Information Security Forum

THREAT HORIZON 2021

THE DIGITAL ILLUSION SHATTERS

Threat Horizon 2021

The digital illusion shatters

JANUARY 2019

PUBLISHED BY

Information Security Forum Limited
+44 (0)20 3875 6868
info@securityforum.org
securityforum.org

PROJECT TEAM

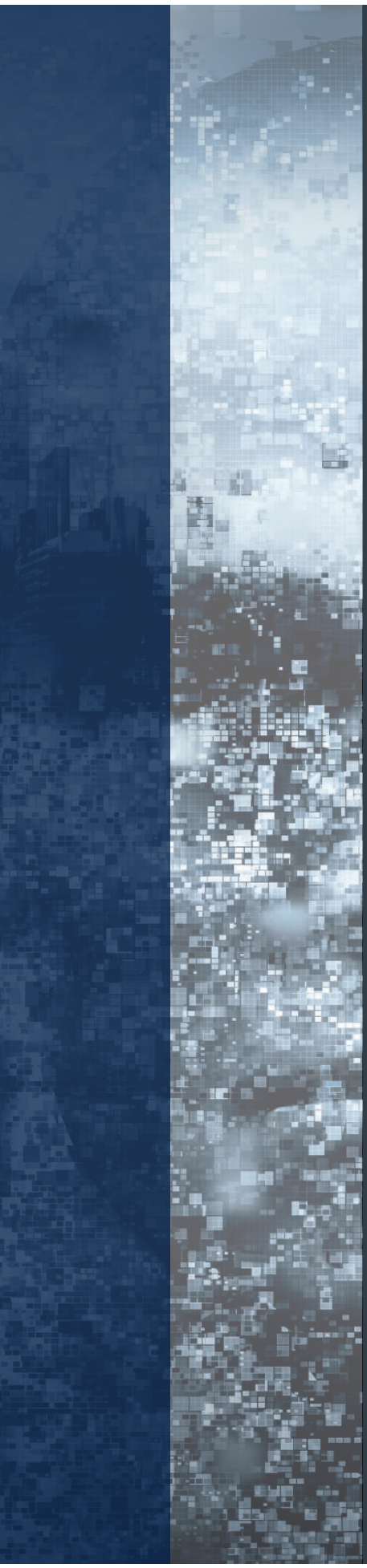
Dan Norman – Lead
Gareth Haken – Contributor

REVIEW AND QUALITY ASSURANCE

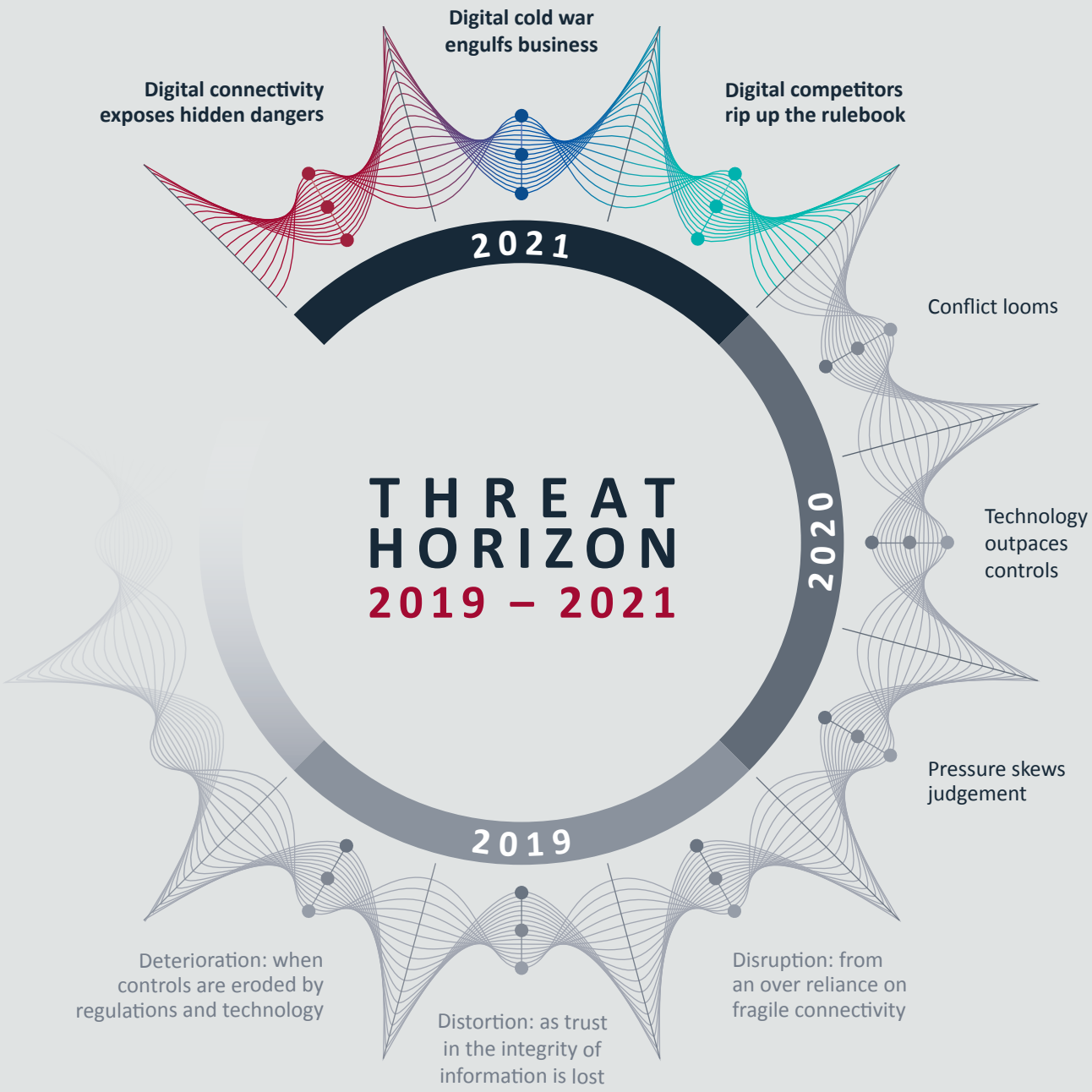
Andy Jones
Richard Absalom
Eleanor Thrower

DESIGN

Shane Kearney
Abigail Palmer
Kim Whyte



CONTENTS



THREAT HORIZON
2019 – 2021

2019

1.1 Premeditated internet outages bring trade to its knees
1.2 Ransomware hijacks the Internet of Things
1.3 Privileged insiders coerced into giving up the crown jewels

2.1 Automated misinformation gains instant credibility
2.2 Falsified information compromises performance
2.3 Subverted blockchains shatter trust

3.1 Surveillance laws expose corporate secrets
3.2 Privacy regulations impede the monitoring of insider threats
3.3 A headlong rush to deploy AI leads to unexpected outcomes

2020

1.1 Cyber and physical attacks combine to shatter business resilience
1.2 Satellites cause chaos on the ground
1.3 Weaponised appliances leave organisations powerless

2.1 Quantum arms race undermines the digital economy
2.2 Artificially intelligent malware amplifies attackers' capabilities
2.3 Attacks on connected vehicles put the brakes on operations

3.1 Biometrics offer a false sense of security
3.2 New regulations increase the risk and compliance burden
3.3 Trusted professionals divulge organisational weak points

2021

1.1 5G technologies broaden attack surfaces
1.2 Manipulated machine learning sows confusion
1.3 Parasitic malware feasts on critical infrastructure

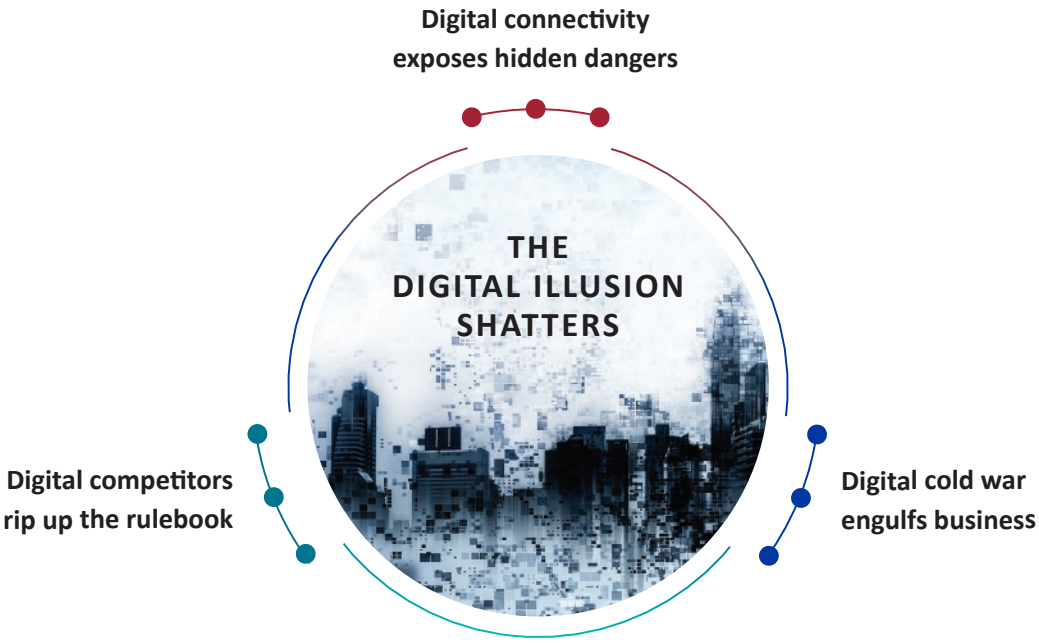
2.1 State-backed espionage targets next gen tech
2.2 Sabotaged cloud services freeze operations
2.3 Drones become both predator and prey

3.1 Digital vigilantes weaponise vulnerability disclosure
3.2 Big tech break up fractures business models
3.3 Rushed digital transformations destroy trust

INTRODUCTION

By 2021 the world will be heavily digitised. Technology will enable innovative digital business models and society will be critically dependent on technology to function. This new hyperconnected digital era will create an impression of stability, security and reliability. However, it will prove to be an illusion that is shattered by new vulnerabilities, relentless attacks and disruptive cyber threats.

This report provides organisations' leaders with an early insight into the profound changes they may expect over the coming years and some of the key actions they should consider now. Produced annually in collaboration with the community of over 480 ISF Member organisations across the globe, this latest version of the ***Threat Horizon*** report series presents nine threats that organisations in all sectors and geographies can expect to disrupt their operations and plans over the next two to three years. The impacts of these threats are set out under three themes.



Over the coming years a range of damaging threats will materialise. Vulnerabilities will be shared across interconnected systems; malware attacks will be amplified by superfast networks; and business models using machine learning techniques will become a prime target. Impacts will reverberate across the digital world.

Nation states will exploit this digitisation, thrusting the world into a new digital cold war. They will vie for winner-takes-all supremacy across a range of next generation technologies, employing espionage techniques to steal intellectual property, sabotage critical infrastructure by attacking cloud services and weaponise drone technologies to undermine business.

Businesses will have to compete in an environment that is being destabilised by tensions between big tech giants and regulators. As the rules change, attempts to thrive will be undermined by both malicious attacks and self-inflicted damage.

Organisations that can see through the digital illusion will succeed. Those that are fooled will not.

THE WORLD IN 2021

This illustration of what the world will look like in 2021 provides context and background to the nine threats in this report. It is set out using the PESTLE model (see Figure 1) to provide a balanced picture and provoke thought and debate.

Figure 1: The PESTLE model

Throughout this report

Each of the nine threats includes a high-level illustration showing which of the PESTLE factors will drive or influence the threat. These can act as an indicator to help the reader validate or prioritise each threat.

Before studying the predicted threats in this report, the reader is encouraged to assess the forecasts presented in this section and to consider them in the context of their own organisation. While these forecasts build on input from ISF Members, the ISF Global Team and external experts, every organisation will have its own view. Are these predictions reasonable? Do some underestimate the severity of certain scenarios? Do others go too far? How might the forecasts be adapted in the context of a specific organisation? What additional material (e.g. relating to specific industries or geographies) would be needed to support an organisational review of the predicted threats in this report?

A WORLD VIEW

By 2021 the world will be significantly digitised and connected. The race to develop the next generation of super-intelligent machines will be in full swing and technology will be intertwined with everyday life. Coupled with heightened global mistrust and rising geopolitical tensions, this will lead to a cyber threat that is relentless, targeted and disruptive. The operating environment for business will become increasingly volatile.

The geopolitical arena will be complex, turbulent and fragile, as the US and China battle for global dominance. The world order will shake as the EU continues to fracture post-Brexit, Russia becomes politically resurgent and disgruntled South American and Asian countries struggle to meet the expectations of a growing middle class. Frustration with liberalism and globalism will lead to more inward-facing policies. National and commercial interests will blur as big tech giants consolidate power and continue to influence politics and society.

Economic tension will grow and protectionism will be rife, as more countries join a global trade war. Governments and businesses will look to technology to drive economic growth, seeking to achieve world-leading positions in next generation technologies. However, major technology investments will fail to live up to expectations, disappointing investors and creating a burden of debt.

Growing understanding of the power and influence big tech giants have on politics and society will lead to social disillusionment. Society will become increasingly polarised as popularism and tribalism spread. Automation will start to pose a significant threat to the job market as AI and robotics mature and enter the workplace. Technology will intrude on many aspects of personal and working life, creating a digital-centric, always-connected society that raises fundamental questions around social well-being.

Technological step changes will affect entire business models, as 5G, Artificial Intelligence (AI), drones, quantum computers and an expanding nexus of Internet of Things (IOT) devices receive significant investment. Superfast and ubiquitous digital interconnectivity will create new business opportunities and help to build more intimate relationships with customers – but at the expense of a more evolved, complex threat landscape.

Privacy regulations will continue to dominate the legal agenda and will be joined by a focus on critical infrastructure and IoT, providing further challenges for global organisations as a plethora of legislation stifles innovation. Growing scrutiny of big tech firms by governments and regulators will result in at least one of those companies being broken up, significantly disrupting the availability of products and services they provide.

The continued extraction of natural resources that are fuelling technological growth (such as cobalt used in batteries) will increasingly become an environmental and supply chain concern. There will be a growing governmental and societal focus on reducing dependencies on resources such as oil and plastic, but global progress will be slow. Extreme weather events will become more frequent and continue to grow in scale and impact.

THEME

1 DIGITAL CONNECTIVITY EXPOSES HIDDEN DANGERS

Vast webs of intelligent devices, combined with increased speeds, automation and digitisation will create possibilities for businesses and consumers that were previously out of reach. The Internet of Things (IoT) will continue to develop at an astonishing rate, with sensors and cameras embedded into a range of devices across critical infrastructure. The resulting nexus of complex digital connectivity will prove to be a weakness as modern life becomes entirely dependent on connected technologies, amplifying existing dangers and creating new ones.

1.1 5G TECHNOLOGIES BROADEN ATTACK SURFACES

The emergence of the fifth generation of mobile networks and technologies (5G) will provide a game-changing platform for businesses and consumers alike. Colossal speeds, minimal latency and a range of newly available radio frequencies will connect previously unconnected devices, accelerate processes and change entire operating models – but with these changes comes a broader attack surface, as millions of telecommunication masts are built with varying levels of security. As organisations become heavily reliant on 5G to operate, new attack vectors will exploit weaknesses in this emerging technology.

1.2 MANIPULATED MACHINE LEARNING SOWS CONFUSION

Machine learning, and neural networks in particular, will underpin processes such as image recognition, pricing analysis and logistics planning. As businesses become reliant upon machine learning and humans are taken out of the knowledge loop, machine learning will become a prime target for attackers. Confusion, obfuscation, and deception will be used by attackers to manipulate these systems, either for financial gain or to cause as much damage and disruption as possible.

1.3 PARASITIC MALWARE FEASTS ON CRITICAL INFRASTRUCTURE

Parasitic malware is a particular strain of malware designed to steal processing power, traditionally from computers and mobile devices. However, attackers will turn their attention to the vast interconnectivity and power consumption of Industrial Control Systems (ICS), IoT devices and other critical infrastructure, which offer an enticing environment for this malware to thrive. All organisations will be threatened as this form of malware sucks the life out of systems, degrading performance and potentially shutting down critical services.

START PREPARING NOW

In a hyperconnected world, attack surfaces and interdependencies will grow astonishingly quickly. By understanding and evaluating how these new technologies will be leveraged for competitive advantage, organisations may be able to invest in controls to protect against any new threats that they pose. Organisations must be agile enough to adapt to heightened digital connectivity, ensuring that new security mechanisms are implemented should existing ones prove ineffective.

1.1 5G TECHNOLOGIES BROADEN ATTACK SURFACES

WHAT IS THE IMPACT OF THIS THREAT?

The arrival of 5G, with significantly faster speeds, increased capacity and lower latency, will change existing operating environments, but at the expense of an exponential growth of attack surfaces. The 5G-enabled devices and networks that underpin society will be compromised by new and traditional attacks, causing chaos and plunging business into disarray.

The impacts of attacks on 5G technologies and infrastructure will be felt across a range of industries who leverage 5G to become more operationally efficient or to automate and speed up processes. There will be countless opportunities to attack 5G infrastructure, including billions of previously unconnected IoT devices and new private networks. Millions of new 5G-enabled masts, built and operated by a plethora of companies and governments to varying levels of assurance, will have new vulnerabilities exposed and create new ingress points for attackers to exploit. The step change in available bandwidth will act as an accelerator to existing attacks and amplify new ones, stretching organisational resilience to its maximum.

Critical national infrastructure (CNI), IoT manufacturers, businesses and citizens will all be heavily or totally dependent on 5G to operate, offering ripe targets for a range of attackers. From nation states aiming to cripple CNI – to hackers spying on private networks – 5G technologies and infrastructure will become a key target.

Imagine this happens… the operators of an industrial-sized farm have leveraged a private 5G network to connect its autonomous combine harvesters, crop microsensors and drone monitors. The goal is to create a real-time analytics environment that can be shared with the farming community to boost productivity and reduce costs. At harvest time the farm's private network is jammed and all networks go offline, plunging the harvesting schedule into disarray. **Has your organisation considered the risks of adopting 5G?**

JUSTIFICATION FOR THREAT

5G is one of the technologies that will define the fourth industrial revolution and will be a game-changer for business and consumers alike. The technologies promise greater speeds, lower latency, reduced power consumption and real-time connectivity provided by leveraging newly available high and low frequencies on the radio spectrum. This will enable a raft of changes to the way people live, work and interact with technology, but will also introduce a number of security challenges that will need to be overcome.

