's increased confidence in security programs insofar as CRQ facilitates cyber risk discussions in terms other leaders understand and helps connect security investments to business outcomes/questions/decisions. When properly tuned, CRQ also enables the setup of capabilities for continuous risk assessment, facilitating automated input from financial systems and business applications, and overlaying IT and security operational risk data.

Obstacles

- Defensibility and scale are primary obstacles to the adoption of cyber-risk quantification. Quantification approaches suit use cases in the finance, utilities, technology, telecom, manufacturing and healthcare sectors, although these remain in early-to-mid stages.

- Among adopters, there is mixed feedback on whether cyber-risk quantification services and solutions offer useful results for business decision making. According to the 2021 Gartner Cyber Risk Quantification Survey, only 36% of respondents said that they have seen action-based results, e.g., convincing risk owners to remediate risks. Primary reasons include a lack of data, especially around probability; CRQ efforts unconnected to a specific business question; and unnecessarily heavy analyses that miss the window on just-in-time communication.

User Recommendations

- Demonstrate the value of CRQ by focusing on the most common, best-value use cases — like security investment prioritization and procuring or renewing cyber insurance. In particular, CRQ provides defensible input into the security investment strategy.
- When discussing CRQ with BU leaders/executives, always link identified risk to business outcomes and outline impact to organizational operations.
- Initiate CRQ via analysis of business assets using objective data from existing business impact analysis (BIA) and monitoring capabilities rather than scenario approaches based on subjective estimates of probability based on historical incidents or rare events.
- Establish a triage process based on clear criteria for when to perform a quantitative assessment.
- Invest in proofs of concept (POCs) to confirm whether CRQ solutions will receive sufficient buy-in. Consider such vendors' AI-based suggestions for best practices to improve your approach, and check for such capabilities before making an investment.

Sample Vendors

Axio; Citalid; C-Risk; CYE; DeNexus; Kovrr; RiskLens; RiskQ; Safe Security; ThreatConnect

Gartner Recommended Reading

Drive Business Action With Cyber Risk Quantification

Quick Answer: What Are CISOs Using Cyber-Risk Quantification For?

Infographic: Benchmarking Cyber-Risk Quantification — Models, Use Cases and Outcomes

Case Study: Criteria to Determine When to Perform Cyber-Risk Quantification

Case Study: Verizon's Cyber Risk Quantification Program

Security Service Edge

Analysis By: Charlie Winckless, John Watts

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Security service edge (SSE) secures access to the web, cloud services and private applications. Capabilities include adaptive access control, data security, visibility and control. Further capabilities include an advanced threat defense and acceptable use control enforced by network-based and API-based integrations. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

Why This Is Important

SSE improves organizational flexibility to secure the usage of web and cloud services, and remote work. SSE offerings are the convergence of security functions (at least, secure web gateways [SWGs], cloud access security brokers [CASBs] and zero trust network access [ZTNA]) to reduce complexity and improve user experience. They are delivered from the cloud. When organizations are pursuing a secure access service edge (SASE) architecture, SSE is paired with software-defined WAN (SD-WAN) to simplify networking and security operations.

Business Impact

Hybrid work is continuing to drive the adoption of public cloud services, especially of SaaS applications. Both hybrid work and the adoption of public cloud services remain business enablers for most Gartner clients. SSE allows the organization to support anytime-anywhere workers by using a cloud-centric approach to enforce a security policy when accessing the web, cloud services and private applications. Simultaneously, SSE reduces the administrative complexity of running multiple products.

Drivers

- Organizations need to secure user, application and enterprise data that is distributed, decentralized and requires secure remote access.
- For many enterprises, a significant amount of critical data is now hosted in SaaS. Therefore, there is a need to perform data loss prevention (DLP) on data that is located in, going to, and leaving these SaaS platforms.
- SSE enables flexible and primarily cloud-based security for users and devices without being tied to on-premises network infrastructure and connectivity. The same security outcome is delivered to users regardless of their location or connectivity.
- Administrators can have enhanced visibility on user traffic and a single configuration and monitoring location for this traffic.
- SSE allows organizations to implement a posture based on identity and context at the edge.
- By consolidating vendors, organizations reduce complexity, costs and the number of vendors used to enforce security policy. Using a single SSE platform rather than multiple point offerings, they can both reduce complexity and reduce gaps in security coverage.
- Sensitive data inspection and malware inspection can be done in parallel across all channels of access. SSE allows doing both inspections in parallel, leading to a better performance and more consistent configuration than doing them separately.
- An adaptive access can take into account more input signals and be more consistently enforced, regardless of the application location or type.
- Organizations look for deeper security capabilities when building a SASE architecture compared to vendors that may have a minimal set of security features as part of their SD-WAN offering.
- Tight integrations that exist between discrete SD-WAN and SSE vendors allow interoperability without requiring a single-vendor approach.

Obstacles

- As the market is being formed by the convergence of capabilities, vendors may be strong in certain capabilities and weak in others. Vendors may also lack overall tight integration between SSE capabilities or with SD-WAN vendors.
- Not all vendors provide sufficiently sensitive data identification and protection to manage business risks.
- Some vendors have focused less on SaaS security and integrations. However, businesses increasingly need this visibility and protection.
- Being cloud-centric, SSE typically doesn't address every need supported by on-premises controls such as internal firewalling.
- Organizations are concerned about uptime or availability of services that they depend on for their business. This is compounded by weak SLAs from some vendors.
- Not all vendors provide all features locally in all geographies, resulting in performance or availability issues.
- Switching costs from incumbent vendors or timing of contract expirations prohibit near-term consolidation.
- Migrating from a VPN will increase costs.

User Recommendations

- Exploit the converged market, consolidate vendors, and cut complexity and costs as contracts renew for SWGs, CASBs and VPNs by replacing them with a ZTNA approach.
- Approach SSE consolidation identifying which elements you may already have in place (for example, existing cloud-based CASB or SWG). Develop a shortlist of vendors based on your use cases regarding secure end-user requirements, the cloud services you use, and the data you need to protect.
- Inventory your equipment and contracts to implement a multiyear phaseout of on-premises perimeter and branch security hardware in favor of the cloud-based delivery of SSE.
- Global enterprises should validate that remote offices have acceptable performance and features with selected vendors. Vendor point of presence (POP) locations and service support are key.
- Actively engage with initiatives for branch office transformation, SD-WAN and Multiprotocol Label Switching (MPLS) offload to integrate cloud-based SSE into the scope of project planning.

Sample Vendors

Broadcom; Cisco; Cloudflare; Forcepoint; iboss; Lookout; Netskope; Palo Alto Networks; Skyhigh Security; Zscaler

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products

Continuous Controls Monitoring

Analysis By: Jie Zhang, Pedro Pablo Perea de Duenas

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Continuous controls monitoring (CCM) automates the monitoring of cybersecurity controls' effectiveness and relevant information gathering in near real time.

Why This Is Important

The growing breadth and depth of security and compliance requirements is putting pressure on security and risk management (SRM) leaders and IT operational teams involved in testing and reporting on cybersecurity controls' effectiveness. Increased attack surfaces, due to cloud adoption and new digital business, are making security assurance tasks even more arduous, error-prone and incomplete than before. Many security organizations lack the capabilities to continuously monitor and measure their controls' effectiveness. This lowers the value of those controls.

Business Impact

CCM tools in cybersecurity help security and IT teams to reduce the manual efforts for security control management, partially relieving staff burden and enabling them to focus on higher-value tasks and reducing costs. The tools also provide constant monitoring of security controls, allowing faster detection of potential threats and minimizing breaches and regulatory noncompliance, preventing significant financial and reputational damage. They not only enhance a company's cybersecurity posture but also build a more secure, successful business.

Drivers

- Organizations are facing growing security and compliance requirements that put pressure on security and IT operational teams involved in control effectiveness testing and reporting, so increasing their productivity by testing more controls within a given time frame is valuable.

- As organizations require continuous visibility into the key control activities and regulations, it is important to provide confidence that controls and gaps are being timely identified and actively managed.

- Streamlining control testing and reducing audit management costs because evidence control activities are collected automatically according to the designated standards and policies. This ensures that security and IT operational teams no longer have to scramble to gather evidence and evaluate controls right before an audit.

- CCM helps avoid fines and boosts business reputation in the eyes of regulators, customers and auditors, as the organization has readily available evidence of risk remediations, protection of valuable assets and an ability to meet its compliance obligation.