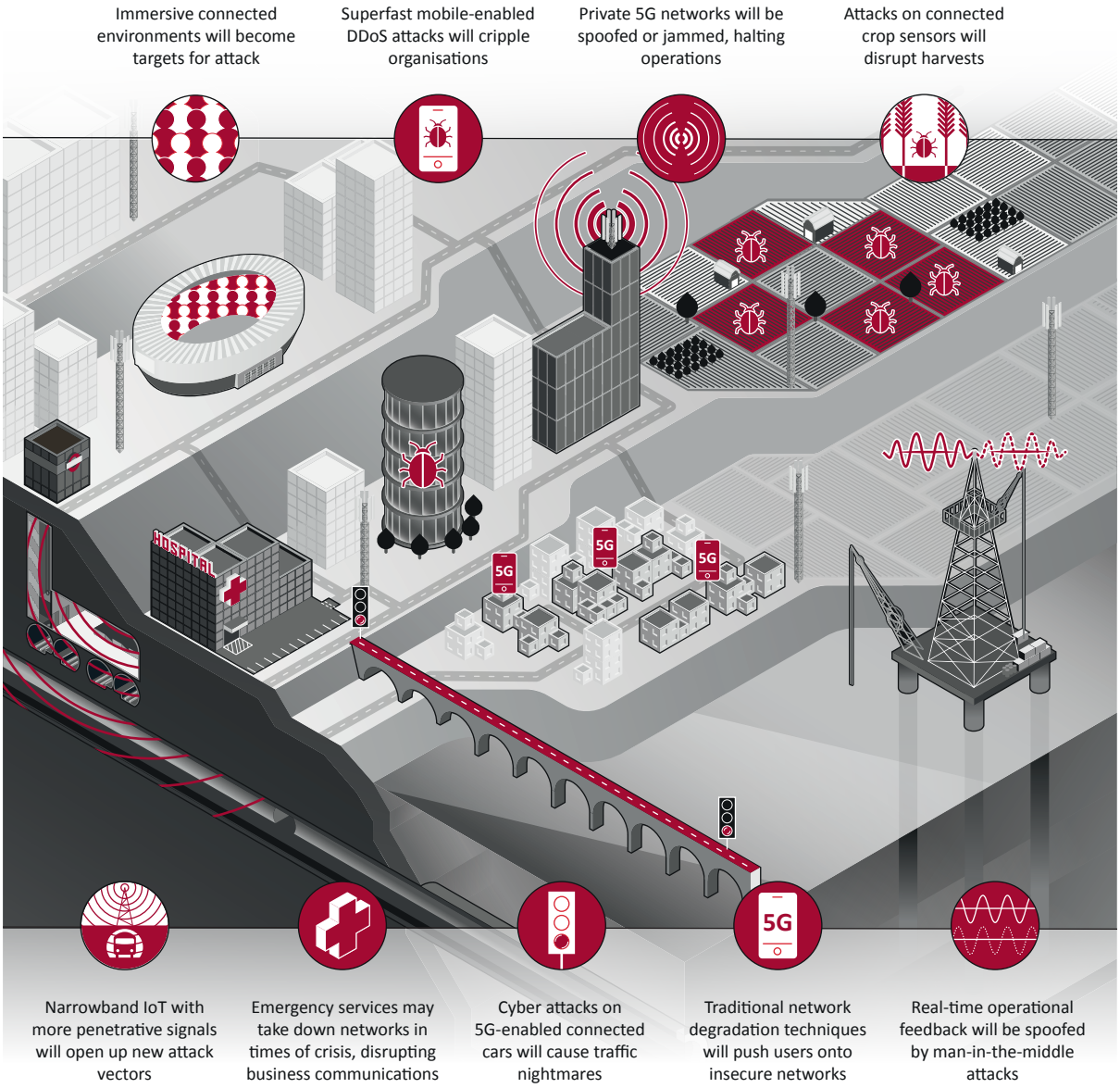
"5G will be a new kind of network, supporting a vast diversity of devices with unprecedented scale, speed and complexity […] 5G will have an impact similar to the introduction of electricity or the automobile, affecting entire economies."

– Stephen Mollenkopf, Qualcomm

5G technologies and infrastructure have attracted significant investment from governments and business alike. Some telecoms providers are expected to roll out consumer mobile networks as early as 2019, whilst other 5G technologies such as private networks will likely be available soon after. China clearly leads the way in terms of 5G development, having built 350,000 new 5G-enabled masts, outstripping US investment by $24bn. The number of masts is only set to grow further across the US, Europe and Asia, as organisations demand further investment in 5G. Many new technologies, including connected cars, augmented reality, immersive connected environments (e.g. smart stadia) and automated drones will be dependent on it to thrive. This has led to significant hype and expectation in the media, which expects 5G to fulfil many future technological promises. However, with these improvements come significant dangers.

Figure 2 demonstrates several examples of how 5G technologies and infrastructure will broaden attack surfaces, as attackers begin to leverage the high-speed data networks to amplify traditional attacks and target new infrastructure, such as masts and hard-to-reach narrowband IoT devices.

Figure 2: Examples of 5G-enabled attacks



CNI that leverages 5G to control machine-to-machine communications will also become a prime target. Deeply embedded IoT devices, such as energy monitors, water meters and waste management sensors, will be systemically targeted by attackers aiming to disrupt supply chains and other dependent infrastructure. The speed of 5G will exceed that of Wi-Fi, tempting organisations to install private 5G networks. Operational environments, from factory floors to farms, will change entirely as 5G-enabled technologies and infrastructure become intertwined with product and service offerings. Spoofing and jamming of 5G networks will become a common attack vector for those aiming to disrupt economies dependent on 5G.

The number of masts required to maintain strong 5G signals at high frequencies (e.g. for live video calls or real-time data analytics) will offer a large number of opportunities for attackers to use traditional network degradation techniques to push users onto insecure networks, or to eavesdrop on communications. Terrorists will also conduct attacks near populous 5G areas, either targeting the masts themselves, or faking an attack, knowing that the emergency services will take down or reprioritise 5G networks during a crisis. The amplification of speed, higher bandwidth and reduced latency offered by 5G will also create a perfect environment for massive DDoS attacks, threatening the availability of dependent operations.

The range of new and traditional attacks, sheer complexity of the standards necessary for 5G technologies and infrastructure to work securely and the speed of their evolution, highlights the concern that security may be overlooked. The 5G spectrum will also be auctioned to a range of businesses and governments which will secure the networks to different levels and standards.

HOW SHOULD YOUR ORGANISATION PREPARE?

Organisations must prepare for the arrival of 5G, by understanding how 5G will be used in their own product offerings and how they might be dependent on 5G networks to operate. Organisations that successfully prepare will gain significant competitive advantage from the technologies. Those who get it wrong will find themselves compromised, their operations disrupted and reputations damaged.

Actions for now

- Identify where 5G may be used across the organisation as part of a thorough risk assessment.
- Consider updating crisis management and business continuity plans to reflect the role 5G will play.

Longer-term actions

- Review contractual agreements with 5G providers, considering the range of services and service level they provide.
- Investigate improved technical controls provided by 5G and network providers.
- Assign responsibility for the maintenance of the organisation's private 5G network.
- Increase capacity to deal with more powerful DDoS attacks.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality
Integrity
Availability

Source of threat

Adversarial
Nation state, terrorist group, hacking group, hacktivists

Potential business impact

Financial
Operational
Legal and Regulatory Compliance
Reputational
Health and Safety

ISF RESOURCES

Securing Mobile Apps – *Briefing Paper*

Network Convergence – *Briefing Paper*

Delivering an Effective Cyber Security Exercise

Information Risk Assessment Methodology 2 (IRAM2)

1.2 MANIPULATED MACHINE LEARNING SOWS CONFUSION

WHAT IS THE IMPACT OF THIS THREAT?

Machine learning, and neural networks in particular, will become a prime target for those aiming to manipulate or disrupt dependent products and services. Attackers will exploit vulnerabilities and flaws in machine learning systems by confusing and deceiving algorithms in order to manipulate outcomes for nefarious purposes.

Impacts will be felt across a range of industries. Malicious attacks may result in automated vehicles changing direction unexpectedly, high-frequency trading applications making poor financial decisions and airport facial recognition software failing to recognise terrorists. Organisations will face significant financial, regulatory and reputational damage and lives will be put at risk if machine learning systems are compromised.

Key terminology

Machine learning: the science of training computers to act autonomously without being explicitly programmed.

Neural networks: a subset of machine learning that uses a series of algorithms that endeavour to recognise underlying relationships in a set of data through a process which mimics the way the human brain operates.

Algorithms: a set of steps or instructions for solving a problem or completing a task.

Nation states, terrorists, hacking groups, hacktivists and even rogue competitors will turn their attention to manipulating machine learning systems that underpin products and services. Attacks that are undetectable by humans will target the integrity of information – widespread chaos will ensue for those dependent on services powered primarily by machine learning.

2021

Imagine this happens… a connected vehicle manufacturer is beginning to test a fleet of connected vehicles in a South American city. The vehicles use a neural network which visually classifies a range of road signs. Just before the vehicles are about to start their journeys a hacktivist group vandalises all of the stop signs. Once the vehicles begin driving around the city, they begin to drastically miscategorise the signs, speeding up when they should be stopping, causing chaos on the roads.
Does your organisation proactively assure its machine learning systems operate as intended?

JUSTIFICATION FOR THREAT

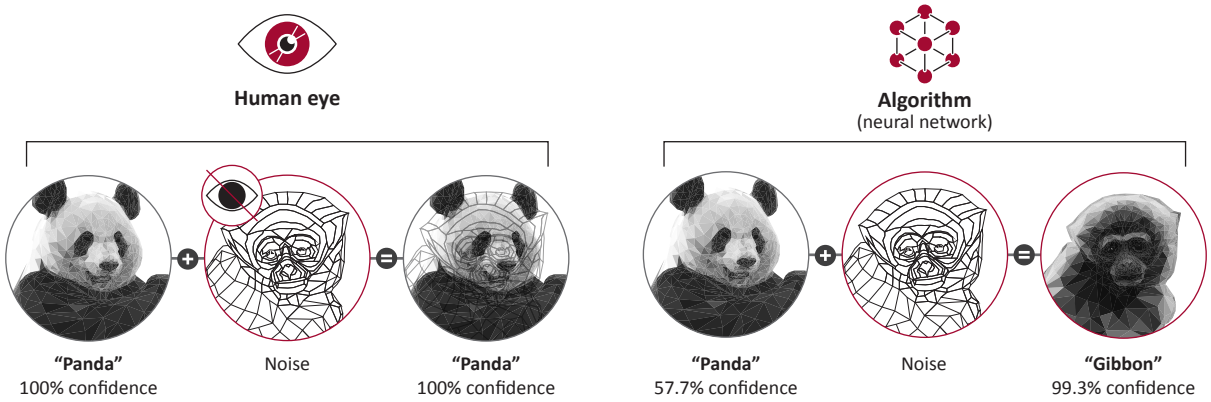
A range of industries will increasingly adopt machine learning systems and neural networks over the coming years in order to help make faster, smarter decisions. They will be embedded into a series of business operations such as marketing, medicine, retail, automated vehicles and military applications. The explosion of data from connected sensors, IoT devices and social media outputs will drive companies to use machine learning to automate processes, with minimal human oversight. As these technologies begin to underpin business models, they will become a prime target.

"These days, nearly every company is using artificial intelligence and machine learning to help make critical business decisions. But few companies have an idea how the systems they employ actually work." – CNBC

Academics have already provided several proof of concept studies highlighting how machine learning can be confused. Students at MIT developed a means of tricking neural network-based image recognition software built on Google's open source software library TensorFlow, forcing the neural network to miscategorise an image of a turtle as a gun. The real-world implications of deliberately miscategorising images used as inputs to machine learning systems would transcend all industries that adopt machine learning for processes and services, significantly threatening human life and damaging corporate reputations.

Figure 3 illustrates how image recognition software built on neural networks can be manipulated. Attackers can place 'noise' over an image or sound, which is undetectable by humans but is picked up by the neural network. This noise fools the neural network into miscategorising the image it sees. In this case the software is deceived into recognising a gibbon instead of a panda.

Figure 3: A proof of concept academic study by Cornell University proving that neural network-based image recognition can be easily manipulated



Applying a similar technique, other academics fooled a neural network in a connected vehicle causing it to miscategorise a stop sign as a different road sign, as shown in Figure 4. By spraying graffiti over the stop sign, the neural network was unable to categorise it correctly; whereas the human eye could make assumptions, even though the sign had been vandalised. If connected vehicles were fooled in this way, there would be significant risk to human life.

Figure 4: A proof of concept joint academic study proving that neural networks in connected vehicles can be confused

Neural networks used in connected vehicles typically gain significant media scrutiny. In March of 2018, a self-driving Uber vehicle travelling at 40 mph in Tempe, Arizona, fatally struck a pedestrian crossing the street in the dark as a result of the vehicle's perception system miscategorising a bicycle she was wheeling as something else. There have also been two cases where image recognition software in Tesla vehicles failed to categorise fire trucks and other vehicles, causing a fatality in one case. While these examples were accidental, they highlight the potential for malicious attacks.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality

Integrity

Availability

Source of threat

Adversarial

Nation state, terrorist group, hacking group

Accidental

Supplier/vendor/partner

Potential business impact

Financial

Operational

Legal and Regulatory Compliance

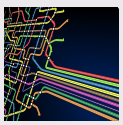
Reputational

Health and Safety

ISF RESOURCES

Threat Intelligence: React and prepare

IRAM2



Securing the Supply Chain: Preventing your suppliers vulnerabilities from becoming your own

HOW SHOULD YOUR ORGANISATION PREPARE?

The damage a compromised machine learning system may bring could be life threatening. Organisations should assess their offerings and dependency on machine learning systems before attackers exploit related vulnerabilities.

Actions for now

- Identify systems which use machine learning, especially recognition-based neural networks, and determine their criticality to the business.
- Employ technical experts in machine learning and recognition-based neural networks.
- Gain assurance that machine learning and recognition-based neural networks provided by external parties are secure by design.

Longer-term actions

- Continuously monitor the dark web for vulnerabilities and exploit code.
- Lobby governments and regulators to introduce regulation around reporting requirements, demanding clear outlines of usage and protection of data used by algorithms in machine learning systems.

1.3 PARASITIC MALWARE FEASTS ON CRITICAL INFRASTRUCTURE

WHAT IS THE IMPACT OF THIS THREAT?

Parasitic malware – which seeks to steal processing power – has traditionally targeted computers and mobile devices. This type of malware will evolve to target more powerful, industrial sources of processing power such as ICS, cloud infrastructures, CNI and the IoT. The malware's primary goal will be to feast on processing power, remaining undetected for as long as possible. Services will be significantly disrupted, becoming entirely unresponsive as they have the life sucked out of them.

Unprepared organisations will have a wide (and often unmonitored) attack surface that can be targeted by parasitic malware. They will see infected devices constantly running at full capacity, raising electricity costs and compromising functionality. Systems will degrade, in some cases leading to unexpected failure that halts critical services.

Every organisation will be susceptible to parasitic malware. However, environments with high power consumption (e.g. power stations, water and waste treatment plants and data centres) and those reliant on industrial IoT (e.g. computerised warehouses, automated factories and smart cities) will become enticing targets for malicious attackers as high power consumption tends to mask the energy usage of parasitic malware.

Imagine this happens… Europe is experiencing an extremely cold winter. Energy providers are working at full capacity to keep citizens warm. One evening a large energy provider's alarms are triggered when a processor in a key heating component fails and thousands of dependent businesses and homes lose power. Incident response teams eventually discover a strain of parasitic malware that had been stealing processing power for months, eventually overloading a key component.
Does your organisation scan for this type of malware?

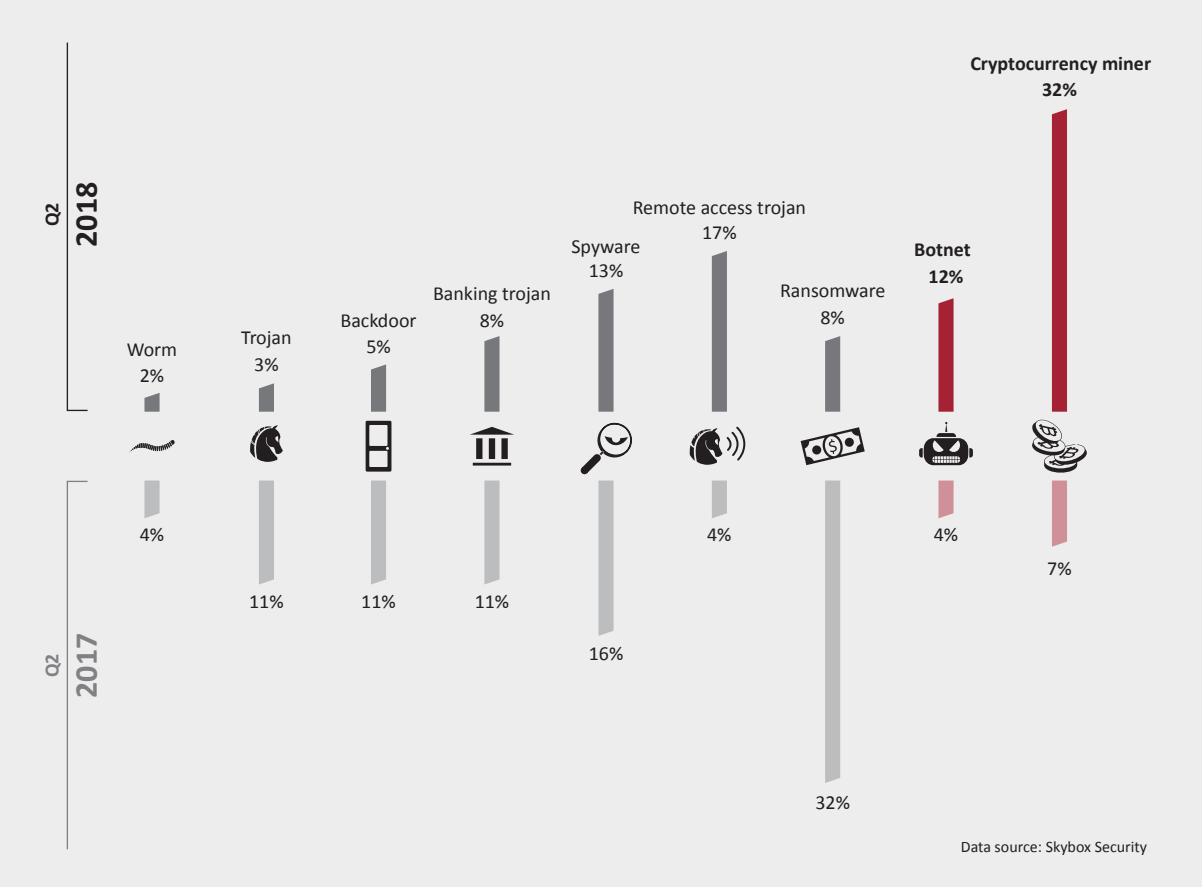
JUSTIFICATION FOR THREAT

ICS, combined with the increased adoption of IoT devices with greater processing power, will provide new and irresistible targets for parasitic malware. Additionally, smart cities have a high degree of digital adoption and, according to ISACA's 2018 Smart City survey, are particularly susceptible to malware.