- Enable the prioritization of risk management communication and decision by providing context and analysis metrics through CCM.

- Improve accuracy by using preconfigured dashboards and reporting to avoid human errors through ad hoc data exports, copy/paste, and hunting files in dispersed locations.

Obstacles

- Availability and customization of CCM connectors affect time and budget when measuring control effectiveness.
- Complexity of CCM technology leads to additional costs for configuration, management and maintenance by trained personnel.
- Technological limitations and manual interactions challenge data integration and limit full automation in CCM.
- Inherent data quality issues in CCM technology require control owners to manage controls effectively and collaborate with security teams.
- Ensuring transparent calculations and proper utilization of CCM output is necessary to avoid misleading statements and achieve a successful investment.

User Recommendations

- Identify security compliance requirements based on frameworks, regulatory and industry standards, and internal policies to determine controls for monitoring.
- Review existing security tools for potential CCM-like functions before evaluating dedicated CCM tools.
- Define and document the scope for CCM tool connection, ensuring agreement on selected systems and applications.
- Determine requirements based on scope, including automation readiness, user roles, cost analysis, IT asset tracking and inventory of security controls.
- Evaluate CCM tools using representative providers against determined requirements and identify crucial data sources for successful deployment.
- Configure the CCM tool and set up alerts, priorities and response processes, and continuously monitor performance to ensure compliance reporting and process integration.

Sample Vendors

ContiNube; CyberSaint; MetricStream; Panaseer; Pathlock; Quod Orbis; RiskOptics; Telos; XM Cyber (Cyber Observer)

Sliding into the Trough

Digital Risk Protection Services

Analysis By: Mitchell Schneider, Jonathan Nunez

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital risk protection services (DRPS) are a set of technology-led services which enable brand protection, third-party risk assessment and discovery of external-facing threats, and provide technical response to identified risks. These solutions provide visibility into the surface web, social media, dark web and deep web sources to identify potential threats to critical assets and provide contextual information on threat actors, their tactics and processes for conducting malicious activities.

Why This Is Important

Modern attacks, from commodity exploits to highly curated and sophisticated fraud schemes, have become increasingly prevalent and effective as threat actor delivery modalities have been commensurately commoditized (clear, deep and dark web). DRPS leverages these modalities to discover and mitigate the risks which may directly impact business operations or reputation. These services typically require specialized skill sets to operate and are most often consumed as an outsourced function.

Business Impact

DRPS proactively identifies external-facing risks from social media-related artifacts, provides dark web findings, and even supports third-party risk initiatives to determine corrective courses of actions, with the purpose of protecting your organization’s brand. Their services aim to associate all malign activity on the public internet related to your organization, enrich those findings with threat context, and perform technical responses to evict certain threats when possible (takedowns).

Drivers

- DRPS has been driven by its ability to support a range of use cases and user roles. Example use cases include digital footprinting (e.g., mapping internal/external assets and identifying shadow IT); brand protection (e.g., impersonations, doxing and misinformation); account takeover (e.g., credential theft, lookalike domains and phishing sites); data leakage detection (e.g., detection of intellectual property, personally identifiable information [PII], credit card data, credentials); and high-value target monitoring (e.g., VIP/executive monitoring).

- Complexities in the management of risks are key reasons why organizations can benefit from DRPS. These complexities include an expanding attack surface, a more hybrid workforce, higher reliance on e-commerce, regulatory compliance, cloud assets, digital business transformation, and the magnitude of information derived from monitored risk and security activities (e.g., preextortion related to ransomware).

- Demand for DRPS is also driven by the accessibility of such an offering for small or midsize businesses (SMBs) that originally couldn't benefit from threat intelligence (TI), due to the lack of specialized skills and resources for security, including the time needed to perform follow-up actions. This is because of the less technical and more accessible nature of the intelligence made available by many DRPS providers, as well as the availability of a managed service type of offering.

Obstacles

- The DRPS market is starting to get crowded with more than 50 vendors, which makes it difficult for vendors to differentiate themselves from one another. Furthermore, the vendor capabilities vary and may be limited in their ability to provide a comprehensive solution. Some vendors have a best-of-breed approach, whereby they focus heavily on single DRPS use cases (e.g., VIP/executive monitoring), whereas many vendors have expanded to support more than one use case, including external attack surface management (EASM) — the latter natively or via acquisition.

- Market consolidation is accelerating and increasingly overlaps with complementary markets, such as TI, managed security service providers (MSSPs)/managed detection and response (MDR) providers, as well as EASM. These markets are experiencing increased competition.

User Recommendations

- Evaluate the capabilities and features of DRPS offerings and match them to the needs of your organization's security programs and business risks. Ask vendors what threats they cover and whether they focus on a specific use case or many (e.g., phishing, dark/deep web monitoring, data leakage and/or social media protection).
- Prioritize best-of-breed solutions to meet specific urgent needs, depending on the urgency and importance of the core use case. One example would be threats arising from consistent look-alike domains and phishing domains requiring takedown services. Assess vendors based on takedown success rates and ability to work with internet service providers (ISPs) and registrars in foreign locations.
- Prioritize solutions that include managed services in their offerings (especially if there are resource constraints), that can predict and prevent issues from occurring in the first place, and have service-level agreements (SLAs) that ensure the fastest remediation time.

Sample Vendors

Allure Security; Bolster Inc.; CloudSEK; CybelAngel; Cyberint; Cybersixgill; GroupSense; ReliaQuest; SOCRadar; ZeroFox

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Tool: Vendor Identification for Security Threat Intelligence Products and Services

Emerging Tech: Adoption Growth Insights in Digital Risk Protection Services

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

Innovation Insight for Attack Surface Management

Threat Modeling Automation

Analysis By: Dale Gardner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Threat modeling automation tools automate the creation of security requirements and threat models. They can integrate with software development life cycle (SDLC) tools to manage requirements and perform validation. Threat modeling automation tools dynamically highlight potential security ramifications of functional requirements and recommend secure coding practices or architectural countermeasures.

Why This Is Important

Threat modeling and security requirements creation are key to efforts to create secure applications. Tools automate and facilitate these processes by shifting security further left, to the very start of the SDLC. Although they do not secure code, they make it easier to create secure code and application architectures. They also help ensure appropriate security requirements, in contrast to broad standards that inadequately secure high-risk apps while overburdening low-risk projects.

Business Impact

Threat modeling automation tools significantly decrease the effort required to create and maintain threat models, security requirements and risk assessments. This ensures security specifications that are specific to individual projects can be defined early, while costs and risks are low, rather than later. This offers significant benefits to multiple groups within an organization, including architects, developers, security teams and even business stakeholders.

Drivers

- Threat modeling is a best practice in application development. Threat modeling automation addresses a challenge that has constrained adoption, the overwhelmingly manual nature of the task. Automation allows threat modeling to proceed at the pace of development, allowing more organizations to adopt the practice.

- The ready availability and increasing sophistication of threat modeling automation tools enable individuals or small groups to carry out threat modeling and requirements generation in a fraction of the time and effort typically required. They can also make the task much more approachable for architectural and development staff who may lack training in application security concepts and requirements.

- Organizations of all kinds continue to struggle to create secure applications. Issues include the creation — and the detection and elimination — of inadvertent vulnerabilities, as well as essential design flaws, all of which leave applications vulnerable to attack. Threat modeling automation tools can help solve these problems. With relatively limited effort — especially compared with manual approaches — these tools can generate relevant security-related requirements aligned with the threat model and attack surface of applications. The data generated in the process can also guide triage and assessment of vulnerabilities discovered, based on their potential impact.

- Automation of threat modeling helps organizations incorporate the process into more rapid development styles, which would otherwise be extremely difficult.

- Threat modeling automation tools make it easier to incorporate specific requirements associated with compliance mandates, helping to ensure those requirements are addressed.

Obstacles

- Capabilities vary. Free and open-source tools enable easy adoption, but fall short when modeling more complex systems. This prompts consideration of commercial tools, though limitations constrain suitability for the most advanced users.
- Most organizations still focus on application security testing in establishing an application security program. These tools are essential, but fail to identify design flaws.
- The ability to accurately represent a rapidly changing application remains a weak spot of threat modeling automation tools. A threat model is only as good as its ability to provide an accurate representation of a system. Most of today's tools require user intervention to update models as applications change, which leads to abandonment. This is improving as vendors begin to link systems directly to cloud platforms or infrastructure as code files, ensuring changes are reflected automatically in the model, which will then automatically produce updated guidance.

User Recommendations

- Treat threat modeling, security requirements generation and enforcement as best practices within a secure SDLC model. Threat modeling automation tools can be used to help automate these tasks, while incorporating content knowledge from the tool vendors on emerging threats and security requirements.
- Take a risk-based approach, which these tools help enable, to align the level of effort involved in threat modeling with the risk posed by an application.
- Use these tools to automate what are otherwise manual or overlooked efforts. This ensures threat modeling and security requirements generation activities are incorporated into the SDLC process and development workflow. Consider integration of test cases to confirm that requirements are met.
- Train development, engineering, operations and architectural staff in the use and value of these tools. Encourage their use early and continuously in the development process and after deployment (to validate application threat protection efforts).

Sample Vendors

IriusRisk; Microsoft; OWASP Foundation; Security Compass; ThreatModeler

Gartner Recommended Reading

5 Frequently Asked Questions About Threat Modeling

12 Things to Get Right for Successful DevSecOps

Use Threat Modeling to Teach Secure Design (ADP)

Environmental, Social and Governance

Analysis By: Malcolm Murray

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Environmental, social and governance (ESG) is the process for setting, managing and reporting strategy and metrics for an organization's environmental and social impacts, governance mechanisms, and related policies. It allows the board and company leadership to synthesize and weigh stakeholder interests to inform corporate strategy, manage a new set of risks, and communicate ambitions and progress to external audiences.

Why This Is Important

ESG finds itself at a crossroads. After many years of being a top priority, the uncertain economic conditions, geopolitical volatility and evolving regulatory requirements are chipping away at the once-impenetrable armor of ESG. ESG is still a must-have for organizations' long-term sustainability; it is requested by customers and employees, and it is required or about to be required by regulators in several large jurisdictions. But the ESG journey has become a more complex one to navigate.

Business Impact

ESG impacts organizational strategy and operations through:

- **Risk-balanced progress:** ESG impacts both the risks (e.g., regulatory, reputational) and the opportunities (e.g., access to capital, customer loyalty).

- **Wide-ranging touchpoints:** ESG now impacts all areas of organizational decision making — suppliers, mergers and acquisitions, etc.
- **Decision timing:** ESG impacts the timing of decisions — too soon may lead to additional costs, while too late may lead to stranded assets or regulatory noncompliance.

Drivers

- **ESG investing:** Investor appetite for ESG assets rose significantly for many years. It took a bit of a breather in 2022, due to geopolitical concerns and changes in how ESG funds were labeled. The year 2023 looks likely to continue the long-term trend, however, as the benefits of ESG investing remain solid.
- **Regulatory disclosures push:** Most of the world's largest economies (the U.S., EU, the U.K., China, India and Japan) now either have in place or are soon to release new guidelines or regulations for ESG disclosures.
- **Customer preferences:** Customers are increasingly concerned about enterprises' environmental and social impact, and are making value-based choices in their purchases of products, choice of employers and votes for officials.
- **Policy:** Enterprises are increasingly impacted by the incentives and disincentives being put in place by policymakers. To hit targets, policymakers are putting in place taxation, bans, penalties and new market mechanisms.
- **Social pressure:** Enterprises increasingly need valid supplier ESG performance and data from deeper in the value chain for Scope 3 greenhouse gas (GHG) emissions. They are focused on responsible sourcing, assessing labor, health safety and environmental risks.
- **ESG strategy:** As the value of having a clear and actionable ESG strategy becomes clear, 94% of public companies now either have or are in the process of setting up an ESG program. Further, boards are increasingly stepping up their oversight of ESG, as they recognize its necessity for long-term resilience.

Obstacles

- **Political backlash in the U.S.:** In the U.S., some states have seen political backlash against ESG and bans on using ESG in investments.
- **Competing demands:** The Russian invasion of Ukraine created geopolitical risk and energy crises that were at cross-purposes to ESG.
- **Macroeconomic environment:** The uncertain macroeconomy has led to a focus on cost, leaving less room for ESG investments.
- **Internal governance:** There is no one place for an ESG program to sit in the organization and there is often duplication of work and unclearly defined responsibilities.
- **Data alignment:** ESG data gathering and comparability remain challenging due to the lack of standardization and the lack of maturity in the vendor space.
- **Quantifying benefits:** Improving ESG performance is often seen as an intangible benefit, where it is difficult to connect to direct financial rewards.
- **Visibility of impact:** The majority of impact is further down in the value chain and organizations struggle to get visibility of supplier performance.

User Recommendations

- **Link ESG objectives to long-term financial stability:** ESG needs to drive a business outcome of long-term sustainability of financial performance.
- **Build capabilities, not program components:** In order to make ESG truly integrated, think ESG building capabilities, not program components.
- **Build in, don’t bolt on ESG capabilities:** Don’t create new processes where not needed; leverage existing capabilities and processes.
- **Create governance:** Create a governance framework that enables the organization to set goals, targets, KPIs and metrics, and monitor and report on them consistently.
- **Include the value chain:** Identify environmental and social impacts, not only under direct control, but also in the value chain. Track supplier performance.
- **Align key performance indicators (KPIs) with compensation:** Build ESG measures into senior leaders KPIs, tying performance to compensation.

Gartner Recommended Reading

Market Guide for ESG Management and Reporting Software

Predicts 2023: Achieving ROI With ESG — Leadership Perspective

Anatomy of an ESG Program

Maverick Research: To Do Good, Stop Following ESG Standards

Prepare for the SEC's New Proposed Climate Disclosure Requirements

IT Vendor Risk Management

Analysis By: Joanne Spencer

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

IT vendor risk management (VRM) is the process of ensuring that the risks associated with vendors and service providers are effectively managed. The discipline of VRM addresses the identification, mitigation and remediation of these risks to avoid business disruption and financial and regulatory impacts. VRM technologies support various activities as part of a broader VRM framework.

Why This Is Important

Organizations rely on an ecosystem of IT vendors to achieve their objectives. However, this dependence exposes them to potential vendor risks, resulting in data breaches or business disruptions, with legal or regulatory fines and reputational impacts. Lack of visibility into third and fourth parties (e.g., subcontractors), along with an increasing reliance on cloud models, makes it very difficult to assess and mitigate IT vendor risks, thus heightening the need for IT VRM solutions.

Business Impact

IT VRM solutions provide a consistent approach to managing vendor risk, while helping organizations comply with changing laws and regulations. Organizations can also track and monitor vendor performance and interactions as IT VRM solutions broaden their capabilities. IT VRM solutions, combined with content, data feeds and risk intelligence, ensure effective management, because everything is stored in one place. AI has reduced processing and response time by importing existing documentation and policies.

Drivers

- Organizations need to manage an ever-increasing number of regulations related to risk, data privacy, cybersecurity, and environmental, social and governance (ESG).

- IT VRM can be a catalyst for improved vendor outcomes, by identifying vendor-related risks early and mitigating them through effective controls and process improvements.

- IT VRM solutions automate part or most of the assessment, analysis and control validation process; provide remediation and mitigation guidance; and facilitate monitoring of risks associated with vendors and other third parties that access, support or control information assets.

- As independent stand-alone solutions arise and ease of implementation improves, we anticipate that the adoption of these solutions will continue to increase.

- Because the world continues to deal with geopolitical unrest and economic uncertainty, organizations will need to proactively manage vendor risks.

Obstacles

- Resource constraints (both personnel and budget) are hindering organizations' ability to provide ongoing monitoring and tracking of vendors.
- A lack of mature VRM programs, expertise and process is leaving organizations open to the impacts of vendor risk. Security breaches and failed vendors are examples of what can happen without an effective VRM program.
- Although they don't have the same capabilities, a couple of options are seen as alternatives to a full IT VRM solution. These include security and risk rating services (BitSight Technologies, Black Kite, RiskRecon, SecurityScorecard, etc.) and vendor risk assessment data in a shared model (CyberGRX, OneTrust, Prevalent, Venminder, etc.).
- A focus on assessing IT vendor risk for the purpose of meeting regulatory requirements can lead to overemphasis on survey-based models, resulting in risk acceptance rather than implementation of effective controls or other mitigation strategies.