"Cryptojacking appeals to attackers […] and with so much potential left, it isn't going away any time soon." – Tyler Moffitt, Webroot

'Cryptojacking' is a particularly popular strain of parasitic malware. It is installed on devices and steals processing power in order to illegally mine cryptocurrency. Figure 5 on page 16 demonstrates that there has been a spectacular growth in cases of cryptojacking on computers and mobile devices and that this form of malware is taking over from ransomware as the most prevalent type of malware. Botnets, which also feast on processing power, are continuing to grow in scale and have already proved to have detrimental impacts on infected devices.

Figure 5: The type and percentage of malware attacks from Q2 2017 to Q2 2018



Parasitic malware infections on computers and other devices have already proven to generate significant costs to business. Their consumption of computational resources can cause business-critical systems to slow down or stop functioning entirely with compromised machines even infecting other network-connected devices. Parasitic malware can also exploit often overlooked security holes in a company's network. Organisations infected with parasitic malware are also likely to be vulnerable to other exploits and attacks, such as ransomware.

Given the significant power consumption of ICS and its relatively weak security, lack of monitoring and poor patching regimes, it will become the next frontier for parasitic malware. ICS environments often rely on older hardware and low-bandwidth networks. Consequently, even a slight increase in load could leave them unresponsive. Early 2018 saw the first documented cryptojacking malware attack on an ICS network, targeting a water utility in Europe. The attack was detected by chance before the network was compromised. However, it is just a matter of time before there is a successful attack and CNI is impacted by a serious infection.

"The major concern is that industrial control systems require high processor availability, and any impact to that can cause serious safety concerns."

– Marco Cardacci, RedTeam Security

Cloud infrastructure will also be a target for parasitic malware because it offers an attack surface with large amounts of processing power in an environment where computer resource consumption is difficult to monitor. In February 2018, Tesla found a strain of parasitic malware mining Monero on its AWS cloud servers. Although there was no major impact in this particular case, it indicates the potential for such malware to affect cloud environments.

HOW SHOULD YOUR ORGANISATION PREPARE?

Organisations should start implementing suitable controls to protect against parasitic malware holistically across the business, including areas that have ICS, IoT and cloud deployments.

Actions for now

- Determine the likelihood of parasitic malware infection, e.g. by considering the size and type of organisation, power consumption and types of devices used.
- Monitor energy consumption and processing power to establish a baseline of what normal and peak usage is. Investigate abnormal activity.
- Invest in plugins that can block browser-based parasitic malware injections.
- Update patch management processes to include vulnerable ICS, IoT and cloud deployments.

Longer-term actions

- Keep malware protection products correctly configured and up to date.
- Capture critical ICS and IoT logs for analysis by the Security Operations Centre (SOC).
- Ensure that security requirements are included when procuring ICS and IoT devices.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality
Integrity
Availability

Source of threat

Adversarial
Nation state, terrorist group, organised criminal group

Potential business impact

Financial
Operational
Legal and Regulatory Compliance
Reputational
Health and Safety

ISF RESOURCES

The Standard of Good Practice for Information Security 2018

Information Security in Smart Cities – *Briefing Paper*

Industrial Control Systems: Securing the systems that control physical environments

THEME

2 DIGITAL COLD WAR ENGULFS BUSINESS

By 2021 a digital cold war will unfold, causing significant damage to business. The race to develop strategically important, next generation technologies will provoke a period of intense nation state-backed espionage – intellectual property (IP) will be targeted as the battle for economic and military dominance rages on. Cloud services will become a prime target for sabotage by those seeking to cause disruption to society and business. Drones will become both the weapon and target of choice as attackers turn their attention skywards.

2.1 STATE-BACKED ESPIONAGE TARGETS NEXT GEN TECH

A new wave of nation state-backed espionage will hit businesses as the battle for technological and economic supremacy intensifies. The target: the next generation of technology. History teaches us that at times of great technological change targeted industrial espionage follows. Organisations developing technologies such as Artificial Intelligence (AI), 5G, robotics and quantum computing, will find their IP systematically targeted by nation state-backed actors.

2.2 SABOTAGED CLOUD SERVICES FREEZE OPERATIONS

Popular cloud providers will have further consolidated their market share – organisations will be heavily, if not totally, dependent on cloud providers to operate. Attackers will aim to sabotage cloud services causing disruption to Critical National Infrastructure (CNI), crippling supply chains and compromising vast quantities of data. Organisations and supply chains that are reliant on cloud services will become collateral damage when cloud services go down for extended periods of time.

2.3 DRONES BECOME BOTH PREDATOR AND PREY

Drones will become predators controlled by malicious actors to carry out more targeted attacks on business. Developments in drone technologies, combined with the relaxation of aviation regulations, will amplify attackers' capabilities as the threat landscape takes to the skies. Conversely, drones used for commercial benefit will be preyed upon, hijacked and spoofed, with organisations facing disruption and loss of sensitive data.

START PREPARING NOW

The digital cold war will involve attacks that will be very difficult to attribute – chaos may descend rapidly but may be diffused quickly too. Organisations will need to evaluate the technologies that underpin their operating and service models to understand if they may become a prime target during this period of uncertainty. Supply chains will require re-evaluation, and crisis management and business continuity plans will need to be updated before critical infrastructure and core services are hit.

2.1 STATE-BACKED ESPIONAGE TARGETS NEXT GEN TECH

WHAT IS THE IMPACT OF THIS THREAT?

Nation states' intelligence services will combine forces with commercial organisations to launch a new wave of industrial espionage. Organisations developing strategically important, next generation technologies will be systematically targeted as national and commercial interests blur.

Business models will unravel as data is compromised by nation state-backed attackers aiming to steal secrets and disrupt development. Strategic plans, IP and other trade secrets regarding the next generation of technologies will become a prime target for nation states aiming to get ahead in the race for economic and military superiority. Whilst the concept of espionage is not new, the digital realm has widened the attack surface. Cyber spies will optimise existing tools and develop new ones to launch espionage attacks on a grand scale. Targeted organisations should expect to face sustained and well-funded attacks, involving a range of techniques such as drone surveillance, zero-day exploits, DDoS attacks and advanced persistent threats. This will be amplified by concerted attempts to infiltrate organisations and coerce existing employees.

Espionage

Spying, or the use of spies to obtain information.

In the digital cold war, espionage will become virtual – harder to detect and harder to prove. Information or intelligence can win or lose wars, and the digital cold war will prove no exception.

The first nation state to develop technologies such as AI, 5G, robotics and quantum computing will gain unparalleled economic, social and military advantage over rivals. Organisations involved in their development will become highly enticing targets for nation state-backed espionage.

Imagine this happens… a technology manufacturer is close to a breakthrough in the development of its prototype quantum computer. The research and development department (R&D) has a culture of collaboration and sharing, but a reputation within the business for low security awareness, weak physical security and poor vetting of employees. **How do you advise the business?**

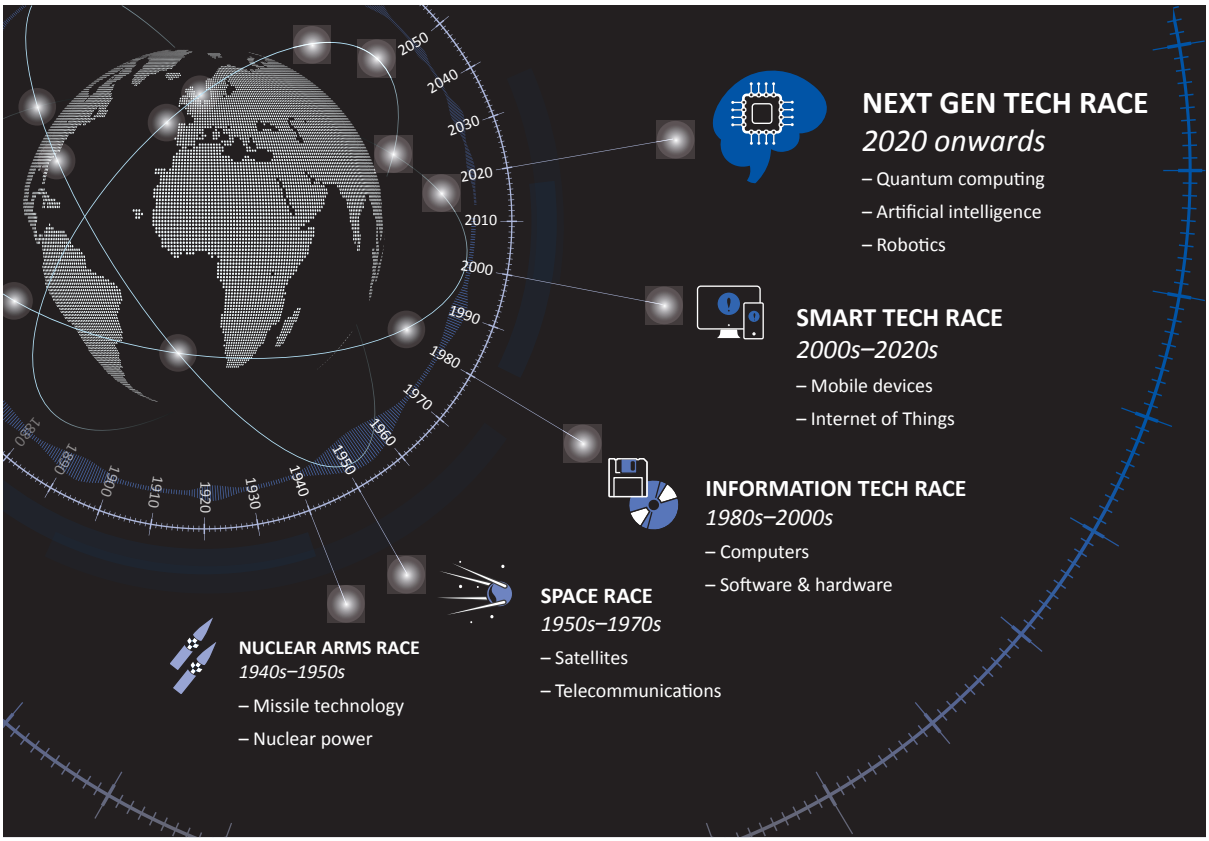
JUSTIFICATION FOR THREAT

Nation states have fought for supremacy throughout history by racing to develop strategic technologies. In recent history this race has involved targeted espionage on nuclear, space, information and now smart technologies, such as IoT. Traditionally, when expectations around next generation technology ramps up, a period of significant espionage ensues. Figure 6 on page 20 illustrates the evolution of key strategic technologies that have been targeted by espionage and IP theft, and highlights the future targets.

"Industrial espionage is nothing new. Theft of trade secrets and corporate intellectual property such as proprietary manufacturing processes, formulas, recipes, and product designs has been happening for decades. […] These days there's an approach that's much easier and less costly for the perpetrator: cyberespionage." – Phil Neray, Cyber X

IP theft accounts for more than 25% of the annual $600bn global cost of cyber crime, with the cost of cyber crime expected to rise year on year. Nation states are going to drive growth in IP theft, with reports that some have already resumed espionage in the high-tech industry.

Figure 6: State-backed espionage targeting strategic technologies – past, present and future



A global retreat into protectionism, increased trade tariffs and embargos will dramatically reduce the opportunity to collaborate on the development of strategically important technology. Indicators of fractured geopolitical relationships have been evident throughout 2018, demonstrated by the developing trade war between the US and China, and the uncertain relationship between the UK and the rest of the EU. For example, in December 2018 the UK pulled out of the Galileo satellite-defence programme after being denied a central role in the project post-Brexit, highlighting a decrease in international collaboration.

Regulatory tit-for-tat battles will manifest across nation states in the form of ‘mandatory technology standards', forcing organisations to disclose IP to domestic rivals. For example, there is already considerable ambiguity over whether foreign companies doing business in China must share sensitive IP if they wish to continue operating there. Organisations will struggle to implement a consistent global approach to controls that help to protect IP across multiple regions of the world, adding another dimension to the difficulties of protecting against espionage.

HOW SHOULD YOUR ORGANISATION PREPARE?

Organisations that use or develop next generation technologies will need to take proactive steps to secure IP or take legal steps to mitigate the impact of espionage.

Actions for now

- Deploy physical security controls, such as turnstiles, blackout blinds or airlocks.
- Increase vetting of staff with access to high-value IP.
- Adopt proactive counter-espionage techniques, such as honeypots.
- Perform a specialised cyber security exercise simulating espionage.
- Adopt a low-profile approach to R&D to avoid becoming a target for espionage.

Longer-term actions

- Adopt a data-centric security posture by:
  - extending a data leakage prevention implementation to cover a wider range of data and attack vectors.
  - implementing digital rights management for high-value IP.
- Legally protect high-value IP, e.g. via copyright, trademark or patent.
- Take out cyber security insurance against competitor espionage or IP theft.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality
Integrity
Availability

Source of threat

Adversarial
Nation state, competitors

Potential business impact

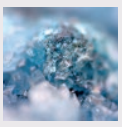
Financial
Operational
Legal and Regulatory Compliance
Reputational
Health and Safety

ISF RESOURCES


Delivering an Effective Cyber Security Exercise


Data Leakage Prevention – *Briefing Paper*


Managing the Insider Threat: Improving trustworthiness – *Briefing Paper*


Protecting the Crown Jewels: How to secure mission-critical information assets

2.2 SABOTAGED CLOUD SERVICES FREEZE OPERATIONS

WHAT IS THE IMPACT OF THIS THREAT?

Cloud service providers will be systematically sabotaged by attackers aiming to disrupt CNI or cripple supply chains. Organisations dependent on cloud services will find their operations and supply chains undermined when key cloud services go down for extended periods of time.

Nation states that engage in a digital cold war will aim to disrupt economies and take down CNI by sabotaging cloud infrastructure through traditional physical attacks or by exploiting vulnerabilities across homogeneous technologies. Attacks on cloud providers will become more regular, resulting in significant damage to businesses which share those platforms. Organisations with a just-in-time supply chain model will be particularly vulnerable to service outages and will struggle to know when services will be restored, as cloud providers scramble to prioritise customer recovery.

Further consolidation of the cloud services market will create a small number of distinct targets that underpin a significant number of business models, government services and critical infrastructure. A single act of sabotage will freeze operations across the globe.

Sabotage

Destructive or obstructive action intended to hinder military or industrial activity.

In the digital cold war, sabotage will be performed from afar at network speed. By attacking common shared platforms, a single blow will devastate industries.

2021

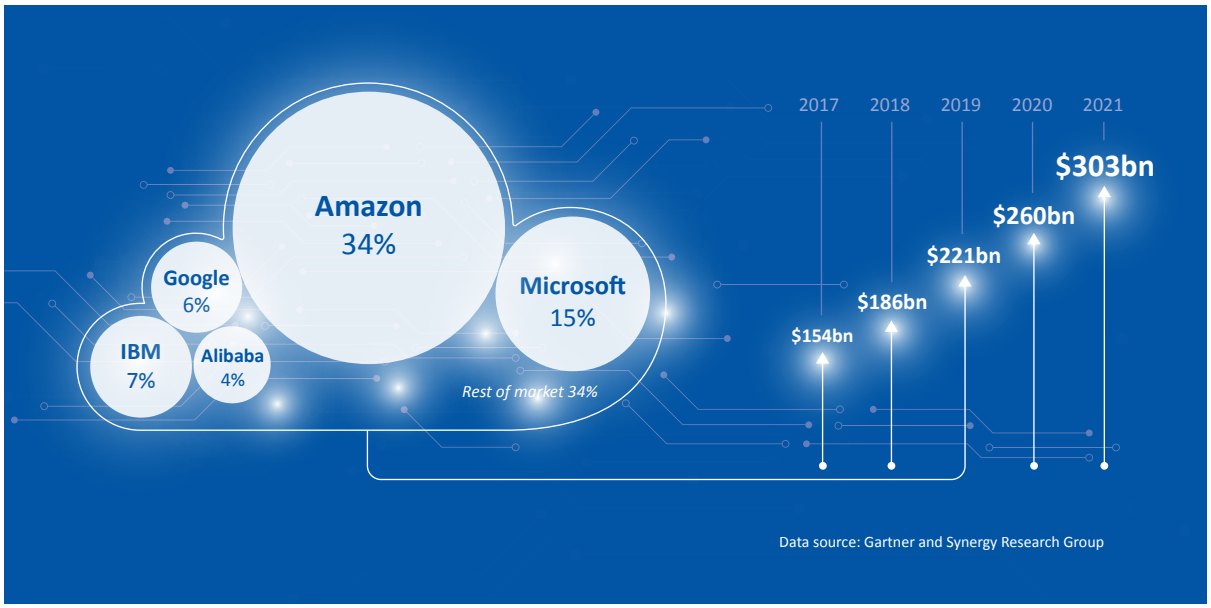
Imagine this happens… one of a supermarket's third party suppliers has moved its systems to a single cloud provider. However, a half-day outage of the cloud provider during the run up to Christmas results in empty shelves across the supermarket's stores nationwide. Panic buying ensues as customers battle for remaining products. **Do you fully understand your cloud dependencies?**

JUSTIFICATION FOR THREAT

According to Gartner, the cloud services market is expected to grow from $221bn in 2019 to $303bn by 2021. As highlighted in Figure 7 on page 23, the five largest cloud providers account for 66% of the global cloud market, with further consolidation of the market expected. This will create an attractive target for attackers – from nation states aiming to disrupt CNI – to organised criminal groups seeking to steal data. These popular cloud providers will become a point of failure, posing significant risk to businesses which are operationally dependent on them or have supply chain partners with similar dependencies.

"Over reliance on cloud services is a bubble that is going to burst very soon. What are organisations going to do when all of their services dependent on one cloud provider goes down?" – ISF Member

Figure 7: A breakdown of market share for cloud services globally, and revenue forecast from 2017–2021



The two largest cloud providers (Amazon and Microsoft) account for nearly half of all cloud services. Microsoft, Google and Alibaba have all grown their market shares substantially, but this has not been at the expense of Amazon – it is the small-to-medium sized cloud providers who collectively have seen their market shares diminish. This has effectively consolidated the market, allowing attackers to focus on fewer, but richer targets.

The large cloud providers boast a plethora of high-profile customers, including government departments, organisations involved with CNI and a number of information security providers. If a cloud provider was to be systematically targeted via traditional DDoS, physical attacks or other means, there would be significant disruption to its services and dependent organisations. Some organisations also rely upon multiple cloud providers to underpin individual systems, but in doing so create multiple points of failure.

In order to optimise their services, cloud providers use common technologies, such as virtualisation. Vulnerabilities discovered in these homogeneous technologies will have wide-reaching impact across multiple cloud providers. Issues of this kind have been seen previously with the Spectre and Meltdown security vulnerabilities, which affected a significant number of organisations.