User Recommendations

- Align your solution decisions with your IT VRM maturity roadmaps.
- Implement a VRM strategy, a VRM governance program and process, and VRM ownership. Remember that a technology solution is not a substitute for these.
- Ensure that any potential VRM solution supports your existing IT VRM processes and methodologies.
- Use solutions that integrate with risk and security rating services, risk exchanges, and content providers to assist with ongoing vendor risk monitoring.
- Ensure that all relevant stakeholders are using the solution for VRM workflows, including risk management, IT security, procurement, vendor management, legal and business continuity management.
- Ensure that vendors perform their contracted risk obligations, including risk reporting, security incident notification, and business continuity planning and testing.

- Use two factors to prioritize risk weightings: the criticality of the solutions and technology, and the sensitivity of the data or intellectual property (IP) that a vendor may access or control.

Sample Vendors

Aravo; Archer; LogicManager; Metricstream; OneTrust; Prevalent; ProcessUnity; ServiceNow; Venminder

Gartner Recommended Reading

Market Finder: Third-Party Risk Management

Market Guide for IT Vendor Risk Management Solutions

Market Guide for Third-Party Risk Management Solutions

Tool: Vendor Identification for Third-Party Risk Management Solutions

Privacy Impact Assessments

Analysis By: Bart Willemsen

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Privacy impact assessments (PIAs) enable organizations to identify and treat privacy risk. Typically conducted before implementing new processing activities and/or major changes, the PIA starts with a quick scan (looking at the process owner and description, types of data processed for specific purposes, and retention periods per purpose). A full PIA adds legal grounds, potential impact on data subjects, and mitigating measures to ensure a controlled personal data processing environment.

Why This Is Important

An ongoing shift in the regulatory privacy landscape mandates that organizations develop foundational insight into what personal data they process, why and how it is protected. Few organizations have the means to demonstrate insight in and control over personal data across the various repositories and silo types, let alone how they're used or intended to be used. This insight, however, is vital to proportionate and adequate deployment of privacy and security controls.

Business Impact

A PIA improves regulatory compliance, control over personal data throughout the data life cycle, and helps determine access management as well as data end of life following a deliberate intent toward purposefully processing people's data. Assisting in prevention of (internal) data breaches and personal data misuse, it helps security and risk management (SRM) leaders quantify risk to subjects and timely apply suitable mitigating controls. Conducting PIAs frequently and consistently provides a basis for responsible and transparent data management.

Drivers

- PIAs are one of the cornerstones of an effective privacy program. However, many organizations conduct PIAs manually, using spreadsheets and questionnaires. With increasing volumes and the need for repetition of PIAs, a manual approach becomes unmanageable.
- Overstandardization traps the skills needed to conduct PIAs with a few people rather than making them part of an organization's data-handling fabric.
- PIA automation tools allow for (API-driven) triggers to initiate the assessment process, collecting the needed information at every step and tracking it through a predefined workflow all the way until a case is closed or flagged for remediation.
- When done well, the PIA sits at the heart of connecting legal requirements and business process reengineering to practical operationalization in privacy by design and enablement of adequate security control application.
- The results of a PIA will help assess records of processing activities (RoPAs), and through intelligence of data fabric from data and analytics leaders, SRM leaders can further automate the intended personal data life cycle in terms of where it should and should not be available. In other words, the PIA outcome with purpose-based processing activities determines purpose-based access controls (PBAC). In addition, it facilitates automation of the determined data end-of-life moments.
- The entire PIA process eases data governance initiatives to a more controlled state, yet the current main drivers still primarily come from regulatory requirements. Additional frameworks do help, like the 2023 revamped ISO 29134.

Obstacles

- Often considered a tedious task because of poorly conceived manual workflows and a one-size-fits-all mentality, there is a certain PIA fatigue in organizations where this activity has been mandatory for a longer period of time.
- Business partners' view of a checkbox mentality does not help the quality of the PIA.
- Others simply underestimate its relevance and position and do not complete accurate PIAs or fail to frequently keep them updated, making the initial attempt an ultimately futile one.
- PIA automation tools are hard to tailor to an organization's needs in the absence of knowledgeable and trained staff. As a result, even an automated approach fails to fulfill the purpose for subsequent automation and alignment of the personal data life cycle governance or management activities that are ideally connected to the PIA.

User Recommendations

- Appoint and mandate business process owners with responsibility over their respective personal data processing activities, and actively involve them in optimizing the process for fluency and detail.
- Require PIAs to be conducted as a mandatory, frequently reiterated activity. Triage the necessity for PIAs in change processes and the introduction of new processing activities.
- Include the PIA's results — especially from large projects — in the corporate risk register for monitoring and follow-up. Depending on scope and focus, it may also help to integrate high-risk PIA activities to overarching business impact assessments.
- Extend the assessment's effectiveness to processing of personal data carried out by service providers by demanding that they complete and periodically revise a full PIA.
- Use a centrally provisioned tool for consistently conducting PIAs (for example, as an internal automated workflow process), or require the PIA to be conducted as a manual exercise when a less-mature procedure suffices.

Sample Vendors

DataGrail; OneTrust; PrivacyPerfect; RESPONSUM; Securiti; Smart Global Governance; TrustArc; WireWheel

Gartner Recommended Reading

Toolkit: Assess Your Personal Data Processing Activities

Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria

Ignition Guide to Implementing a Privacy Impact Assessment Process

Security Rating Services

Analysis By: Christopher Ambrose, Oscar Isaka

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Security rating services (SRSs) for cybersecurity provide continuous, independent scoring for enterprises with a visible presence on the internet. They gather data from public and private sources via nonintrusive means, analyze the data, and rate security using proprietary scoring methodologies. These tools are used for internal security, cyberinsurance underwriting, due diligence in mergers and acquisitions (M&As), and third-party/vendor cybersecurity assessments and monitoring.

Why This Is Important

The focus on cybersecurity threats and privacy regulations is expanding. At the same time, reliance on third parties — especially, but not exclusively, cloud service providers — is increasing. These forces have created a growing need to understand internal and external threats and security postures. The traditional approaches for assessing third-party security controls are stressed and have limitations, especially when hundreds or even thousands of external parties are involved.

Business Impact

With an SRS, security and risk management (SRM) organizations can obtain an objective, relatively low-cost, “outside-in” evaluation that may be useful yet incomplete. SRSs have been used to engage corporate boards and senior leadership in facilitating ongoing security investments. SRS findings can be used to supplement data derived from security assessments and business impact analyses. However, a “rating score” without context provides limited value for business executives and board members.

Drivers

- Third-party security assessments or certifications provide point-in-time snapshots, but are not always available or shared by third parties.
- Vendor-completed security questionnaires are also point-in-time. In addition, they are highly subjective, labor-intensive, and inefficient for infosec departments and the vendors asked to complete them.
- Some enterprises are under increased pressure to provide cybersecurity posture measures to senior management and to their customers, ideally in comparison with peers and competitors.
- Increasingly, enterprises struggle to translate cybersecurity metrics into quantifiable measures of risk.
- Vendors can use SRSs to support sales and marketing by demonstrating that they practice good security.
- An SRS represents an independent source of data to support a number of use cases.
- In addition to the use cases listed above, Gartner expects more use cases to emerge to address the growing demands for measuring and monitoring cybersecurity controls. Moreover, Gartner expects to see more M&As in this market, which continues to expand with limited differentiation among new entrants.

Obstacles

- Although SRSs provide some useful metrics of an entity's cybersecurity posture, these services don't provide a complete assessment of security controls, as their information is primarily publicly sourced (from accessing internet IP addresses, for example).
- In practice, a numeric "security rating" provides less information than most organizations are looking for. However, this gap is encouraging SRS vendors to provide more complex offerings that combine a score with other forms of data and capabilities (i.e., questionnaire libraries, cyber-risk quantification, and policy and control mapping).
- No service or solution has matured to provide consistently time-tested ratings, and some may not have full visibility into cloud environments, especially SaaS.
- Although we see these services as important innovations in improving an enterprise's ability to assess and monitor the potential for cybersecurity vulnerabilities, they are not a replacement for due diligence and assessment of internal or third-party controls.

User Recommendations

SRM organizations can use SRSs to:

- Evaluate the security posture and possible control inadequacies of a third party.
- Monitor and receive alerts on the security status of key vendors and service providers.
- Provide leadership with an independent assessment of their enterprise's own security posture, and compare that to peers or competitors.
- Provide leadership and internal stakeholders with a rudimentary quantification of a vendor's (or another third party's) risk to the enterprise.
- Demonstrate their security posture to prospects and customers by sharing scores.
- Evaluate the enterprise's security posture in support of cyberinsurance underwriting processes.
- Inform M&A decisions.

- Engage third parties in a discussion about their security rating and the adequacy of their controls.

Sample Vendors

BitSight Technologies; Black Kite; BlueVoyant; Panorays; RiskRecon; SecurityScorecard; UpGuard

Gartner Recommended Reading

Market Guide for Third-Party Risk Management Solutions

Tool: Vendor Identification for Third-Party Risk Management Solutions

Supply Chain Risk Management

Analysis By: Heather Wheatley, Christian Titze

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Supply chain risk management (SCRM) provides a consistent framework for organizations to identify and mitigate supply chain risks. A comprehensive end-to-end approach to SCRM focuses on collaboration to develop and deploy a framework and mindset to both shape disruption to design out risk and manage identified risks across diverse ecosystems of partners — digital and physical. It is strengthened by the technology used for risk identification, holistic impact analysis, mitigation and monitoring.

Why This Is Important

Supply and operational disruptions continue to be front and center for organizations. They are increasingly finding that siloed risk frameworks are ineffective at managing response strategies to a variety of risks, with disruptions leading to commercial, financial, regulatory, reputational, environmental and digital impacts. The importance of balancing available risk mitigations with other objectives such as revenue, growth, availability, cost, innovation, sustainability and competitiveness has taken priority.

Business Impact

Organizations are finding that the cost of responding to each risk after it disrupts the supply chain is prohibitively expensive and exceeds their appetite for risk. A holistic framework to proactively tackle end-to-end supply chain risks aligned to organizational strategy is essential to direct risk management. This framework combines operational risk management with strategic risk management at the organizational level.

Drivers

- The volume and diversity of risks potentially impacting the supply chain have increased. Risks can occur in technology, political, economic, social/cultural, trust/ethics, regulatory/legal and environmental areas. A reactive approach to risk management is not enough in a globalized world where risks are harder to predict, increasingly interconnected, and have further-reaching and longer-lasting consequences.
- The majority of supply chains are globally extended and extremely complex, making them a large target for disruption in an environment that is experiencing more risk. Compounding this, the partner ecosystem has expanded significantly, introducing more entry points for risk to disrupt the organization. Visibility within the partner ecosystem remains challenging.
- In a supply constrained market, management of risk in the supply chain is critical to the achievement of organizational objectives including driving top-line growth.

Obstacles

- Identifying and prioritizing interconnected risks is complicated in organizations with evolving strategies while managing global issues in high uncertainty.
- Organizations must dedicate funds and resources for ongoing end-to-end risk governance and risk mitigation. Demonstrating the return on investment for proactive mitigations remains challenging particularly where priorities are unclear.
- Digitalization and the availability of accurate data on the risks associated with ecosystem partners or level of impact from risk events in far-flung regions can be challenging, requiring emerging technologies such as graph technology, AI and advanced analytics to overcome.
- Gaining visibility into the extended operations is a difficult and important task. With global, complex networks where the partner ecosystem might be continuously shifting, identifying vulnerabilities beyond direct partners can be strenuous.

User Recommendations

- Link risk management activities explicitly to organizational and supply chain strategy to focus on the ability to profitably deliver key activities, products and services.
- Establish processes and governance to identify and prioritize risks, risk appetite, response and escalation. Identify and establish measurement criteria such as time to survive, time to recover and value at risk. Define measurable risk appetite and tolerances.
- Design out risk and reduce the rate of disruption within the supply chain by employing a shaping disruption strategy.
- Employ technology to track interdependencies, and organizational and ecosystem partner potential failure points to baseline and continually monitor emerging risks.
- Perform assessment and seek assurance on the effectiveness of proactive and reactive risk mitigations.

Gartner Recommended Reading

Identify and Assess Supply Chain Risks to Improve Your Capabilities to Respond

Creating a Supply Chain Resilience Framework

Shaping Disruption: A New Strategy for Supply Chain Risk Management

Market Guide for Supplier Risk Management Solutions

Respond to Increasing Supply Chain Risks by Strengthening Risk Governance

Climbing the Slope

Data Classification

Analysis By: Ravisha Chugh, Bart Willemsen, Andrew Bales

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Data classification is the process of organizing information assets using an agreed-upon categorization, taxonomy or ontology. The result is typically a large repository of metadata useful for making further decisions. This can include the application of a tag or label to a data object to facilitate its use and governance, either through the application of controls during its life cycle, or the activation of metadata using data fabric.

Why This Is Important

Data classification facilitates effective and efficient prioritization of data within data governance and data security programs concerned with value, access, usage, privacy, storage, ethics, quality and retention. It is vital to security, privacy and data governance programs. Data classification helps organizations distinguish the sensitivity of the data that they process, promotes a risk-based approach and improves the effectiveness of data protection controls.

Business Impact

Data classification supports a wide range of use cases, such as:

- Implementation of data security controls
- Privacy compliance
- Enablement of purpose-based access controls
- Risk mitigation
- Master data and application data management
- Data stewardship

- Content and records management
- Data catalogs for operations and analytics
- Data discovery for analytics and application integration
- Efficiency and optimization of systems, including tools for individual DataOps

Drivers

- Data classification approaches — which include classification by type, owner, regulation, sensitivity and retention requirement — enable organizations to focus their security, privacy and analytics efforts on important datasets.
- When properly designed and executed, data classification serves as one of the foundations supporting ethical and compliant processing of data throughout an organization.
- Data classification is also an essential component of data governance, as by classifying the data, organizations can establish data retention, data access and data protection policies that can help reduce the risk related to data exfiltration.

Obstacles

- Data classification initiatives have often failed because they were dependent on manual efforts by users with insufficient training.
- Data classification adoption is typically a reflection of the security posture of the organization. If the purpose of data classification is not clearly defined for employees using natural language, engagement in the data classification program is minimized.
- Data classification often fails due to poor communication. Program objectives, policies and procedures should be effectively communicated to all necessary stakeholders to avoid resistance to data classification initiatives.
- Although many vendors offer automated data classification tools that can classify more data more accurately while minimizing user effort, they are not 100% accurate — especially if they use machine learning or artificial intelligence algorithms for which models require ongoing training.

User Recommendations

- To identify, tag and store all of their organization's data, security and risk management leaders and chief data officers should collaboratively architect and use classification capabilities.
- Implement data classification with user training as part of a data governance program.
- Use a combination of user-driven and automated data classification for success in a data classification program.
- Determine organizationwide classification use cases and efforts, and, at minimum, keep all stakeholders informed.
- Combine efforts to adhere to privacy regulations with security classification initiatives. Information can be classification-based by nature (i.e., personally identifiable information, protected health information or PCI information), or by type (i.e., contract, health record or invoice. Records should also be classified by risk category, so as to indicate the need for confidentiality, integrity and availability. Additionally, records can be classified to serve specific purposes.

Sample Vendors

BigID; Concentric AI; Congruity360; Microsoft; Netwrix; OneTrust; SecuritiAI; Spirion; Varonis

Gartner Recommended Reading

Building Effective Data Classification and Handling Documents

Improving Unstructured Data Security With Classification

How to Succeed With Data Classification Using Modern Approaches

Video: What Is Data Classification, and Why Do I Need It?

Hazard/Threat Intelligence Services

Analysis By: David Gregory

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Hazard/threat intelligence services evaluate incidents (local to global) that may threaten the health and safety of citizens and workers, damage critical physical and digital technology infrastructure, or disrupt business operations. These services send predictive alerts about the weather, public health, terrorism, civil unrest, earthquakes, cyberattacks and other events in real time — as early warnings and while events are in progress.

Why This Is Important

The COVID-19 pandemic, the permanence of hybrid working, Russia's invasion of Ukraine and supply chain delays are increasing adoption of these services because organizations see their value for use cases such as duty of care, physical security and product manufacturing. Increased adoption will help mature overall crisis/emergency management processes within organizations.

Business Impact

Hazard/threat intelligence services can help mature organizations' crisis/emergency management processes when:

- Operations are in locations subject to heightened threat from environmental, geopolitical, cybersecurity, weather-related or health-related incidents.
- Organizations support hybrid workplaces, in which workers are more dispersed than before.
- Cybersecurity alerts from a cybersecurity team indicate potential for follow-on physical security threats. Sharing such information could help improve organizations' preparedness and reduce business disruption.