Several previous cloud outages have been caused by human errors or natural disasters. In February 2017 one of Amazon's regions, US-East-1, was taken offline due to human error. This had a direct effect on IoT devices which use Amazon's cloud services, such as the smart home app Hive. A number of high-profile websites were also taken completely offline, resulting in lost revenue. In July 2018 Google Cloud also experienced an outage, affecting users' ability to access Snapchat and Spotify. These incidents exemplify the potential impact of cloud outages. Determined attackers are likely to develop skills and resources to deliberately compromise and exploit these cloud services over the coming years.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality
Integrity
Availability

Source of threat

Adversarial
Nation state, terrorist group, hacking group, hacktivists

Accidental
Employee (external), employee (internal)

Environmental
Hurricane, tornado, earthquake, volcanic eruption, fire (wild), fire (structural)

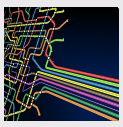
Potential business impact

Financial
Operational
Legal and Regulatory Compliance
Reputational
Health and Safety

ISF RESOURCES

Securing Cloud Computing: Addressing the seven deadly sins

Cyber Security Strategies: Achieving cyber resilience



Securing the Supply Chain

HOW SHOULD YOUR ORGANISATION PREPARE?

Organisations that are reliant on cloud providers for one or more critical system or service should prioritise preparation and planning activities to ensure future resilience.

Actions for now

- Profile how cloud services are integrated across the business.
- Understand how cloud services are used by third parties in the supply chain.
- Update and review business continuity plans and procedures to prepare for a cloud provider takedown.
- Review service level agreements with cloud providers.

Longer-term actions

- Ensure technical infrastructure is resilient by design.
- Identify any single points of failure related to a cloud deployment.
- Renegotiate contracts with cloud providers with a greater focus on availability and recovery.

2.3 DRONES BECOME BOTH PREDATOR AND PREY

WHAT IS THE IMPACT OF THIS THREAT?

Commercial drones will become a predator controlled by attackers to conduct targeted assaults on business. Drones will become smaller, more autonomous with increased range and equipped with cameras for prolonged surveillance missions. Flying in close proximity to operating environments, they will also be used to conduct advanced man-in-the-middle attacks, degrade mobile networks or spoof and jam other signals.

Conversely, drones will become prey as they are targeted by attackers in order to disrupt dependent businesses. Drones will be knocked out of the sky and hijacked. Information collected by drones will be stolen or manipulated in real time. Industries that leverage drones to become more efficient, such as construction, agriculture and border control, will see their drones targeted as attackers spoof and disrupt transmissions.

Weapon

An instrument of attack or defence.

In the digital cold war small commercial drones (e.g. quadcopters) will be weaponised or simply become a 'spy in the sky'. A dangerous game of cat and mouse will play out overhead.

Technological breakthroughs in drone technologies, combined with developments in 5G, big data, the IoT, and the relaxation of aviation regulations, will mean that drones will become increasingly important to operating models. Organisations will rely upon them for delivery, monitoring, imagery and law enforcement, whilst attackers will embrace drones as their new weapon of choice. The threat landscape will take to the skies.

2021

Imagine this happens… an oil company has invested heavily in a fleet of drones to monitor oil pipelines in real time. The drones record imagery and report deficiencies back to the data centre so that engineers can quickly fix any issues. However, in the early hours of the morning, local authorities report an oil spill where the pipeline had burst. Incident response recall all drones that were meant to be monitoring the pipeline and find that their signals had been jammed by an unknown attacker, distorting the true image. **Has your organisation considered how it will use drones?**

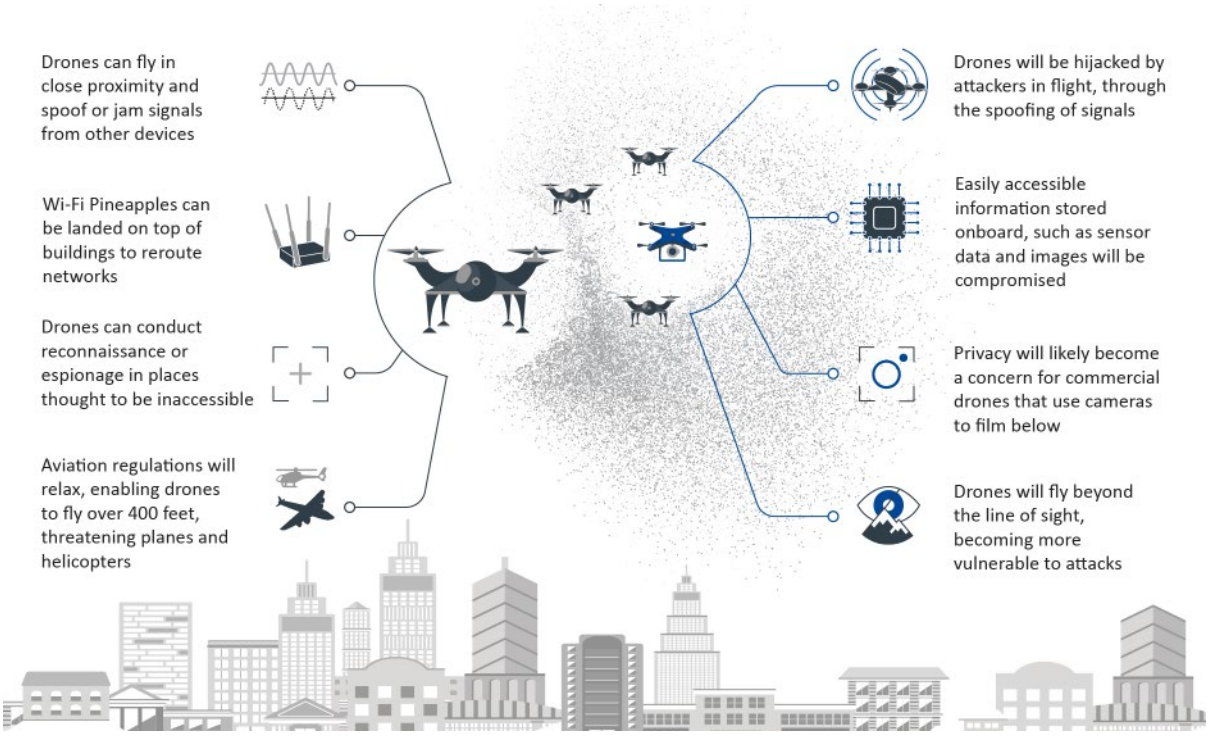
JUSTIFICATION FOR THREAT – PREDATOR

Drones used in the military for reconnaissance, targeted missile attacks and battlefield intelligence have been commonplace for years now. However, the line between military and civilian usage has somewhat blurred over the last few years as smaller, unmanned aerial vehicles or quadcopters have become more popular and commercialised. Close calls have been reported more frequently in the media with cases of assassination attempts, near fatal crashes, injuries and spying all being recorded. Moreover, two high-profile incidents of drones grounding flights at London's Gatwick and Heathrow airports took place in late December 2018 and early 2019, illustrating significant business disruption from drone activity.

"As with other dual-use technologies, the task for regulators is to encourage the good uses of drones while preventing the bad." – The Economist

Quadcopter-style drones, supposedly capable of carrying out electronic warfare and cyber attacks, are currently being developed. For example, American-Italian contractor, Selex Galileo, recently built a small drone that can interfere with communication systems such as Bluetooth or Wi-Fi and can self-destruct if captured. Septier Communications is developing a drone that can eavesdrop on mobile phone calls, intercept other mobile data or force devices on a high-security 4G network to downgrade to an older, lower quality and less secure network. If terrorist groups, hacking groups or hacktivists managed to get their hands on this technology then their armoury would be significantly enhanced.

Figure 8: Examples of how drones may become both predator and prey



JUSTIFICATION FOR THREAT – PREY

Drone-based delivery is expected to start in European countries in 2019 following the relaxation of air traffic regulations, allowing drones to fly out of sight and above 400 feet. This will revolutionise the supply chain, opening up a range of new attack vectors that hackers will undoubtedly target. According to Goldman Sachs, the forecasted market opportunity for drones will grow to $100bn by 2020, helped by growing demand from commercial and government sectors. There are over one million active drone devices currently operating in test environments in the US alone, with over 100,000 pilots registered with the FAA.

Drone usage will be particularly prominent across the agricultural, construction and oil and gas industries as business models are adapted to take advantage of drone technology. Activities such as monitoring of crop yields, airborne inspection of oil pipelines and safeguarding of construction sites will be entrusted to drones as businesses look to further automate key processes. Fire and police services will use drones to greatly enhance their capability to locate people, whether that be survivors of an incident or persons of interest. All industries that leverage this relatively immature technology will find themselves targeted as attackers aim to take advantage of drones.

Like other IoT devices, drones currently have very poor security controls, making them vulnerable to hijacking. Commercial drones will become a fresh privacy concern as they begin to store sensitive information on board. The majority will be fitted with cameras or a range of sensors, collecting information such as GPS location, credit card numbers, email addresses or physical addresses. This type of information will be a prime target for attackers over the coming years.

HOW SHOULD YOUR ORGANISATION PREPARE?

If an organisation is reliant upon drones for critical operations then diligent risk assessments need to be conducted, and controls must be implemented or upgraded to mitigate risk to the business. As drones take to the skies, organisations must become more vigilant and wary.

Actions for now

- Determine how drones are likely to be used across the business and incorporate business continuity arrangements should these drones be disrupted.
- Regularly update or patch drones.
- Apply specialised technical controls such as signal jamming, geofencing and hardening Wi-Fi.
- Protect locations from drone spying by installing blinds and curtains, mirrored windows or white noise generators.

Longer-term actions

- Lobby drone manufacturers or providers to ensure that drones have security features incorporated.
- Keep up to date with future legal and regulatory requirements, considering that they may differ or conflict across jurisdictional boundaries.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality
Integrity
Availability

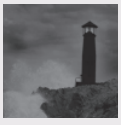
Source of threat

Adversarial
Nation state, terrorist group, hacking group, hacktivists, competitors, organised criminal group

Potential business impact

Financial
Operational
Legal and Regulatory Compliance
Reputational
Health and Safety

ISF RESOURCES


Aligning Business Continuity and Information Security


Information Security Incident Management


The 2018 Standard


IRAM2

THEME

3 DIGITAL COMPETITORS RIP UP THE RULEBOOK

Competing in the digital marketplace will become increasingly difficult, as businesses develop new strategies which challenge existing regulatory frameworks and social norms, enabling threats to grow in speed and precision. Vulnerabilities in software and applications will be frequently disclosed online with ever-decreasing time to fix them. Organisations will struggle when one or more of the big tech giants are broken up, plunging those reliant on their products and services into disarray. Organisations will rush to undertake overly ambitious digital transformations in a bid to stay relevant, leaving them less resilient and more vulnerable than ever.

3.1 DIGITAL VIGILANTES WEAPONISE VULNERABILITY DISCLOSURE

Ethical vulnerability disclosure will descend into digital vigilantism. Attackers will weaponise vulnerability disclosure to undercut organisations, destroy corporate reputations or even manipulate stock prices. Organisations will find their resources drained as digital vigilantes reduce the timelines to fix vulnerabilities and apply patches, seriously threatening operations, reputations and endangering customers.

3.2 BIG TECH BREAK UP FRACTURES BUSINESS MODELS

Calls for the break up of big technology giants will reach their peak by 2021. By then, at least one of them will be broken up, significantly disrupting the availability of the products and services they provide to dependent organisations. From email to search engines, advertising, logistics and delivery, the entire operating environment will change. Malicious actors will also prey upon vulnerable, transitioning organisations.

3.3 RUSHED DIGITAL TRANSFORMATIONS DESTROY TRUST

The demand for organisations to remain relevant in a technology-centric world will drive them to undertake rushed digital transformations. Organisations will deploy technologies such as blockchain, Artificial Intelligence (AI) and robotics, expecting them to seamlessly integrate with ageing systems. Organisations will be faced with significant disruption to services, as well as compromised data when digital transformations go wrong.

START PREPARING NOW

Due diligence will be key to competing in an increasingly turbulent digital marketplace. Basic security controls such as regular patching will play a role, as will more proactive approaches through threat intelligence, study of the regulatory environment and engagement in strategic initiatives. The demands upon the information security function will be significant; the response must be agile.

3.1 DIGITAL VIGILANTES WEAPONISE VULNERABILITY DISCLOSURE

WHAT IS THE IMPACT OF THIS THREAT?

Vulnerability disclosure will evolve from a predominantly altruistic endeavour to one that actively damages organisations. Attackers will search for, and publicly disclose, vulnerabilities to undercut competitors and destroy corporate reputations. Fraudsters will manipulate financial markets by releasing exploits at opportune moments. A lack of regulation will lead to a culture of digital vigilantism whereby vulnerability disclosure is weaponised for commercial advantage.

Organisations will be caught unaware as their vulnerabilities are disclosed at an accelerated pace, often without knowledge or consent. They will face unachievable timeframes to fix disclosed vulnerabilities, draining internal resources. The release of exploit code, the self-propagating nature of some malware and the interconnectivity of devices could see vulnerabilities exploited faster than ever before (accelerated by developments in AI) with major impacts to business.

Software providers and organisations that rely on their products will experience disruption from strategic vulnerability disclosure by rogue competitors, organised criminal groups and hacktivists. Given the global dependence on commercial software, the weaponisation of vulnerabilities will have far-reaching consequences for businesses and their customers alike.

Imagine this happens… the CISO of a gambling organisation receives an email from a key competitor, highlighting that they have discovered a 'critical vulnerability' in their mobile app. The competitor has given them ten days to fix the flaw or they will disclose the vulnerability publicly. The CISO scrambles resources to fix the vulnerability but ten days just isn't enough.
What would your organisation do in this situation?

JUSTIFICATION FOR THREAT

Currently the key players concerned with vulnerability discovery and disclosure are big tech giants, which have significant resources. Google's Project Zero and Microsoft's vulnerability discovery team are examples of well-known vulnerability disclosure programmes which actively search for vulnerabilities in their own and other companies' software.

To date, big tech giants have been able to define their own policies and practices regarding vulnerability disclosure. This enables the redefinition of policies at will, justifying the strategic disclosure of vulnerabilities that directly undermine the reputation or commercial viability of other organisations. Google, in particular, has its own disclosure guidelines for the release of vulnerabilities in third party software, disclosing them in confidence before giving 90 days to issue a patch, after which the vulnerability and exploit code are publicly released.

In 2016, Google discovered a vulnerability in Microsoft's Windows 10 operating system that allowed an attacker to break out of a sandbox environment. Google categorised the flaw as critical, and publicly disclosed the vulnerability ten days after reporting it. Microsoft criticised the disclosure and responded with the statement: "we believe in coordinated vulnerability disclosure, and today's disclosure by Google puts customers at potential risk." Figure 9 on page 30 highlights how time-consuming it is to build patches for vulnerabilities, demonstrating that ten days is an unrealistic timeframe to build, test and release a critical patch.

Figure 9: Average time taken to build patches for differing levels of vulnerability severity

In 2017 Microsoft publicly disclosed a Google Chrome web browser vulnerability, alerting Google to its discovery 30 days prior to the disclosure. The outcome of this tit-for-tat exchange was a more constructive approach to disclosure adopted by both parties. However, it does highlight the potential for vulnerability disclosure to be weaponised.

A market for vulnerability acquisition is emerging, driven by organisations such as Zerodium, which will pay millions of dollars for individual zero-day vulnerabilities. This illustrates the increasing monetary value of vulnerabilities and potentially changes the motivation for disclosure. As criminal groups or nation state actors understand the potential of zero-day vulnerabilities, unethical vulnerability disclosure will escalate, leading to more vulnerable software and associated disruption to business and endangerment of customers.

"Many software vendors find themselves in […] precarious situations. They want to secure their software, but do not want to be held at ransom, or have vulnerabilities in their products sold to zero-day brokers." – Ken Westin, Tripwire

Vulnerabilities may also be monetised in other ways, such as by manipulating the share prices of organisations. For example, in March 2018, a small security company claimed to have found vulnerabilities in AMD processors, releasing the details shortly afterwards. About 30 minutes later a financial organisation published an 'obituary' for AMD citing the recent vulnerability discovery as evidence the company was now worthless and would have to file for bankruptcy. Links between the research company and financial organisation later surfaced, showing it to be an attempt to game the stock market. Whilst these attempts to use vulnerability disclosure to short stock ultimately failed, it is just a matter of time before cases of vulnerability disclosure grow in scale and complexity.

The market for buying and selling vulnerabilities will continue to expand at an alarming rate. At the same time, AI developments will accelerate the speed at which vulnerabilities are found. Organisations will be faced with an unsustainable patching regime, and will face significant disruption and damage if vulnerabilities are exploited.

HOW SHOULD YOUR ORGANISATION PREPARE?

Dealing with zero-day vulnerabilities should be business as usual for organisations. However, as vulnerability disclosure becomes weaponised this will require re-evaluation of current approaches to patch management, threat intelligence and resilience.

Actions for now

- Review and improve processes for managing technical vulnerabilities to include vulnerability scanning, remediation and patch management systems.
- Carry out more targeted and detailed penetration testing.

Longer-term actions

- Vendors should invest in secure coding practices.
- Increase threat intelligence activities in conjunction with threat hunting to move from a reactive to a proactive stance.
- Implement a cyber resilience programme.
- Ensure that zero-day vulnerabilities are a tested scenario during a cyber security exercise.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality
Integrity
Availability

Source of threat

Adversarial
Nation state, organised criminal groups, hacking group, hacktivists, terrorists

Potential business impact

Financial
Operational
Legal and Regulatory Compliance
Reputational
Health and Safety

ISF RESOURCES


Delivering an Effective Cyber Security Exercise


Threat Intelligence: React and prepare


Application Security: Bringing order to chaos


Cyber Security Strategies: Achieving cyber resilience

3.2 BIG TECH BREAK UP FRACTURES BUSINESS MODELS

WHAT IS THE IMPACT OF THIS THREAT?

The big tech giants are currently at a crossroads. Both the public and regulators will continue to demonstrate concern that the dominance of a few big players is not healthy for either society or business. This will result in the forced break up of one or more of the big tech giants, significantly disrupting organisations that are dependent on them. Product and service offerings will be fractured and organisations will scramble to sustain operating models.

If big tech giants are forced to change, so will business. Organisations will need to find new vendors for a range of products and services, potentially having to use the services of unproven companies located in areas of the world with divergent regulatory approaches. There will be a period of significant turbulence in IT operations. Hundreds of systems will need to be replaced, with terabytes of data repatriated and thousands of contracts renegotiated, fracturing long-term IT strategies.

During this time of intense change, information security will be stretched to its limit. New and existing services will need to be assessed, as business continuity and recovery processes need to be revised and data needs to be transferred in a timely, secure manner. Meanwhile, amid this period of turbulence, malicious actors will seek out and prey on vulnerable, transitioning organisations.

Imagine this happens… a government organisation decides to use one of the big tech giants for a range of services. All of its data relating to its citizens is stored across cloud services and distributed storage platforms. Over a period of mere months this big tech provider is broken up by a regulator, fracturing all of the services it provides to the government organisation.
What would your organisation do if one of the big tech giants were broken up?