Drivers

- Without accurate, timely information, it is difficult to know when an incident will turn into a crisis that requires a directed organizational response. Also, monitoring a multitude of data sources can result in “analysis paralysis” and under- or overreaction. Hazard/threat intelligence services help address these challenges.

- Government and private-enterprise professionals use these services in areas such as corporate security, business continuity management, HR, supply chain management, and data and analytics. They help with risk assessments of operating locations undertaken as part of due diligence in a number of scenarios. Examples include deciding where to relocate personnel and operations, creating situational awareness to gauge a disruption’s impact on operations, complying with traveler and expatriate duty of care needs, and response management for large-scale events.

- These services deliver alerts and reports at a facility, neighborhood, regional, national and international level to clients via email, SMS, phone and print. They use artificial intelligence to draw on thousands of information sources, such as news outlets, social media, government agencies, academic, political and business sources, and technological resources such as applications and devices.

- Situational awareness is greatly improved by the use of, for example, GIS services for a geolocation analysis of people, facilities, suppliers and other resources, as well as layered data visualization for the risks an organization may face. Therefore, more organizations, especially those with a multilocation footprint, are adopting hazard/threat intelligence services that use GIS information. By categorizing the severity of incidents and geocoding their resources/assets, alerts can be prioritized and directed to the right people within the organization in real time for investigation and faster, more coordinated responses.

Obstacles

- The biggest obstacle to using hazard/threat intelligence services is not their technical aspects. It is ensuring that the organization has an internal procedure to receive, process, disseminate and respond to the alerts generated by these services.
- Outputs from hazard/threat intelligence services do not align specifically with any one part of an organization, and alerts may relate to the physical or the digital, as may the impacts. For example, physical operations alerts might be sent to the corporate security department and public health alerts might be sent to HR or facilities management (for occupancy management). Cybersecurity personnel might perceive a heightened threat of physical damage from a cybersecurity alert. Cross-organizational groups that can coordinate responses to such alerts are rare, and internal processes must account for multiple scenarios so that organizations do not overrespond or underrespond to an incident.

User Recommendations

- Create a coordinated internal team so that alerts produce coordinated, business-informed responses across your organization. Include representatives from corporate security, cybersecurity, HR, IT operations and the business continuity management office.
- Evaluate solutions that integrate with an emergency or mass notification service (EMNS) and crisis or emergency management tools to gain strong situational awareness before and during incidents.
- Ensure the chosen solution provides a visual display of organizational facilities, suppliers and other operational assets, and maps these to threats.
- Select a solution that handles sources of alerts for multiple types of crisis, both global and hyperlocal. The incidents that can be managed can range from human-made events as well as natural ones.
- Ensure the solution includes a GIS capability that can be customized to your operational footprint, and a mobile device app for communications and interactive situational-awareness activities.

Sample Vendors

AlertMedia; Crisis24; Dataminr; Everbridge; Factal; International SOS; Kinetic Global; Risk Intelligence; WeatherOptics

Gartner Recommended Reading

Toolkit: Vendor Identification and Selection Guide for Business Continuity Management Software

Risk Management KCIs

Analysis By: Julie Tani

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

The growing interdependencies of risks require greater risk management focus on the state and effectiveness of controls by measuring and designing risk management key control indicators (KCIs). KCIs also enable risk management leaders to monitor the effectiveness of controls and proactively manage them as they provide insight into, and monitoring of, the business's activities and responses to a risk.

Why This Is Important

Leaders must help the business develop risk treatment plans and determine the ability of control investments to manage risk within tolerance. To do so, they must understand control effectiveness. Organizations primarily use key risk indicators (KRIs) to signal increasing risk exposures, but these offer no insight into the state of controls. Using KRIs together with KCIs, which measure a control's outcomes versus its objectives, will provide earlier warning for risk events.

Business Impact

There is a higher need than before to use KCIs because:

- Risks are more interconnected than ever. KCIs offer valuable insight into the potential for control failures that can simultaneously impact a multitude of risks.
- Risks are increasing in speed of impact and complexity. KRIs on their own don't always show control weaknesses and, therefore, cannot fully enable proactive risk reduction. KCIs coupled with KRIs provide earlier warning into increasing residual risk levels.

Drivers

- KCIs can complement, or supplement, point-in-time control assessments as a tool for continuous control monitoring. Risk management practices tend to underutilize KCIs. But guidance and regulation (such as the Basel Committee on Banking Supervision's *Corporate governance principles for banks*) state that a board of directors needs, among other key pieces of information, reports on internal control failures to fulfill its responsibilities.

- Increased regulatory focus on operational resilience requires enhanced monitoring and reporting of risks and controls related to a firm's core business services. This ensures it can resist, absorb, recover and adapt to business disruption and continue delivering its core customer products and services.

Obstacles

- KCIs do not provide insight into control coverage (that is, whether an associated risk is fully addressed by the control across the entire environment). It is especially important to understand the control coverage when comparing a control to related and relevant KRI exposure levels.

- KCIs alone do not indicate the reason a control failed. In some instances, a performance problem in a separate control or process may have led to the control failure. Another example is a change in the covered risk environment beyond the control's designed mitigation range.

- Effectiveness of KCIs depends on the organization's ability to operationalize and apply risk appetite. Since risk appetite outlines the amount of risk a firm is willing to accept in pursuit of its strategic goals, it, therefore, helps define the parameters for control effectiveness. If risk appetite is not well-understood, establishing KCI effectiveness definitions and thresholds may be a challenge.

User Recommendations

- Develop a suite of key controls and their alignment with key risk exposures and associated KRIs.

- Clearly state control objectives and their measurements for all key controls, creating an awareness of the outcomes each control is expected to deliver.

- Institute frequent or continuous monitoring of the KCIs, increasing the ability to catch potential control failures before they happen.

Gartner Recommended Reading

Use KPIs, KRIs and KCIs to Better Understand Financial Services' Risk Profile

Tool: Defining and Mapping KPIs, KRIs and KCIs to Each Other and to Strategic Objectives

Entering the Plateau

ITRM Solutions

Analysis By: Sema Yuce, Michael Kranawetter

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

IT risk management (ITRM) solutions operationalize the risk management life cycle. Their main use cases are IT risk and control assessment; regulatory, industry and policy compliance; U.S. federal assessment and authorization; and cyber-risk management. ITRM solutions have core capabilities ranging from workflow management, risk analysis, reporting and digital asset discovery to data integrations and third-party connectors. ITRM is a capability of governance, risk and compliance (GRC) software.

Why This Is Important

The ITRM market maturity level has reached mainstream with the necessity to manage risk from an integrated perspective. With a clear focus on GRC-related processes and security risk exposures, buyers have maintained interest in ITRM, though attention has started shifting toward emerging, specialized cyber-risk management solutions, Many organizations use ITRM solutions to manage technology risk, typically with a business and enterprise risk context.

Business Impact

ITRM solutions provide cost savings by replacing manual coordination of risk and compliance governance in the digital environment. They track deviations against standards and facilitate monitoring risk indicators. Buyers align data with cyber-risk initiatives or adopt dedicated cyber-risk management solutions. ITRM is integrated as a capability within GRC or enterprise risk management (ERM) solutions, simplifying risk reporting and enhancing decision making for the board and senior management.

Drivers

- Ongoing business transformation initiatives have put the spotlight on IT operational dependencies, alongside wider digitisation initiatives.

- Organizations using ITRM solutions to manage more than IT compliance risk and governance are shifting attention to emerging ones such as cyber-risk management solutions.
- The prioritization of business context aligns with a steadily increasing maturity in the risk management discipline, leading to a strong integration of IT risk into enterprise risk management solutions.

Obstacles

Key obstacles for the adoption of ITRM solutions include:

- Balancing between immediate needs and mid- to long-term requirements as buyer organizations scale.
- A lack of process definition and an updated asset and process inventory.
- Not knowing what is the best value in using automation.
- Risk workflows or technical data consolidation.

User Recommendations

- Ensure your processes have reached a level of sufficient maturity as a buyer before looking to automate them through adoption of technology, as it often causes more confusion and loss of investment.
- Select vendors based on their ability to scale and flex with your risk management journey.
- Include in your prework to deploy ITRM solutions the labor associated with populating asset, process, risk and control repositories. This is significant.
- Generate interest in ITRM/GRC solutions to automate risk-related activities, as they combine vendor risk, corporate compliance, operational risk or audit management solutions with other risk and compliance activities. The main advantage of this is the integration of risk data, workflow and dashboards as well as different risk managers from different parts of the organization.