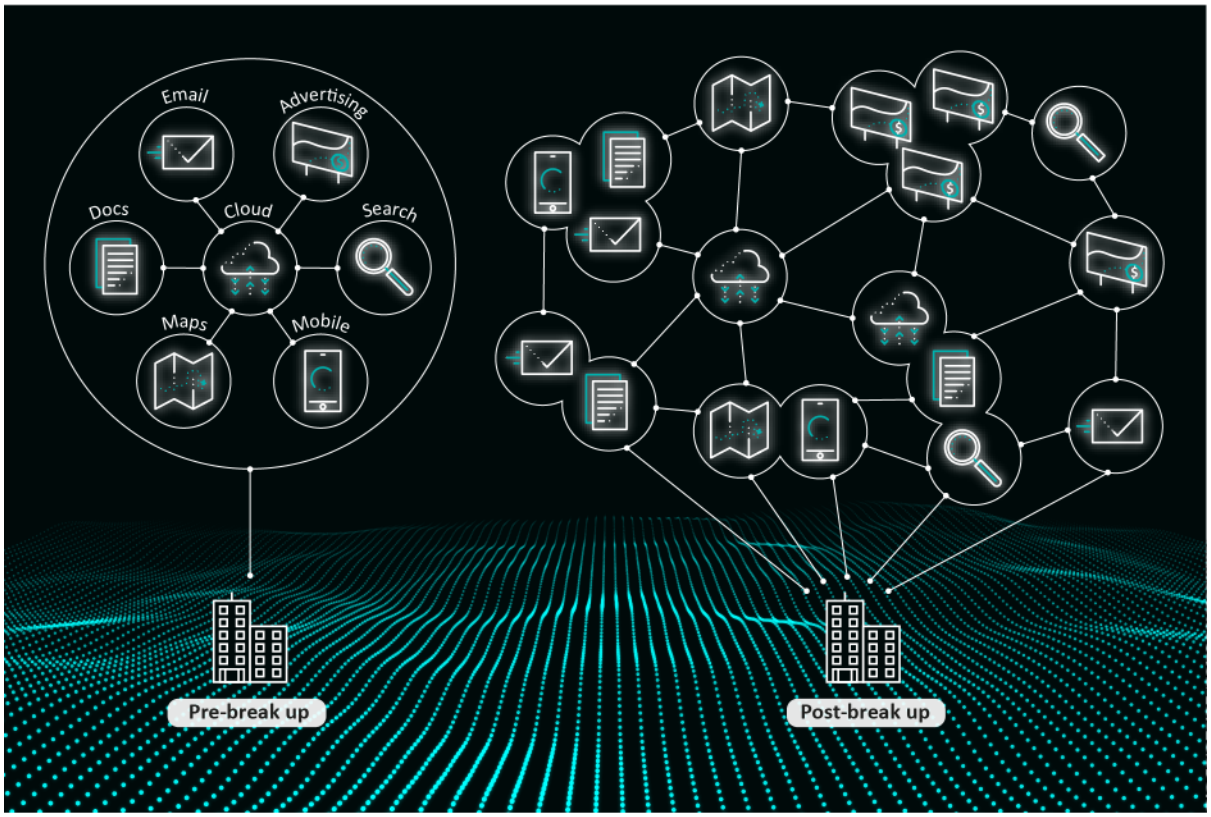
JUSTIFICATION FOR THREAT

Between them, the big tech giants – Alphabet (parent organisation of Google), Amazon, Apple, Facebook and Microsoft – are some of the most powerful companies in the world and dominate sectors such as online commerce, social media, search engines, mobile operating systems, streaming and cloud services; all areas on which organisations are dependent. In many cases, organisations are critically dependent on one or more of the big tech giants to provide their services and products. As illustrated in Figure 10 on page 33, if a break up of one of the big tech giants happens there would be significant disruption to basic services that businesses take for granted. The entire IT landscape would change, as organisations are forced to disentangle business functionality from a single ecosystem into a complex and distributed nexus of smaller providers. They would also need to fund previously free or inclusive services and retrieve and repatriate terabytes of data.

ATTRACTING UNWANTED ATTENTION

In addition to the operational disruptions (including data loss, service outages and scalability issues) that will result from a large-scale, short-notice migration to new and unproven suppliers, the global impact of a break up of one or more big tech giants will attract the attention of criminal groups. Organisations which are engaged in remediation efforts will be targeted by malicious actors. They will pose as prospective suppliers in order to gain access to strategic or restricted information, or take advantage of weakened security controls to attack and compromise large-scale data transfer programmes. For the malicious hacker or motivated criminal, the global nature of this activity, combined with an organisational urgency that leads to a lack of rigour, will constitute a golden opportunity for compromise.

Figure 10: A breakdown of services offered by big tech giants pre and post-break up



Public and government opinion of big tech firms has been negatively impacted by some high-profile scandals. In December 2018, it was reported that Facebook allowed other high-profile tech companies to access personal data on its platform by reading user messages. Facebook was also hit by the Cambridge Analytica scandal reported in early 2018, and Google was hit by a large European anti-trust fine.

"What naturally happens is you end up with one company dominating the field so […] there is no alternative to really coming in and breaking things up." – Sir Tim Berners-Lee

Calls for a break up of one or more of these big tech giants are getting louder, owing to their significant power and influence over business, politics and society, as well as their sheer dominance over industries. Many commentators draw comparison with the power and influence of Standard Oil in the early 20th Century, before it was broken up by regulators. This break up led to a period of significant turbulence for dependent businesses, as well as a reshuffling of many supply chains. The chair of America's Federal Trade Commission and the European Commissioner for Competition signalled in late 2018 that legal changes aimed at correcting market distortions were being crafted on both sides of the Atlantic, suggesting a break up of one or more of the big tech giants may be imminent.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality

Integrity

Availability

Source of threat

Adversarial

Organised criminal groups, hacking groups, individual hacker

Accidental

Regulator

Potential business impact

Financial

Operational

Legal and Regulatory Compliance

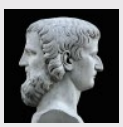
Reputational

Health and Safety

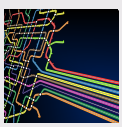
ISF RESOURCES

Information Risk Management in Outsourcing and Offshoring

Delivering an Effective Cyber Security Exercise



Threat Intelligence: React and prepare



Securing the Supply Chain

HOW SHOULD YOUR ORGANISATION PREPARE?

Organisations should evaluate overall dependencies on the big tech giants to ensure that if one of them is broken up risk can be mitigated.

Actions for now

- Understand exposure to the services of the big tech giants.
- Review IT strategies, particularly in relation to the balance between insourcing and outsourcing.
- Update resilience and business continuity in the context of a break up.
- Revise and validate exit strategies.

Longer-term actions

- Reduce dependency on single providers.
- Seek engagement in IT activities during the procurement of alternative products and services.
- Consider legal issues relating to data, which is transferred to new regions or jurisdictions.
- Increase monitoring and threat intelligence gathering activities during a period of disruption.

3.3 RUSHED DIGITAL TRANSFORMATIONS DESTROY TRUST

WHAT IS THE IMPACT OF THIS THREAT?

Organisations will rush to conduct digital transformation programmes in order to stay relevant in the marketplace – winners will dominate industries, losers will be left behind. However, as organisations race to adopt cutting-edge technology to digitise and automate, hurried and weak integration with underlying, legacy systems will lead to disastrous outcomes.

Organisations will create new applications, deploy AI and other tools (using different protocols and technology) which are expected to work seamlessly with existing and legacy systems. Consumers and dependent supply chains will lose trust in organisations that do not integrate systems and services effectively. Digital transformations will attract the attention of opportunistic attackers, who will target transitioning organisations that hold sensitive information, such as credit cards or personal details, exploiting new vulnerabilities as they are introduced.

Organisations that have built digital transformation programmes on top of legacy systems will find that they have introduced new attack vectors and exposed previously hidden vulnerabilities. They will also experience availability and supportability issues, leading to service disruption as older technologies struggle to deal with step changes in performance requirements that newer technologies demand.

Imagine this happens… a manufacturing company decides to undertake a digital transformation programme by introducing a blockchain application to manage its supply chain. Senior management learn that competitors are about to launch a similar system and move the launch date forward. On the day of release, amidst a blaze of publicity, the application fails: data is exposed and supply chains are compromised. **Does your organisation put security first during digital transformations?**

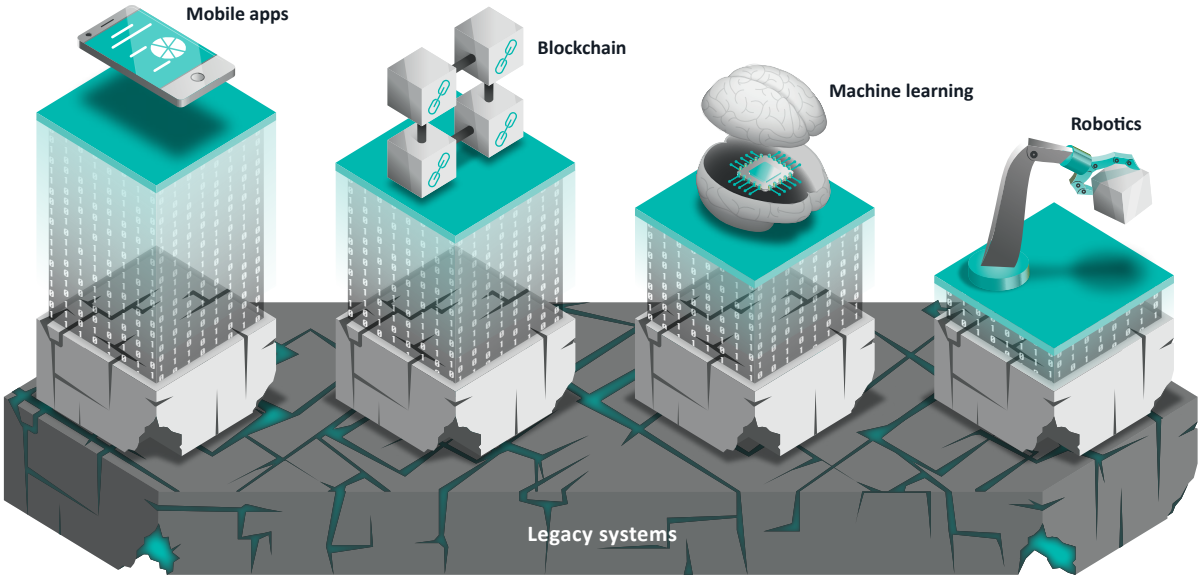
JUSTIFICATION FOR THREAT

The corporate desire to digitise and automate is significant across a range of industries. However, a survey by the Center for Digital Government found that 70% of respondents depend on legacy applications (built using COBOL, PowerBuilder, etc.) for their operations. Legacy technologies often underpin core business functions but are usually cost prohibitive to redevelop.

"The overwhelming consensus […] is that new business demands – many of them brought by forces outside the company – are putting additional pressure on organizations and technologies to deliver better ecosystem integration solutions. And when they can't, it's costing the business money." – Tushar Patel, Cleo CMO

Figure 11 on page 36 illustrates technologies that organisations may aim to implement during a digital transformation. Emerging next generation technologies such as blockchain, machine learning and robotics promise to increase efficiency and make operations more streamlined, thereby convincing organisations to undertake increasingly complex digital transformations with a range of new, immature technologies. Ill-conceived, rushed or botched digital transformations will create opportunities for compromise by exposing new or previously hidden vulnerabilities.

Figure 11: Technologies that will be implemented during digital transformations



In many cases organisations will rush to keep up with competitors, with many executives falling prey to the 'shiny object syndrome': investing in 'cool' digital technologies without a clear understanding of how they will generate sustainable value. According to a global survey from Couchbase, regarding organisations that have undertaken enterprise digital transformations, the majority of respondents agreed that the pressure to digitally transform causes companies to rush into projects too soon; with potential wasted costs reaching an average of $28m per organisation.

Digital transformations will also have a significant effect on the organisational workforce as skillsets are computerised and absorbed into the functionality of machine learning or other more automated technologies. The resultant de-skilling of the workforce will present challenges for continuity and resilience initiatives in the event of a technology outage, should organisations become entirely dependent on technology for a range of products or services.

"When you digitise and automate you lose the fundamental knowledge of how processes work. What happens when technologies fail and no one knows how to operate without them?" – ISF Member

The potential harm a botched digital transformation can cause was demonstrated by an outage at a the UK bank, TSB, in early 2018. Rushed, inadequate testing and poor internal communication led to over 1.9 million customers being unable to access their accounts, with many reports of fraud being associated with the outage. Many other large organisations have also struggled with the complexity of digital transformations, such as General Electric, which faced significant delays and technological issues during a large digital transformation programme in 2015.

It is highly likely that the hype surrounding new technologies entering the marketplace will drive business leaders to pursue ever more complex digital transformations. Rushing digital transformations will destroy consumer trust, attract the attention of opportunistic fraudsters and lead to financial and operational damage.

HOW SHOULD YOUR ORGANISATION PREPARE?

Organisations that undertake a digital transformation of any kind must carefully consider the risks that new technologies may bring, as well as how they are going to effectively integrate with legacy or underlying systems.

Actions for now

- Review whether planned digital transformation programmes have a sustainable dependency on legacy or underlying systems.
- Assess new risks introduced by a digital transformation.
- Prepare an action plan that includes regression testing.
- Ensure that fail-safe principles are built into the digital transformation programme.

Longer-term actions

- Engage with other parts of the business to ensure that the information security function is involved during the planning stage of digital transformation programmes.
- Leverage digital transformation programmes as an opportunity to champion the removal of legacy or insecure systems.

PESTLE

PESTLE factors that will drive the threat

Key information attribute affected

Confidentiality

Integrity

Availability

Source of threat

Adversarial

Organised criminal groups, hacking groups, individual hacker

Accidental

Supplier/vendor/partner, employee (privileged), customer

Potential business impact

Financial

Operational

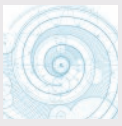
Legal and Regulatory Compliance

Reputational

Health and Safety

ISF RESOURCES

Blockchain and Security: Safety in numbers – *Briefing Paper*



Security Architecture: Navigating complexity

Embedding Security into Agile Development

IRAM2

CONCLUSION

Driven by demands for increased speed, automation and efficiency, organisations are about to face a period of significant technological upheaval as they transition into a hyperconnected digital world. Supporting this world will be new, innovative technologies and business models that will create an illusion of stability, reliability and security. However, new and re-energised threats will compromise success and shatter that illusion.

Threat Horizon 2021 has described nine threats driven by global events and major developments, that individually and collectively have the potential to cause severe disruption to an organisation's ability to conduct business.

As with any technological era, new threats will develop, and old threats will evolve. Businesses must be fully aware of the risks the new digital world will bring before jumping head first into adopting new technologies. A dependency on digital products and services will be unavoidable, but mitigations and preparations can, and must, be made.

Organisations will need to ensure that intellectual property is secured, as the next generation of technologies become a prized target for nation states. The coming years will be volatile, but the targets will be predictable. Establishing security by design, re-examining resilience and continuity arrangements, and reviewing supply chain dependencies will prepare organisations against disruption.

Digitisation promises much, and development of the next generation of technologies will bring significant benefits to business and society. To survive in the new digital world organisations will have to adapt. To thrive they will need to evolve.

Join the vibrant **Threat Horizon** community on ***ISF Live*** to share your experience and discuss the findings and recommendations presented in this report. Please engage with other Members to address these threats and develop effective strategies to protect your organisation.

FURTHER READING

Members will gain most value from this report if they question, challenge and revise the proposed threats in the context of their own organisation. A rich set of related reading is included in Appendix G, which supports the threats within the report. Members are invited to review the references used, to create their own view of ***Threat Horizon 2021***.

APPENDIX A: Methodology

Threat Horizon is the ISF's flagship publication and has been released every year for over a decade. The report predicts the top cyber security threats that will emerge over the next two to three years. The PESTLE model is used to provide context and background to these threats. Researchers draw upon material from a variety of sources. Of particular value is the structured input from Members at ISF Chapter meetings, ***ISF Annual World Congress*** and on ***ISF Live***.

APPENDIX B: Assessing predictions from Threat Horizon 2018

This appendix assesses the nine predictions made in ***Threat Horizon 2018*** now that the end of the prediction period has been reached.

The original ***Threat Horizon 2018*** predictions are summarised below and on the following pages, together with:

- a scale indicating the accuracy of the prediction
- a rating showing the degree to which the threat merits continued consideration
- supporting evidence.

Threat Horizon 2018 prediction	Supporting evidence
The IoT leaks sensitive information Organisations will adopt IoT devices with enthusiasm, not realising that these devices are often insecure by design and therefore offer many opportunities for attackers. It will be problematic for organisations to know what information is leaving their networks or what data (e.g. audio or video) is being secretly captured and transmitted. **Accuracy level:** **Ongoing threat rating:** 	Development of IoT devices continues to be rushed, with little attention paid to security, providing opportunities for criminals to exploit personal data and compromise privacy. In mid-2018 Wired magazine reported that security of Google's AI home speaker and Chromecast were deeply flawed, in some cases revealing users' locations. This threat is only set to grow. Manufacturers of consumer IoT devices are constantly adding new features that have the potential to capture sensitive information, expanding the attack surface and making these devices a more attractive target.
Opaque algorithms compromise integrity Organisations will increasingly use algorithms to operate and make decisions in critical systems. As a result, organisations will have less visibility into how their systems function and interact, and this lack of transparency will pose significant information security risks. **Accuracy level:** **Ongoing threat rating:** 	Whilst algorithms are not used extensively within every type of organisation, they are now being used in safety-critical applications, attracting significant media attention. In March 2018, an algorithm used in a Tesla vehicle was suspected to have caused a fatal crash during autopilot mode, failing to recognise a concrete lane divider as an obstacle. The lack of transparency of what the algorithm did led to disputes over liability for the incident. Algorithms will continue to be used, particularly in machine learning applications, and a deeper understanding of this threat is merited.
Rogue governments use terrorist groups to launch cyber attacks Rogue governments have already formed partnerships with terrorist groups. These partnerships will evolve to include advanced cyber capabilities (transferred to terrorist groups through government experts and technical training) and will be used to attack infrastructure or organisations worldwide. **Accuracy level:** **Ongoing threat rating:** 	There has been no evidence to suggest that terrorist groups are launching cyber attacks on behalf of governments. Whilst this tactic would give governments plausible deniability, the unpredictability and uncertain allegiance of terrorist groups makes this type of alliance an unlikely one. Given the lack of evidence, this threat is less likely to materialise in its original form and it is more likely that governments will use either in-house expertise or organised criminal groups.

Threat Horizon 2018 prediction	Supporting evidence
Unmet board expectations exposed by a major incident Boards will expect that their approval of increased information security budgets will have enabled the CISO and the information security function to produce immediate results. Misalignment between a board's expectations and the reality of the security function's ability will cause the organisation substantial harm, with repercussions also reflecting badly on the individual and collective reputations of the board members. **Accuracy level:** **Ongoing threat rating:** 	Whilst there has been a number of high-profile security incidents, there is little publicly available evidence proving a direct link between investment in information security and results. A report by Forbes in 2018 suggested that most CISOs struggle to push information security higher up the company's business agenda, with many organisations still not prioritising sufficient investment. Despite the lack of evidence, this threat will remain a board-level concern, and alignment between expectations and results should improve with a better understanding of information risk in the context of wider enterprise risk.
Researchers silenced to hide security vulnerabilities As software replaces hardware across all major sectors, security researchers will regularly uncover vulnerabilities and make them public in an effort to improve security for everyone. In response, many manufacturers will threaten researchers with legal action instead of working with them to fix the vulnerabilities, which will be left in place for months or even years, leaving organisations open to attack from malicious actors. **Accuracy level:** **Ongoing threat rating:** 	The threat of legal action for disclosure of vulnerabilities has been particularly prevalent throughout 2017 and 2018 – however this hasn't stopped researchers from disclosing them anyway. In late December 2017, a Google security researcher found and publicly disclosed a vulnerability in Keeper, a password manager provider. However, Keeper actually filed a lawsuit against the journalist who reported the vulnerability (rather than the researcher) for 'defamation of character'. Additionally, fear of legal action led a researcher to publicly disclose an Oracle vulnerability rather than approaching the company. The legal threat to individual researchers remains. However, as discussed in *Threat 3.1: Digital vigilantes weaponise vulnerability disclosure*, the majority of vulnerability discovery will be undertaken by larger organisations, which will be less susceptible to legal action.
Cyber insurance safety net is pulled away Several large data breaches will result in insurance companies suffering significant financial losses as a result of mispricing risk. This sudden shock will swiftly drive many insurers out of the cyber insurance market and force the surviving insurers to take action. These actions will disrupt a primary method for transferring cyber risk, upon which many organisations have become dependent. **Accuracy level:** **Ongoing threat rating:** 	As cyber criminals make bolder attacks and organisations struggle to defend themselves, demand for cyber security insurance is expected to grow. According to Orbis Research, the cyber security insurance market is expected to reach $17.55bn in 2023, up from $4.52bn in 2017. Significant cyber insurance disputes have emerged, such as that between Mondelēz International (which was hit by the NotPetya attack in 2017) and the insurance company Zurich. Mondelēz's claim was disputed by their insurer, which stated that the NotPetya attack should be classified as an act of war and was therefore exempt from the policy. Disputes of this nature are likely to continue well into 2019 and beyond, highlighting significant discrepancies as to what cyber insurance actually is – and if it is worth paying for.

Threat Horizon 2018 prediction	Supporting evidence
Disruptive companies provoke governments Aggressive commercial strategies (by companies that are disrupting their sector, such as Uber, Airbnb and Alphabet) will prompt politicians and regulators around the world to take a closer interest in the domestic impact of new technologies. Under pressure to react, poorly conceived government policies and regulations that neither encourage economic growth nor increase data protection for their citizens will be adopted. **Accuracy level:** **Ongoing threat rating:** 	Governments have realised that existing laws and regulations governing technology are inadequate as big tech companies begin to dominate markets. Some governments have pursued legal actions, fines and bans to penalise these companies in recent years, with the descriptive term 'techlash' becoming common. In late 2018, the Australian government passed controversial legislation allowing the country's intelligence agencies to access to end-to-end encrypted digital communications through backdoors. The dilemma between balancing privacy rights and law enforcement capability is being debated across the world. Poorly conceived legislative attempts to redress the balance will only serve to amplify this threat.
Regulations fragment the cloud Regulatory and legislative changes will impose new restrictions on how personal data is collected, stored, exchanged and disposed of. Organisations will be presented with an unmanageable tension of trying to remain compliant with new data protection and data localisation requirements while continuing to conduct business as usual. **Accuracy level:** **Ongoing threat rating:** 	Cloud providers have responded to this threat by developing specific products and services (e.g. regional cloud offerings) that mitigate the risk of non-compliance. A report from the World Business Council for Sustainable Development has recommended that financial, legal, technological and political barriers must be removed to ensure that legislation can support innovative business models, owing to the fear that a range of services that cross international borders may be affected (such as the cloud). As discussed in *Threat 2.2: Sabotaged cloud services freeze operations*, the threats to the cloud will come from malicious actors rather than regulators.
Criminal capabilities expand gaps in international policing The technical capabilities and reach of cyber criminals are now level with those of governments and organisations. By 2018, these capabilities will extend far beyond those of their victims. As a result, the ability of current control mechanisms and international policing to protect organisations is likely to diminish, exposing these organisations to greater impact. **Accuracy level:** **Ongoing threat rating:** 	Police forces around the world lack the fundamental skills and resources to counter the increasing capability of cyber criminals as evidenced by the significant activity of cyber crime and confusion over jurisdictional responsibility. In November 2018, Interpol reported that criminals operating on the dark web and underground economy have created new challenges for law enforcement, which is also struggling to recruit and retain personnel with the right skill sets to investigate cybercrime. This threat will become an increasing concern for businesses, governments and citizens.

APPENDIX C: Assessing predictions from Threat Horizon 2019

This appendix examines the nine threats identified in ***Threat Horizon 2019***, presenting the ISF's level of confidence in each individual prediction coming true.

The original 2019 predictions are summarised below and on the following pages, together with the level of confidence in the threat materialising and supporting evidence for the confidence rating.

These threats should be assessed and prioritised to reflect an organisation's specific circumstances.

Threat Horizon 2019 prediction	Supporting evidence
Premeditated internet outages bring trade to its knees In an environment of fractured international relations, core internet infrastructure will become a target as nation states and terrorist groups aim to inflict widespread economic damage on their adversaries. **Confidence level:**	Whilst relatively small-scale examples of this threat have been seen (e.g. the US reportedly temporarily disabled North Korea's internet in September 2017), there has not yet been a sustained or significant outage. However, rising political tensions indicate that the threat is still relevant and targeted attacks are likely. Confidence in this threat remains high and this was supported by a statement from the head of the British military in December 2017, warning that adversaries could catastrophically impact the economy by cutting undersea fibre optic cables.
Ransomware hijacks the Internet of Things Already one of the most prevalent ways to exploit the value that organisations place on digital information, ransomware will evolve to target connected smart physical devices, potentially putting lives in danger. **Confidence level:**	This threat has yet to materialise. Whilst the number of IoT devices continues to proliferate, and vulnerabilities continue to be found, the challenge of how to actually issue a ransom to the owner of an IoT devices still remains. The number of IoT devices is predicted to grow from over 23 billion in 2018, to over 30 billion by 2020 and F-Secure sees few improvements to their security. Attacks on IoT devices increased by 600% between 2016 and 2017, but were primarily focused on co-opting devices into botnets rather than holding them to ransom. However, the possibility remains that attackers will develop techniques for successful ransomware deployment on the IoT.
Privileged insiders coerced into giving up the crown jewels 'Soft' human targets, with access to mission-critical information, will be subjected to various old-fashioned criminal techniques of coercion. **Confidence level:**	A report by Wombat Security highlights that 48% of organisations experienced a rise in phishing in 2018, 17% of which were successful, however there was no evidence that privileged users were targeted specifically. Although such attacks are mainly phishing emails, these could be leveraged by attackers to blackmail victims into giving up crown jewels. Whilst social-engineering attacks on employees with privileged access rights, such as system administrators, remains a possibility, the confidence in this threat is reduced.

Threat Horizon 2019 prediction	Supporting evidence
Automated misinformation gains instant credibility The practice of deliberately spreading misinformation will evolve to target commercial organisations, driven by advances in artificially intelligent personas (AI chatbots). **Confidence level:**	AI chatbots have not developed as fast as initially predicted, with no notable AI persona yet passing the Turing test. Additionally, regulatory pressure against the big social media companies is resulting in significant effort in removing existing chatbots and reducing misinformation (or 'fake news') following the backlash from supposed election meddling. News organisations are also actively challenging misinformation from political figures to help mitigate the impact of chatbots in social media echo chambers. It remains possible that, by the end of 2019, sophisticated AI chatbots may be created and deployed but the combination of technology and regulatory pressures has reduced the confidence in this threat.
Falsified information compromises performance Attacks that compromise the integrity of an organisation's internal information will increase in number, scale and complexity. The tactic of leaking distorted information will become prevalent, with attackers aiming to use misinformation to damage reputations and disrupt operations. **Confidence level:**	By its very nature this type of attack would leave little evidence in the short term, especially if conducted by competent actors. It would also require significant investment to be successful. Other types of attack, such as theft of IP, ransomware or cryptojacking can achieve similar outcomes for a reduced cost, and hence these other types of attack are expected to dominate. The upward trend in cloud adoption (up 15% from 2017 and forecast to grow by 17.3% in 2019) may also help to mitigate this threat by raising the barrier for successful attacks, through increased integrity checking and imposing strict privileged access control. Consequently, confidence in this threat is reduced.
Subverted blockchains shatter trust Blockchains will be subverted to commit fraud or launder money, shattering the trust on which they rely. This could result in abandoning the affected blockchain, along with the loss of process efficiencies. **Confidence level:**	Slow uptake of non-cryptocurrency related blockchains across a range of sectors has meant that the opportunity to subvert them has been minimal. Concerns about possible fraud or subversion has also led many organisations to reject the use of blockchain. For example, the Australian government rejected the use of blockchain in October 2017 following a 6 month review of the technology. The Register also found that none of 43 blockchain projects assessed in November 2018 had been found to be 'worthwhile', causing earlier advocates to disavow blockchains' use. However, if non-cryptocurrency related blockchain does become more popular across a range of industries, the threat of subversion will remain and the confidence level in this threat will increase.
Surveillance laws expose corporate secrets Organisations will not be able to define the security arrangements around reservoirs of data collected in bulk by communications providers. Attackers will exploit this. **Confidence level:**	Surveillance legislation remains broadly unchanged from 2017 around the world, despite legal challenges. Regulations such as the UK's Investigatory Powers Act 2016 still require Internet Service Providers and telecommunication companies to store communications metadata (such as call details, rather than conversations) on all transmissions passing through their network. Although telecommunication companies continue to be targeted, no evidence has been found that this type of information has become a specific target, and the confidence level in this threat is relatively low.

Threat Horizon 2019 prediction	Supporting evidence
Privacy regulations impede the monitoring of insider threats Restrictions on individual profiling will result in a conundrum for the organisation: either lose the ability to monitor the insider threat; or defy regulations. Both will have negative consequences. **Confidence level:**	The GDPR legislation may limit some organisations' ability to monitor insider threats, but businesses may still track activity, provided it is proportionate and for a legitimate business interest. As per a late 2017 ruling by the European Convention on Human Rights, companies must have policies clearly informing employees when and how they could be monitored. The monitoring must also be neither covert nor overly intrusive. Whilst legal challenges are still possible, such as defining when communications sent from a company device are personal or those of the business, the monitoring activity is likely to continue, reflected in a low confidence level for this threat.
A headlong rush to deploy AI leads to unexpected outcomes The use of AI will produce outcomes that go beyond the understanding of business leaders, developers and system managers, creating new vulnerabilities. **Confidence level:**	Development of AI continues to grow and speculation about its benefits gather significant hype and expectation across the media. However, organisations are reluctant to adopt such an immature technology, in the light of examples such as the International Space Station's automated assistant CIMON, which was deactivated in November 2018 after errors appeared when it first interacted with astronauts. Some businesses recognise AI's limitations. However, as outlined in *Threat 3.3: Rushed digital transformations destroy trust*, this threat may come to fruition by 2021.

APPENDIX D: Assessing predictions from Threat Horizon 2020

This appendix examines the nine threats identified in ***Threat Horizon 2020***, presenting the ISF's level of confidence in each individual prediction coming true.

The original ***Threat Horizon 2020*** predictions are summarised below and on the following pages, together with the level of confidence in the threat materialising and supporting evidence for the confidence rating.

These threats should be assessed and prioritised to reflect an organisation's specific circumstances.

Threat Horizon 2020 prediction	Supporting evidence
Cyber and physical attacks combine to shatter business resilience Attackers will combine physical and cyber weapons to cause widespread damage or chaos. Organisations will be unable to operate during these disastrous circumstances. **Confidence level:**	Whilst targeted attacks on cities have not yet taken place, tensions continue to rise between the East and the West, with militaries training to take down CNI, and watering-hole attacks attempting to reach ICS being developed. Physical terrorist attacks continue to proliferate throughout the world. As terrorist groups expand their cyber capabilities, the prospect of hybrid attacks on cities will become more likely.
Satellites cause chaos on the ground Compromised satellite signals will cause widespread chaos down on earth, as global positioning systems (GPS) signals are spoofed or jammed, affecting global trade, communications and other operational functions. **Confidence level:**	There has been cases of nation states targeting satellites throughout 2018, but few causing significant damage on the ground. In June 2018, US warships had their GPS hacked and in September 2018 France accused Russia of spying on its satellite communications. Technology which is beginning trials in 2020 to repair satellites and clear orbital debris in space could just as easily be utilised to compromise signals by redirecting or destroying other satellites. Although government support for international security standards to secure satellites, is growing, the threat should continue to be monitored.
Weaponised appliances leave organisations powerless Enemies aiming to inflict damage will take advantage of homogeneous vulnerabilities across a range of connected appliances, creating power surges strong enough to knock out regional power grids. **Confidence level:**	The number of IoT devices is predicted to grow from over 23 billion in 2018 to over 30 billion by 2020, with the uptake of connected home appliances growing substantially across the world. Numerous commentators report no sign of IoT security improvements, which, combined with reports of electrical grids being probed significantly by attackers throughout 2018, indicates that the threat remains potent.

Threat Horizon 2020 prediction	Supporting evidence
Quantum arms race undermines the digital economy The emergence of quantum computing will herald a step change in processing power, shifting perceptions about what computers can achieve. However, the increase in performance will enable those who develop or acquire the technology to break current encryption standards. With a fundamental security mechanism rendered obsolete, information and transactions of all kinds will suddenly become vulnerable. **Confidence level:**	Development of universal quantum computers is progressing, but slower than anticipated. Whilst one major manufacturer has announced a product offering the levels of Qbit interactivity currently achieved are not yet sustainable enough for computations to take place at the required speeds to outperform existing computers. The US National Academies of Sciences, Engineering, and Medicine estimate that an operational universal quantum computer will exist by 2030. Efforts are already underway to create quantum-proof cryptography, with the automobile sector being particularly active. Some commentators propose that widespread implementation of quantum-proof cryptography will take at least 20 years to develop, suggesting that a quantum computer is likely to be built before suitable encryption standards are in place.
Artificially intelligent malware amplifies attackers' capabilities Attackers will take advantage of breakthroughs in AI to develop malware that can learn from its surrounding environment and adapt to discover new vulnerabilities, exposing information including mission-critical information assets and causing financial, operational and reputational damage. **Confidence level:**	Given the increasing availability and development of machine learning, and advances in malware automation, the threat of artificially intelligent malware looms. In the first half of 2018 IBM's Deeplocker researchers successfully integrated malware with AI, to enhance its functions. Having now established the proof of concept, it is very likely that developments of artificially intelligent malware will be on the horizon over the next couple of years.
Attacks on connected vehicles put the brakes on operations By hacking connected systems in vehicles, attackers will cause accidents that threaten human life and disrupt supply chains – not to mention impacting the reputation and revenue of vehicle manufacturers. **Confidence level:**	Automobile manufacturers are taking the threat seriously, issuing bug-bounties, creating car-in-a-box pen-testing kits and establishing the Automotive Information Sharing and Analysis Centre (Auto-ISAC) to develop and disseminate good practice. However, software vulnerabilities are common, and as vehicles become increasingly connected to the internet (e.g. with the first truly driverless trucks coming to Swedish roads in early 2019) opportunities for attackers will grow.
Biometrics offer a false sense of security Biometric authentication methods will frequently be compromised by attackers who learn to find increasingly sophisticated ways to overcome them, compromising sensitive data in the process. **Confidence level:**	Use of biometric authentication is on the increase, with NuData Security reporting that GDPR is a significant driver for adoption. Although biometrics are improving, new exploits continue to be found. Coupled with an over-reliance on biometrics as the sole layer of authentication on consumer devices and applications, exploits are already appearing. The ubiquity of the mobile phone and the popularity of biometrics results in a high confidence level in this threat.

Threat Horizon 2020 prediction	Supporting evidence
New regulations increase the risk and compliance burden Organisations will wrestle with an incredibly burdensome risk environment, with complex, conflicting and confusing regulatory demands overwhelming existing compliance mechanisms. **Confidence level:**	FTSE 350 companies spent over $1bn in preparation for the GDPR, and Fortune 500 companies spent $8bn. Some media organisations operating in the US preferred to withdraw from the European market rather than deal with the complexity of regulatory requirements. Further regulation (such as the California's Consumer Privacy Act 2018) will increase the penalties for data breaches. The risk and compliance burden is only set to grow further, and therefore confidence in this threat is high.
Trusted professionals divulge operational weak points Increasing pressure on trusted professionals will lead some to divulge their organisation's weak points. Financial temptation, coercion and simple trickery will combine with reduced employee loyalty – taking the insider threat to a new dimension. **Confidence level:**	The definition of 'trusted professionals' seems to be blurring. CyberArk's 2018 Global Advanced Threat Landscape Report highlights that the percentage of employees with administrator rights on their devices has jumped from 62% in 2016 to 87% in 2018, meaning that more people than ever have access to sensitive information. The resurgence and sophistication in phishing attacks, combined with the continued financial incentives, the threat posed by the malicious or coerced insider is on the rise.

APPENDIX E: ISF Threat Radar

The ISF Threat Radar (the Radar) is a visual aid created to accompany ***Threat Horizon*** reports.

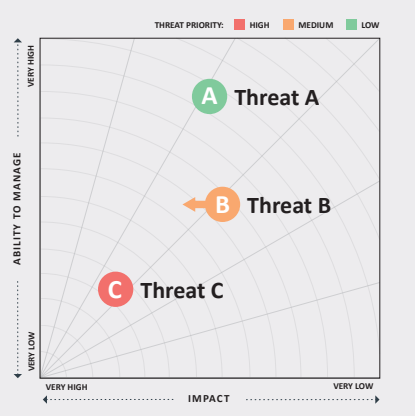
The Radar (see Figure 12) is designed to help:

- record relevant future threats to information presented in ***Threat Horizon*** reports or that are identified as specific to the organisation
- assess the potential impact of these threats
- determine the organisation's ability to manage these threats
- prioritise plans and investment needed to remediate threats.

Each threat is shown as a red, amber or green circle denoting the priority the threat has been assigned. The closer a threat is to the bottom left of the Radar, the more attention it merits.

The Radar is dynamic, using arrows to highlight anticipated changes to impact or ability to manage threats.

Figure 12: The ISF Threat Radar



The Radar is not a traditional risk matrix or heatmap and should therefore not be treated as such: it does not consider likelihood, probability or frequency.