Business Continuity Management Program Solutions

Analysis By: David Gregory, Ron Blair

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Business continuity management program (BCMP) solutions are the primary tools used to manage BCM programs through all phases of the life cycle, from planning and recovery development to crisis activation and business recovery. BCMP solutions provide capabilities for availability risk assessment, business impact analysis, business process and resource/asset dependency mapping, recovery plan management, exercise and crisis management, and BCM program management metrics and analysis.

Why This Is Important

Executives and regulators are seeking assurance that organizations have best-practice BCM methodologies and frameworks in place in response to events such as persistent ransomware attacks and the Russia-Ukraine war. The sophistication of BCMP solutions is improving — with all vendors now offering SaaS solutions — which are beneficial in case of disasters in which internal IT systems are unavailable, and its functionality is expanding to include operational resilience.

Business Impact

Increased interest in robust BCM programs has led to increased interest in the BCMP solution market as organizations seek help to provide a consistent and scalable BCM development process. Regulators, especially in the financial services sector, are focusing on operational resilience, which includes BCM, cybersecurity, third-party risk management and cyber risk management. As a result, organizations need to prove their level of compliance, and BCMP solutions can help.

Drivers

- Businesses from all market sectors, and of differing types, are increasingly interested in BCMP solutions because they see them as an easy way to start a BCM program. These solutions offer great benefits, due to their standardization and centralization of BCM activities.

- Some BCMP solutions have operational resilience functionality in support of the Bank of England's Operational Resilience regulation and in anticipation of the EU's Digital Operational Resilience Act (DORA).

- BCMP solutions can benefit every organization that wants to perform a comprehensive analysis of its preparedness to cope with business or IT interruptions.

- Many vendors offer a modular, "prebuilt" or "out-of-the-box" approach to implementing their solutions. This enables smaller organizations to start a program while controlling costs and to build the functionality in their solution at their own pace.

- Information from BCMP solutions can enhance business operations and resilience for more than just recovery purposes. This is especially the case for business operations and in areas like cyber risk management and digital risk management.

- Some governance, risk and compliance (GRC) vendors offer BCMP capabilities, which could increase interest in BCMP solutions by enabling the customer to fulfill an integrated risk management process within their organization.

- The BCMP solution market is used chiefly by large and extra-large organizations, regulated enterprises, government agencies and organizations with complex business operations. But more vendors are taking a modular approach to implementation of BCMP solutions and offering adaptability to increase accessibility to small and midsize enterprises.

- There is wide adoption of BCMP solutions in the following sectors: financial services/banking, insurance, healthcare/life sciences, public sector/government, technology solutions and manufacturing. There is also wide adoption in North America, South America, Europe, Asia/Pacific and the United Arab Emirates.

Obstacles

- If an organization is not committed to BCM, it should not buy a BCMP solution.
- If an organization's BCM processes are highly ad hoc and nonstandardized, it would have to rationalize some of those processes before implementing a BCMP solution, in order not to instantiate "bad process."
- An organization's risk management department may already be using a GRC solution that has a BCMP module. In that case, it is important not to implement BCM functionality for the sake of having just one vendor to manage multiple risk domains.

User Recommendations

- Review all use cases for risk management, business continuity, disaster recovery, emergency notification and crisis management to ensure a BCMP solution can fulfill current and future requirements.
- Implement a BCMP solution when: you are starting a new BCM program or maturing one and want to follow standard practices, or if greater program management analytics are required; you want more control over the execution of the BCM program life cycle; or when integrating recovery plans from several departments, business units, divisions and legal entities into a consistent and easily updated set of recovery plans.
- Do not overbuy. Focus on ease of use for all users; ease of configuration and reporting; ease of integration with key business applications (enterprise directories, HR tools, business process management tools, IT asset management tools and other BCM solutions); and mobile device support for recovery plan access and execution during a business disruption.

Sample Vendors

Agility Recovery; Castellan Solutions; CLDigital; Fusion Risk Management; Infinite Blue; Premier Continuum; SAI360; ServiceNow; Symphony Software

Gartner Recommended Reading

Toolkit: Vendor Identification and Selection Guide for Business Continuity Management Software.

The BCM Software Ecosystem — Presentation Materials

Cybersecurity Maturity Assessments

Analysis By: Deepti Gopal, Mia Yu

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

A cybersecurity maturity assessment evaluates an organization's cybersecurity program, and its underlying people, processes and technologies. This evaluation generally includes a defined model that is based on guidance from industry standards and frameworks, and assesses distinct levels of maturity. Maturity assessments are used to guide priorities and highlight areas for improvement that may be required.

Why This Is Important

Organizations find it challenging to articulate the benefits of cybersecurity and maintain support for further investment. Cybersecurity maturity assessments are a common method to measure the capability of their cybersecurity program against a set of predefined outcomes and desired capabilities. As a result, adoption is widespread across all industries.

Business Impact

Cybersecurity maturity assessments are critical during initial cybersecurity strategy planning, helping form an understanding of how well the security organization is performing in its current state, and guiding priorities and investments to achieve the desired target state. Increased maturity can help transform the overall security function and optimize investments based on dependencies between capabilities.

Drivers

Cybersecurity maturity assessments have become an essential tool to:

- Inform the strategic planning activities in pursuit of the desired level of cybersecurity capability.

- Demonstrate the perceived effectiveness of the cybersecurity function against an industry model by providing the ability to benchmark against similar organizations and industries. Ensure that a minimum standard of care is met when compared to peers.
- Demand investment in cybersecurity and subsequently demonstrate improvements over time, as a result of the investment.
- Help reach internal consensus on actual and desired maturity levels over time as expectations on the cybersecurity program increase.

Obstacles

- Most assessments measure only the implementation of controls, with “maturity” reflecting implementation tiers, such as the Australian Cyber Security Centre’s (ACSC’s) Essential Eight Maturity Model or the National Institute of Standards and Technology’s (NIST’s) Cybersecurity Framework (CSF). NIST’s CSF explicitly states that the implementation tiers do not necessarily represent maturity. A small subset assesses people, processes and technology capabilities to determine overall maturity.
- Most maturity assessments claim to be based on the Capability Maturity Model Integration (CMMI) method. However, there is no industry standardization on the capabilities assessed, nor are there standard algorithms for assessing the maturity levels. Hence, no meaningful comparisons can be drawn between results from different assessments.
- Maturity assessments are typically self-assessments or facilitated self-assessments performed in conjunction with recognizable consulting firms. Neither provides an in-depth assessment of the capabilities’ effectiveness.

User Recommendations

- Assess maturity regularly to guide priorities and inform strategic plans aimed at the desired levels of cybersecurity capability. Remember that the value of a maturity assessment will diminish as maturity increases.
- Select a maturity assessment that evaluates the broader security function and not only the implementation of controls.
- Avoid using a maturity assessment in isolation. Maturity neither translates directly into reduced risks or increased value nor does it replace an audit.
- Validate the outputs with an outcome-driven assurance program. Then, supplement them with an assessment of external threats, value of the information assets being protected, business objectives, vulnerabilities, risk appetite and risk profile. This way, you translate maturity into an understanding of risk.
- Interpret the source of the assessment correctly to avoid creating a false sense of security based on a self-assessed maturity score.

Sample Vendors

Accenture; Blue Lava; Deloitte; EY; KPMG; PwC; RealCISO; TrustMAPP; V3 Cybersecurity

Gartner Recommended Reading

IT Score for Security and Risk Management

Cybersecurity Controls Assessment

Frequently Asked Questions on the IT Score for Security and Risk Management

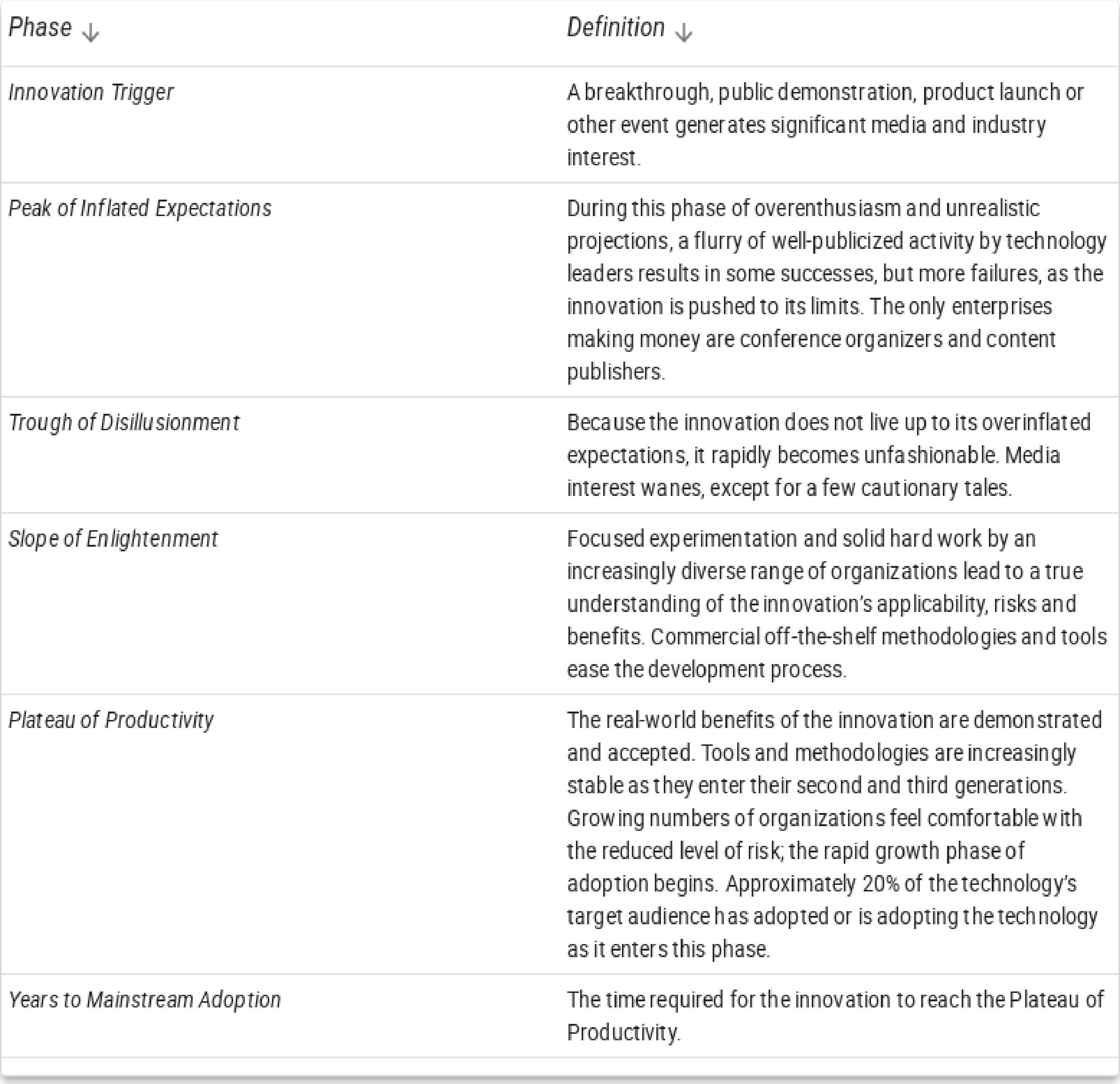
Appendixes

See the previous Hype Cycle: Hype Cycle for Cyber Risk Management, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)



Phase ↓	*Definition* ↓
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

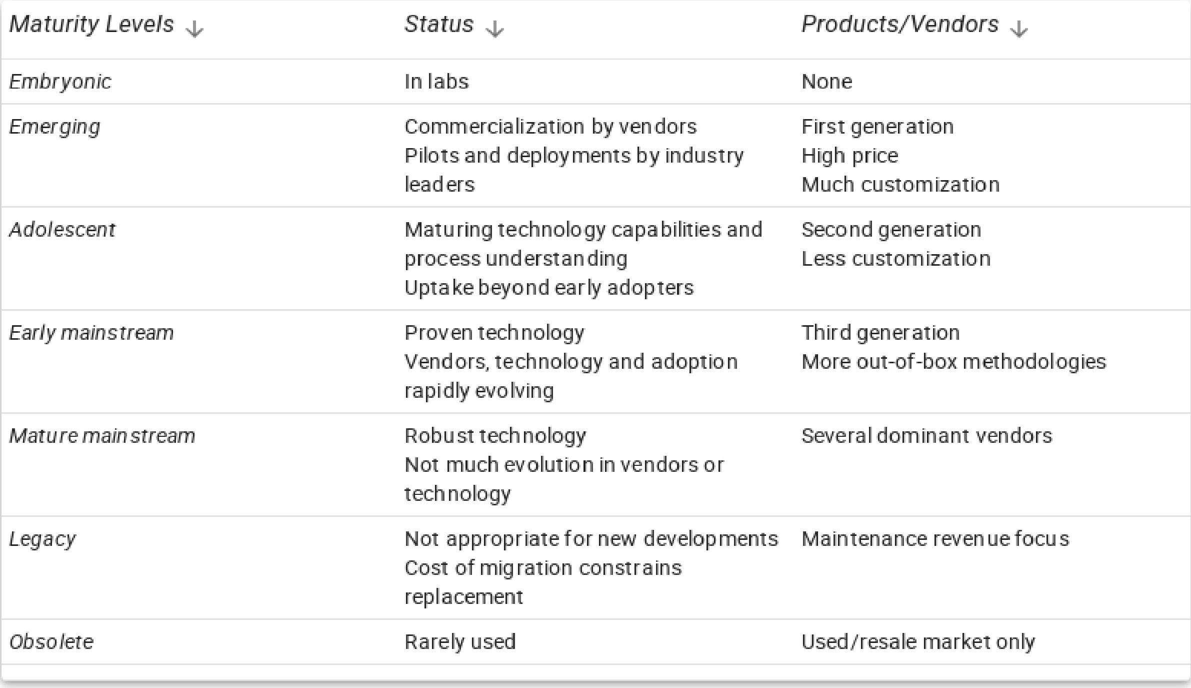
Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)



Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Document Revision History

Hype Cycle for Cyber Risk Management, 2022 - 27 July 2022

Hype Cycle for Cyber and IT Risk Management, 2021 - 19 July 2021

Hype Cycle for Risk Management, 2020 - 9 July 2020

Hype Cycle for Risk Management, 2019 - 24 July 2019

Hype Cycle for Risk Management, 2018 - 13 July 2018

Hype Cycle for Risk Management, 2017 - 19 July 2017

Hype Cycle for Risk Management Solutions, 2016 - 6 July 2016

Hype Cycle for Governance, Risk and Compliance Technologies, 2015 - 10 July 2015

Hype Cycle for Governance, Risk and Compliance Technologies, 2014 - 17 July 2014

Hype Cycle for Governance, Risk and Compliance Technologies, 2013 - 24 July 2013

Hype Cycle for Governance, Risk and Compliance Technologies, 2012 - 30 July 2012

Hype Cycle for Governance, Risk and Compliance Technologies, 2011 - 26 July 2011

Hype Cycle for Governance, Risk and Compliance Technologies, 2010 - 28 July 2010

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Dynamic Risk Governance Is the New Risk Mandate for Executive Leaders

Quick Answer: What Are CISOs Using Cyber-Risk Quantification For?

4 Ways Generative AI Will Impact CISOs and Their Teams

Business Capability Maturity Model (RBC)

Innovation Insight: Cybersecurity Continuous Control Monitoring

Innovation Insight on Security Behavior and Culture Program Capabilities

Market Guide for CPS Protection Platforms

Table 1: Priority Matrix for Cyber Risk Management, 2023

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Cyber-Physical Systems Dynamic Risk Governance Security Service Edge	FinDRA Generative Cybersecurity AI	
High	Business Continuity Management Program Solutions Hazard/Threat Intelligence Services ITRM Solutions	CPS Risk Management Cyber-Risk Quantification Data Classification Environmental, Social and Governance Privacy Impact Assessments Supply Chain Risk Management Threat Modeling Automation	Continuous Controls Monitoring	Connected Governance
Moderate	Cybersecurity Maturity Assessments Risk Management KCIs Security Rating Services	Continuous Compliance Automation Digital Risk Protection Services IT Vendor Risk Management	CAASM	
Low				

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase ↓	*Definition* ↓
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	*Definition* ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)