A customisable, interactive Microsoft PowerPoint version of the Radar can be found in the **Threat Horizon** community on ***ISF Live***.

USING THE RADAR IN PRACTICE

To populate the Radar, information security and risk specialists should:

- review threats in ***Threat Horizon*** reports and determine their applicability to the organisation
- identify additional threats that are specific to the organisation
- assess the potential impact of each threat to the organisation and its ability to manage them
- plot these threats on the Radar, adding colours and arrows as required.

Once populated, the completed Radar can be used to:

- brainstorm factors that might affect threats over time with IT and business representatives
- explain the threats to business leaders
- workshop the threat placements with business leaders to gain buy-in
- determine how threats can be addressed
- create remediation plans.

The Radar can facilitate engagement with the board, offering a way to visualise the extent of impending threats to the organisation and to identify areas that require investment or further development to support the business in the future.

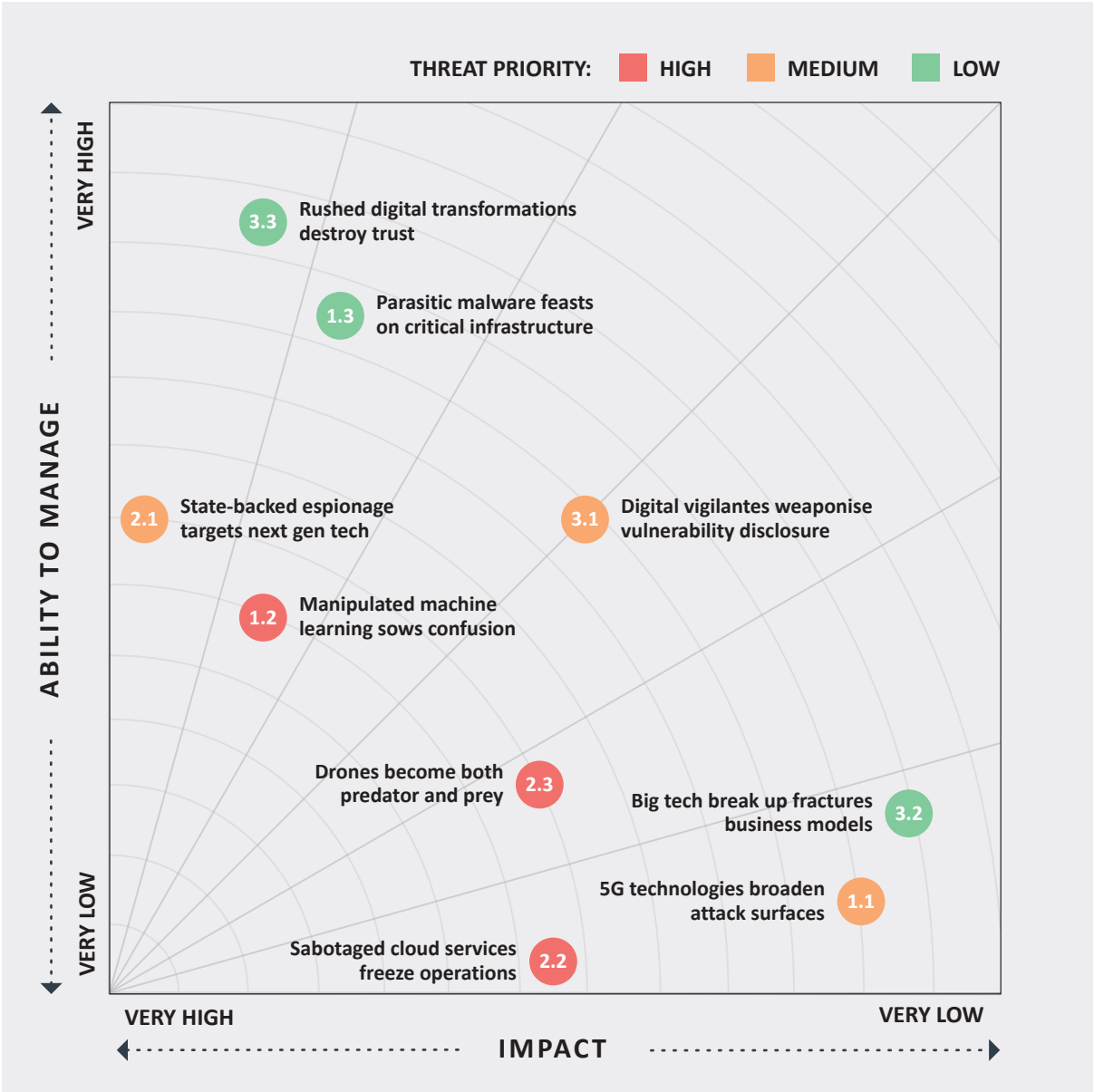
AN EXAMPLE RADAR

An example of how a fictitious organisation might assess the nine threats in this report, and plot them on the Radar, is presented below and on the following page.

In this example, the organisation is a farm vehicle designer and manufacturer. It is also a dominant player in the Agritech industry and aspires to be a market leader in terms of innovation, with aims to revolutionise the vertical farming industry. It relies on cutting-edge technological solutions, such as machine learning, drones and always-connected machinery, to maintain its dominant position in the industry. Machinery is manufactured and assembled in 20 plants of varying size across ten different countries including the US, UK and throughout mainland Europe, with a mixture of operational and information technology at each location.

How the fictitious organisation has plotted the nine threats in this report on the Radar is illustrated in Figure 13, with its reasoning presented on page 51.

Figure 13: Example ISF Threat Radar



1.1 5G technologies broaden attack surfaces

Impact: **Very Low** | Ability to manage: **Very Low**

The agriculture machinery we make uses mobile networks to transfer data for analysis. We have no control over the underlying technology, therefore our ability to manage any related threat is very low. The data we collect enriches the services we offer. A loss of connectivity could result in damage to our reputation, together with minor financial impacts.

1.2 Manipulated machine learning sows confusion

Impact: **High** | Ability to manage: **Medium**

Our hyper spectral imaging systems feed and utilise proprietary machine learning algorithms to spot crop diseases. If manipulated, our customers' crops could be seriously impacted and hence our reputation damaged. Our algorithms are proprietary, so we maintain a level of control. However, customer drones remain connected to our servers, and once sold we have limited control over them.

1.3 Parasitic malware feasts on critical infrastructure

Impact: **High** | Ability to manage: **High**

We have a fast growing vertical farming division for optimised crop production indoors. This has a high-power consumption providing an environment for this type of malware, so we monitor overall power usage. An infection could compromise the entire environment resulting in ruined crops and loss of revenue.

2.1 State-backed espionage targets next gen tech

Impact: **Very High** | Ability to manage: **Medium**

Our research and developments place us in the top 5% of crop growers worldwide for quality and productivity. We consider the IP generated from R&D our most prized asset and a target for nation states or competitors. We are comfortable with our ability to protect these assets, but any theft of them could see serious impacts to our revenue and future financial viability.

2.2 Sabotaged cloud services freeze operations

Impact: **Medium** | Ability to manage: **Very Low**

A cloud outage would impact our data analysis and collection capabilities used to maximise agricultural machinery use and create optimal environments for our indoor crops. With no analytical capability, our vertical farming and customers would suffer. Beyond service level agreements we have limited control over cloud infrastructure and no alternative plans.

2.3 Drones become both predator and prey

Impact: **Medium** | Ability to manage: **Low**

Our hyper spectral imaging system is deployed using drones. Each drone is connected to our control centre so remote patching is possible. If our drones were targeted with malware this could affect our reputation, but physical attacks would be out of our control with very little impact.

3.1 Digital vigilantes weaponise vulnerability disclosure

Impact: **Medium** | Ability to manage: **Medium**

Much of our operational technology uses proprietary software so vulnerability disclosure is not a big threat. Were vulnerabilities discovered the operational effectiveness of our machinery would be impacted. Our internal systems use standard vendor software more susceptible to vulnerability disclosures and an element of concern for this threat remains.

3.2 Big tech break up fractures business models

Impact: **Very Low** | Ability to manage: **Low**

Whilst technology plays a large part in our business, we are not overly reliant on services associated with big tech, other than our cloud offering discussed elsewhere. We don't hold lots of personal information but do have lots of operational data associated with our machinery. Like others, any changes to regulations could have an impact on us.

3.3 Rushed digital transformations destroy trust

Impact: **High** | Ability to manage: **Very High**

Due to the nature of our business we are under serious pressure to keep pace with technological advancements. We have just completed a digital transformation project, which overall was very successful. Had it not been successful the impacts would have been high as we rely on technology for a lot of our processes, but we feel we have control over any transformation programme we undertake due to the collaboration between business functions.

APPENDIX F: Making the most of Threat Horizon 2021

This appendix provides three suggested steps for using ***Threat Horizon 2021*** and previous ***Threat Horizon*** reports to help protect the organisation against future threats.

Threat Horizon helps senior business leaders to:

- understand possible future threats to information
- assess the potential financial, operational, legal and regulatory, reputational and health and safety impacts on the organisation
- coordinate responses across various business functions affected by the threats.

Threat Horizon helps security leaders to:

- discuss and report information risk with the board
- define information security strategy and set budgets
- build a secure IT infrastructure
- influence research and development of new products or services, transformation programmes or M&A plans.

THREE STEPS FOR MAKING THE MOST OF THREAT HORIZON 2021

Each of these three steps is presented together with specific actions to consider, parties who may need to be involved, and ISF reports or tools that may provide value.

☑ STEP 1

Validate the predictions in ***Threat Horizon 2021*** in the context of the organisation

Actions to consider

- Share the ***Threat Horizon 2021*** report (as well as the separate Executive Summary) with relevant parties across the organisation.
- Become familiar with 'The World in 2021' forecast, nine threats and ISF Threat Radar. Each threat should be considered both individually and in combination with others.
- Discuss the potential impact of each threat on the organisation, and the organisation's ability to manage them.

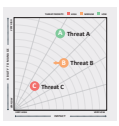
Parties to involve

CISO, information risk management team, IT managers, senior business leaders/business representatives

Related ISF reports and tools

IRAM2

Threat Horizon 2020 and previous Threat Horizon reports



ISF Threat Radar

ICS Threat Reference Guide

☑ STEP 2

Create a list of future threats that are specific to the organisation

Actions to consider

- Gather relevant parties to review findings from Step 1 and tailor ***Threat Horizon 2021*** (and other ***Threat Horizon*** reports) for the organisation. This may involve developing, adapting, modifying or removing threats.
- Rank all threats, including those that have been modified or not covered at all in ***Threat Horizon*** reports, leveraging the organisation's existing risk management tools and methodologies.
- Use the ISF Threat Radar as a visualiser to present the customised threat list in a clear and compelling manner.
- Present the customised list of threats to board members in order to shape decisions over remediation plans.

Parties to involve

Risk committee, senior business leaders, board members, CISO, IT managers

Related ISF reports and tools


IRAM2


Threat Horizon 2020 and previous Threat Horizon reports


Threat Intelligence: React and Prepare

ISF Threat Radar


ICS Threat Reference Guide

☑ STEP 3

Develop and implement remediation plans

Actions to consider

- Prepare to address emerging threats, for example by:
  - updating the organisation's information security strategy
  - collaborating across the organisation to rethink and rehearse business continuity and disaster recovery plans
  - identifying changes required to critical systems.
- Create plans to remediate each threat, assigning responsibilities to named individuals and setting target dates for specific actions.
- Align actions with the organisation's information risk management approaches, structures and frameworks.

Parties to involve

Risk committee, senior business leaders, CISO, IT managers

Related ISF reports and tools


Delivering an Effective Cyber Security Exercise


The Standard of Good Practice for Information Security 2018


Protecting the Crown Jewels: How to secure mission-critical information assets


IRAM2


Industrial Control Systems: Securing the systems that control physical environments


Aligning information risk management with operational risk management – *Briefing Paper*

APPENDIX G: References

This appendix lists sources that readers may find useful for further research around each section of the report.

These references are accurate and available as of the date of publication.

The World in 2021

Political

The Associate Press, "Putin's Russia: From basket case to resurgent superpower", *WTOP*, 12 March 2018, https://wtop.com/world/2018/03/putins-russia-from-basket-case-to-resurgent-superpower/slide/1/

N. Barkin, "China's vice premier says no country can win a trade war", *Reuters*, 27 November 2018, https://www.reuters.com/article/us-china-europe-liu/chinas-vice-premier-says-no-country-can-win-a-trade-war-idUSKCN1NW1HH

The Guardian, "The Observer view on Brexit and the future of Europe", 25 November 2018, https://www.theguardian.com/commentisfree/2018/nov/25/brexit-britain-europe-also-fractured

Y. Noah Hurari, "21 Lessons for the 21st Century", *Penguin*, 2018

K. Rapoza, "China thinks it's an emerging market. It doesn't look like one", *Forbes*, 29 November 2018, https://www.forbes.com/sites/kenrapoza/2018/11/29/china-thinks-its-an-emerging-market-it-doesnt-look-like-one/#220bd3869572

M. Wood, "Does big tech have more influence on the economy than the president", *Market Place*, 17 October 2018, https://www.marketplace.org/2018/10/16/tech/does-big-tech-have-more-influence-economy-president

Economic

S. Kennedy, "Made in China 2025", *CSIS*, 01 June 2015, https://www.csis.org/analysis/made-china-2025

D. Pollock, "The fourth industrial revolution built on blockchain and advanced with AI", *Forbes*, 30 November 2018, https://www.forbes.com/sites/darrynpollock/2018/11/30/the-fourth-industrial-revolution-built-on-blockchain-and-advanced-with-ai/

A. Yao, "The worsening US-China trade war might cost the world much more than US$430 billion of lost GDP", *South China Morning Post*, 27 September 2018, https://www.scmp.com/comment/insight-opinion/united-states/article/2165755/worsening-us-china-trade-war-might-cost-world

Social

J. Anderson, L. Raini, "The future of well-being in a tech-saturated world", *Pew Research Center*, 17 April 2018, http://www.pewinternet.org/2018/04/17/the-future-of-well-being-in-a-tech-saturated-world/

K. Hart, D. McCabe, M. Allen, "Google CEO: Big tech scrutiny is 'here to stay'", *Axios*, 12 December 2018, https://www.axios.com/google-sundar-pichai-interview-big-tech-scrutiny-40d655a7-25f2-4414-b8fb-ac4f65ab62e4.html

J. Kolko, "5 questions we should be asking about automation and jobs", *Harvard Business Review*, 19 December 2018, https://hbr.org/2018/12/5-questions-we-should-be-asking-about-automation-and-jobs

T. Marshall, "Divided: Why we are living in an age of walls", *Elliott & Thompson Limited*, 2018

Y. Noah Hurari, "21 Lessons for the 21st Century", *Penguin*, 2018

Technological

5G Americas, "Global forecast 2023: 10 billion mobile connections including 1.3 billion 5G connections", 19 December 2018, https://globenewswire.com/news-release/2018/12/19/1669806/0/en/Global-Forecast-2023-10-Billion-Mobile-Connections-Including-1-3-Billion-5G-Connections.html

European Commission, "Quantum technologies flapgship kicks off with first 20 projects", 29 October 2018, https://ec.europa.eu/digital-single-market/en/news/quantum-technologies-flagship-kicks-first-20-projects

J. Mullen, "China won't back down in its plan to dominate tech", *CNN Business*, 18 December 2018, https://edition.cnn.com/2018/12/17/tech/china-tech-us-future/index.html

J. Naughton, "'The goal is to automate us': welcome to the age of surveillance capitalism", *The Guardian*, 20 January 2019, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

Legal

C. Isidore, J. Sarlin, "Big tech is way too big", *CNN Business*, 17 December 2018, https://edition.cnn.com/2018/12/17/tech/big-tech-too-big-tim-wu/index.html

T. Mullahy, "A new era of privacy – why regulations like the GDPR are actually a good thing for your business", *CPO Magazine*, 16 January 2019, https://www.cpomagazine.com/data-protection/a-new-era-of-privacy-why-regulations-like-the-gdpr-are-actually-a-good-thing-for-your-business/

Environmental

T. Batchelor, "China and Russia's climate plans could push global temperature rises above 5C, new study warns", *Independent*, 16 November 2018, https://www.independent.co.uk/environment/climate-change-temperature-paris-agreement-environment-china-russia-report-a8637546.html

C. Felter, "The cobalt boom", *Council on Foreign Relations*, 15 June 2018, https://www.cfr.org/backgrounder/cobalt-boom

Theme 1: Digital connectivity exposes hidden dangers

1.1 5G technologies broaden attack surfaces

R. Cheng, "Not just speed: 7 incredible things you can do with 5G", *CNET*, 02 March 2017, https://www.cnet.com/news/5g-not-just-speed-fifth-generation-wireless-tech-lets-you-do-vr-self-driving-cars-drones-remote/

J. Chin, S. Krouse, D. Strumpf, "The 5G race: China and U.S. battle to control world's fastest wireless internet", *Wall Street Journal*, 09 September 2018, https://www.wsj.com/articles/the-5g-race-china-and-u-s-battle-to-control-worlds-fastest-wireless-internet-1536516373

ETSI, "5G", 2018, https://www.etsi.org/technologies/5g

D. Goovaerts, "Blog: Who is thinking about 5G security?", *Mobile World Live*, 29 May 2018, https://www.mobileworldlive.com/blog/blog-who-is-thinking-about-5g-security/

Home Office, "Emergency services network: overview", *UK Government*, 30 November 2018, https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network

S. Kavanagh, "What is Narrowband IoT?", *5G Guides*, 13 November 2018, https://5g.co.uk/guides/what-is-narrowband-iot/

C. Kelly, "EE confirms 5G launch in 2019", *Total Telecom*, 11 September 2018, https://www.totaltele.com/501021/EE-confirms-5G-launch-in-2019

B. Marr, "The 4th industrial revolution is here – are you ready?", *Forbes*, 13 August 2018, https://www.forbes.com/sites/bernardmarr/2018/08/13/the-4th-industrial-revolution-is-here-are-you-ready/#5c7167f2628b

R. Milne, "Nokia wins $500 European loan for 5G investment", *Financial Times*, 27 August 2018, https://www.ft.com/content/50d54a7a-a9db-11e8-94bd-cba20d67390c

P. Nelson, "Private 5G networks are coming", *Network World*, 07 November 2018, https://www.networkworld.com/article/3319176/mobile-wireless/private-5g-networks-are-coming.html

1.2 Manipulated machine learning sows confusion

Associated Press, "Tesla that crashed in autopilot mode sped up before hitting truck – police", *The Guardian*, 25 May 2018, https://www.theguardian.com/technology/2018/may/24/tesla-that-crashed-in-autopilot-mode-sped-up-before-hitting-truck-police

G. Bailey, "The golden age of algorithms", *Forbes*, 15 November 2018, https://www.forbes.com/sites/gerogebailey1/2018/11/15/the-golden-age-of-algorithms/#1d3ab6e72179

L. Dormehl, "That turtle is a gun! MIT scientists highlight major flaw in image recognition", *Digital Trends*, 02 November 2017, https://www.digitaltrends.com/cool-tech/image-recognition-turtle-rifle/#/1

K. Eykholt et al, "Robust physical-world attacks on deep learning visual classification", *University of Michigan, Ann Arbor, University of Washington, University of California, Berkeley, Samsung Research America and Stony Brooke University,* https://arxiv.org/pdf/1707.08945.pdf

I.J. Goodfellow, J. Schlens, C. Szegedy, "Explaining and harnessing adversarial examples", *Cornell University Library*, 20 March 2015, https://arxiv.org/abs/1412.6572

Investopedia, "Algorithm", 22 May 2018, https://www.investopedia.com/terms/a/algorithm.asp

Investopedia, "Neural Network", 25 July 2018, https://www.investopedia.com/terms/n/neuralnetwork.asp

K. Quach, "How we fooled Google's AI into thinking a 3D-printed turtle was a gun: MIT bods talk to EI Reg", *The Register*, 06 November 2017, https://www.theregister.co.uk/2017/11/06/mit_fooling_ai/

S. Rodriguez, "This former Facebook engineer wants to help companies unlock the A.I. 'black box' to see how it makes decisions", *CNBC*, 24 January 2018, https://www.cnbc.com/2019/01/23/facebook-samsung-engineers-quit-to-form-ai-startup-fiddler-labs.html

The Week Staff, "When will self-driving cars take over", *The Week*, 17 November 2018, https://theweek.com/articles/807864/when-selfdriving-cars-take-over

D. Yadron, D. Tynan, "Tesla driver dies in first fatal crash while using autopilot mode", *The Guardian*, 01 July 2016, https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk

1.3 Parasitic malware feasts on critical infrastructure

J. Bloomberg, "Cryptojacking displaces ransomware as most popular cyberthreat", *Forbes*, 29 July 2018, https://www.forbes.com/sites/jasonbloomberg/2018/07/29/cryptojacking-displaces-ransomware-as-most-popular-cyberthreat/#51c3bd1a86e9

C. Cimpanu, "Tesla internal servers infected with cryptocurrency miner", *Bleeping Computer*, 20 February 2018, https://www.bleepingcomputer.com/news/security/tesla-internal-servers-infected-with-cryptocurrency-miner/

CISION PR Newswire, "Radiflow reveals first documented cryptocurrency malware attack on SCADA network", 08 February 2018, https://www.prnewswire.com/news-releases/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network-300595714.html

R. Eitzman et al, "How the rise of cryptocurrencies is shaping the cyber crime landscape: the growth of miners", *Fireye*, 18 July 2018, https://www.fireeye.com/blog/threat-research/2018/07/cryptocurrencies-cyber-crime-growth-of-miners.html

L. Hay Newman, "Now cryptojacking threatens critical infrastructure, too", *Wired*, 12 February 2018, https://www.wired.com/story/cryptojacking-critical-infrastructure/

ISACA, "Smart Cities: new threats and opportunities", 2018, http://www.isaca.org/info/smart-cities-survey/index.html

Skybox Security, "Vulnerability and threat trends", 2018, https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_Threat_Trends_2018_Mid-Year_Update.pdf

Theme 2: Digital cold war engulfs business

2.1 State-backed espionage targets next gen tech

T. Coleman, "The CIA helped win the Space Race", *International Policy Digest*, 21 July 2014, https://intpolicydigest.org/2014/07/21/the-cia-helped-win-the-space-race/

V. Harini, "China could reportedly use its 'unwritten' tech rules as an 'invisible tool' against US firms", *CNBC*, 14 Aug 2018, https://www.cnbc.com/2018/08/15/us-china-trade-war-chinese-cybersecurity-standards-could-be-employed.html

C. Jasper, "Airbus slams EU as Brexit leads U.K. to quit key defense program", *Bloomberg*, 03 December 2018, https://www.bloomberg.com/news/articles/2018-12-03/airbus-slams-eu-as-brexit-leads-u-k-to-quit-key-defense-program

J. Lewis, "Economic impact of cybercrime – no slowing down", *McAfee*, February 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

P. Neray, "Industrial espionage is a major threat to the manufacturing sector", *Cyber X*, 26 June 2017, https://cyberx-labs.com/blog/industrial-espionage-major-threat-manufacturing-sector/

F. O'Connor, "China increases attacks against US companies as trade war looms", *Cybereason*, 08 June 2018, https://www.cybereason.com/blog/china-us-trade-war-cyberattack-increase

U.S Department of Energy – Office of History and Heritage Resources, "The Manhattan Project, an interactive history", https://www.osti.gov/opennet/manhattan-project-history/Events/1942-1945/espionage.htm

2.2 Sabotaged cloud services freeze operations

Amazon Web Services, "All customer success stories", https://aws.amazon.com/solutions/case-studies/all/

M. Mazur, "Six ways drones are revolutionizing agriculture", *MIT Technology Review*, 20 July 2016, https://www.technologyreview.com/s/601935/six-ways-drones-are-revolutionizing-agriculture/

T. Morrow, "12 risks, threats & vulnerabilities in moving to the cloud", *SEI Insights*, 05 March 2018, https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

S. Nichols, "AWS's S3 outage was so bad Amazon couldn't get into its own dashboard to warn the world", *The Register*, 1 March 2017, https://www.theregister.co.uk/2017/03/01/aws_s3_outage/

J. Novet, "Microsoft narrows Amazon's lead in cloud, but the gap remains large", *CNBC*, 27 April 2018, https://www.cnbc.com/2018/04/27/microsoft-gains-cloud-market-share-in-q1-but-aws-still-dominates.html

J. Sanders, "How the Spectre and Meltdown chip flaws will impact cloud computing", *TechRepublic*, 05 January 2018, https://www.techrepublic.com/article/how-the-meltdown-and-spectre-chip-flaws-will-impact-cloud-computing/

H. Sarmah, "Cloud outages that shook the tech world: 2018", *Analytics India*, 24 December 2018, https://www.analyticsindiamag.com/cloud-outages-that-shook-the-tech-world-2018/

C. Stamford, "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018", *Gartner*, 12 April 2018, https://www.gartner.com/en/newsroom/press-releases/2018-04-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-21-percent-in-2018

Synergy Research Group, "The leading cloud providers increase their market share again in the third quarter", 25 October 2018, https://www.srgresearch.com/articles/leading-cloud-providers-increase-their-market-share-again-third-quarter

2.3 Drones become both predator and prey

BBC, "Gatwick drones: two arrested over flight disruption", 22 December 2018, https://www.bbc.co.uk/news/uk-england-46657505

BBC, "Google's Wing delivery drones head to Europe", 05 December 2018, https://www.bbc.co.uk/news/technology-46456694

BBC, "Heathrow airport: Drone sighting halts departures", 08 January 2018, https://www.bbc.co.uk/news/uk-46803713

The Economist, "Drones need to be encouraged, and people protected", 24 January 2019, https://www.economist.com/leaders/2019/01/26/drones-need-to-be-encouraged-and-people-protected

D. Effin, "The drones are coming", *Fleet Owner*, 15 October 2018, https://www.fleetowner.com/technology/drones-are-coming

C. Forrest, "17 drone disasters that show why the FAA hates drones", *TechRepublic*, 13 June 2018, https://www.techrepublic.com/article/12-drone-disasters-that-show-why-the-faa-hates-drones/

D. Galeon, "As drones become tools of war, companies turn to hacking them", *Futurism*, 20 February 2018, https://futurism.com/drone-hack-technology

Goldman Sachs, "Drones, reporting for work", 2017, https://www.goldmansachs.com/insights/technology-driving-innovation/drones/

A. Heathman, "Amazon-style drone deliveries could be launched within the next year", *Evening Standard*, 06 March 2018, https://www.standard.co.uk/tech/amazon-drone-deliveries-next-year-a3782276.html

Kaspersky, "Drone gone in 11 milliseconds", 19 April 2017, https://www.kaspersky.co.uk/blog/drone-gone-in-11-ms/8654/

R. Bradshaw, "Watch over your head: drones to become new cyberwar weapon", *Hitech News Daily*, 7 February 2018, http://hitechnewsdaily.com/2018/02/watch-over-your-head-drones-to-become-new-cyberwar-weapon/

E. Niiler, "Your drone can give cops a surprising amount of your data", *Wired*, 16 November 2018, https://www.wired.com/story/your-drone-can-give-cops-a-surprising-amount-of-your-data/

P. Howell O'Neill, "Drones emerge as new dimension in cyber war", *Cyber Scoop*, 05 February 2018, https://www.cyberscoop.com/apolloshield-septier-drones-uav-cyberwar-hacking/

RT, "UK defenceless against 'disruptive drone attacks' at British airports, minister admits", 14 January 2019, https://www.rt.com/uk/448733-uk-airport-drone-disruption/

Theme 3: Digital competitors rip up the rulebook

3.1 Digital vigilantes weaponise vulnerability disclosure

L. Franceschi-Bicchierai, "Can AMD vulnerabilities be used to game the stock market?", *Motherboard*, 15 Mar 2018, https://motherboard.vice.com/en_us/article/bj5wy4/amd-flaws-viceroy-short-selling-stock-market

C. Evans, "Announcing Project Zero", *Google Security Blog*, 15 July 2014, https://security.googleblog.com/2014/07/announcing-project-zero.html

C. Osborne, "Zerodium will now pay $2 million for Apple iOS remote jailbreaks", *ZDNet*, 09 January 2019, https://www.zdnet.com/article/zerodium-will-now-pay-2-million-for-apple-ios-remote-jailbreaks/

E. Protalinski, "Google discloses actively exploited Windows vulnerability just 10 days after reporting it to Microsoft", *Venture Beat*, 31 October 2016, https://venturebeat.com/2016/10/31/google-discloses-actively-exploited-windows-vulnerability-just-10-days-after-reporting-it-to-microsoft/

F. Y. Rashid, "Extortion or fair trade? The value of bug bounties", *InfoWorld*, 09 September 2015, https://www.infoworld.com/article/2981695/security/extortion-or-fair-trade-value-bug-bounty-programs.html

tCell, "Security report for in-production web applications", 2018, https://info.tcell.io/hubfs/DemandGen_Content/Research%20Papers/tCell_wp-stateofsecurity-2018-web.pdf

3.2 Big tech break up fractures business models

The Economist, "Do major web companies such as Google, Facebook and Amazon need to be reined in?", 04 September 2018, https://twitter.com/TheEconomist/status/1037220559661277184

G. Faulconbridge, P. Sandle, "Father of web says tech giants may have to be split up", *Reuters*, 01 November 2018, https://www.reuters.com/article/us-technology-www/father-of-web-says-tech-giants-may-have-to-be-split-up-idUSKCN1N63MV

Gartner, "Gartner says worldwide IaaS public cloud services market grew 29.5 percent in 2017", *Gartner*, 01 Aug 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-01-gartner-says-worldwide-iaas-public-cloud-services-market-grew-30-percent-in-2017

A. Hern, "Facebook shared private user messages with Netflix and Spotify", *The Guardian*, 19 December 2018, https://www.theguardian.com/technology/2018/dec/19/facebook-shared-user-data-private-messages-netflix-spotify-amazon-microsoft-sony

A. Lotz, "'Big tech' isn't one big monopoly – it's 5 companies all in different businesses", *The Conversation*, 23 March 2018, https://theconversation.com/big-tech-isnt-one-big-monopoly-its-5-companies-all-in-different-businesses-92791

K. McCarthy, "Biggest Washington DC lobbyist is now a tech giant (yes, it's Google), *The Register*, 24 January 2018, https://www.theregister.co.uk/2018/01/24/google_washington_lobbying/

J. Rankin, "Google fined £3.8bn by EU over Android antitrust violations", *The Guardian*, 18 July 2018, https://www.theguardian.com/business/2018/jul/18/google-faces-record-multibillion-fine-from-eu-over-android

R. Reich, "Break up Facebook (and while we're at it, Google, Apple and Amazon)", *The Guardian*, 20 November 2018, https://www.theguardian.com/commentisfree/2018/nov/20/facebook-google-antitrust-laws-gilded-age

Statista, "Most popular social network sites worldwide as of October 2018, ranked by number of active users (in millions)", October 2018, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Statista, "Worldwide desktop market share of leading search engines from January 2010 to October 2018", October 2018, https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/

J. Titcomb, R. Pagnamenta, "Watchdogs close in on Silicon Valley giants as monopoly concerns mount", *The Telegraph*, 15 December 2018, https://www.telegraph.co.uk/technology/2018/12/15/watchdogs-close-silicon-valley-giants-monopoly-concerns-mount/

H. Weisbaum, "Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal", *NBC News*, 18 April 2018, https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011

C. Weller, "7 insane facts that reveal how big Amazon has become", *Business Insider*, 7 Sep 2017, https://www.businessinsider.com/amazon-size-insane-facts-about-company-2017-9/international?r=UK&IR=T/#75-of-seattles-working-age-population-are-amazon-employees-1

3.3 Rushed digital transformations destroy trust

T. Catlin, L. LaBerge, S. Varney, "Digital strategy: the four fights you have to win", *McKinsey*, October 2018, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-strategy-the-four-fights-you-have-to-win

Couchbase, "Couchbase research reveals organizations risk wasting an average of $28 million on digital projects as pressure to transform mounts", 14 August 2018, https://www.couchbase.com/press-releases/couchbase-research-reveals-organizations-risk-wasting-an-average-of-usd28-million-on-digital-projects-as-pressure-to-transform-mounts

T. H. Davenport, G. Westerman, "Why so many high-profile digital transformations fail", *Harvard Business Review*, 9 March 2018, https://hbr.org/2018/03/why-so-many-high-profile-digital-transformations-fail

K. Hill, "Casualties of digital transformation? Poor integration costs businesses, report says", *RCR Wireless News*, 23 January 2019, https://www.rcrwireless.com/20190121/software/casualties-digital-transformation-poor-integration-costs-report-says

B. Prassad Narayana, "Legacy vs. modern systems: 5 things that you can do better with the latter!", *Infosys*, 01 February 2018, http://www.infosysblogs.com/government/2018/02/legacy_vs_modern_systems_5_thi.html

F. Toesland, "How five brands learned from digital transformation failure", *Raconteur*, 26 September 2018, https://www.raconteur.net/digital-transformation/digital-transformation-failure

S. ZoBell, "Why digital transformations fail: closing the $900 billion hole in enterprise strategy", *Forbes*, 13 March 2018, https://www.forbes.com/sites/forbestechcouncil/2018/03/13/why-digital-transformations-fail-closing-the-900-billion-hole-in-enterprise-strategy/#442af34f7b8b

Appendix B: Assessing predictions from Threat Horizon 2018

The IoT leaks sensitive information

M. Burgess, "Google Home's data leak proves the IoT is still deeply flawed", *Wired Magazine*, 20 June 2018, https://www.wired.co.uk/article/google-home-chromecast-location-security-data-privacy-leak

K. O'Flaherty, "Cyber security: Assessing the evolving threat landscape", *The Land Mobile*, 14 November 2018 http://www.landmobile.co.uk/indepth/cyber-security-evolving-threat-landscape-wi-fi-cellular/

G. Rosner, "The internet of things is built to leak", *The Hill*, 06 August 2018, https://thehill.com/opinion/cybersecurity/391347-the-internet-of-things-is-built-to-leak

Opaque algorithms compromise integrity

S. Levin, "Tesla fatal crash: 'autopilot' mode sped up car before driver killed, report finds", *The Guardian*, 08 June 2018, https://www.theguardian.com/technology/2018/jun/07/tesla-fatal-crash-silicon-valley-autopilot-mode-report

Electronic Privacy Information Center, "Algorithmic transparency: end secret profiling", 10 December 2018, https://www.epic.org/algorithmic-transparency/

Rogue governments use terrorist groups to launch cyber attacks

N/A

Unmet board expectations exposed by a major incident

H. Broadman, "Corporate boards' oversight of cyber risks is too passive", *Forbes*, 28 November 2018, https://www.forbes.com/sites/harrybroadman/2018/11/28/corporate-boards-cannot-afford-to-be-passive-in-oversight-of-cyber-risk-mitigation/#7473841e68e4

P. German, "Getting cybersecurity to the top of the boardroom agenda", *ITProPortal*, 05 December 2018, https://www.itproportal.com/features/getting-cybersecurity-to-the-top-of-the-boardroom-agenda/

M. Settle, "Talking to the board about information security", *Forbes*, 20 July 2018, https://www.forbes.com/sites/forbestechcouncil/2018/07/20/talking-to-the-board-about-information-security/#689b4c736158

Researchers silenced to hide security vulnerabilities

C. Doctorow, "Oracle's bad faith with security researchers led to publication of a Virtualbox 0-day", *BoingBoing*, 11 November 2018, https://boingboing.net/2018/11/11/unreliable-oracle.html

Z. Whittaker, "Security firm Keeper sues news reporter over vulnerability story", 20 December 2017, https://www.zdnet.com/article/security-firm-keeper-sues-news-reporter-over-vulnerability-story/

Cyber insurance safety net is pulled away

A. J. Martin, "Redacted documents: cyber security breaches rising across UK defence sector", *Sky News*, 18 December 2018, https://news.sky.com/story/cyber-security-breaches-rising-across-uk-defence-sector-11584827

Intelligent Insurer, "Cyber insurance: a not so global market", 18 December 2018, https://www.intelligentinsurer.com/article/cyber-insurance-a-not-so-global-market

O. Ralph, R. Armstrong, "Mondelez sues Zurich in test for cyber hack insurance", *Financial Times*, 10 January 2019, https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e

Disruptive companies provoke governments

R. Foroohar, "Year in a word: Techlash", *Financial Times*, 16 December 2018, https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e

L. Hay Newman, "Australia's encryption-busting law could impact global privacy", *Wired*, 07 December 2018, https://www.wired.com/story/australia-encryption-law-global-impact/

M. Scott, L. Cerulus, L. Kayali, " Six months in, Europe's privacy revolution favors Google, Facebook", *Politico*, 23 November 2018, https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/

J. Sommerlad, "Facebook data breach: Why is Mark Zuckerberg appearing before Congress?", *Independent*, 05 April 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/mark-zuckerberg-congress-how-watch-hearing-facebook-data-breach-cambridge-analytica-a8289316.html

Regulations fragment the cloud

WebWire, "New report explains how business and government can accelerate the circular built environment", 06 December 2018, https://www.webwire.com/ViewPressRel.asp?aId=232505

Criminal capabilities expand gaps in international policing

A. Peters, "Closing the global cyber enforcement gap", *Lawfare*, 18 December 2018, https://www.lawfareblog.com/closing-global-cyber-enforcement-gap

P. Ryan, "Dubai Interpol summit told dark web drug deals and 'new dimension' of cyber crime pose great threat", *The National*, 18 November 2018, https://www.thenational.ae/uae/dubai-interpol-summit-told-dark-web-drug-deals-and-new-dimension-of-cyber-crime-pose-great-threat-1.793127

Appendix C: Assessing predictions from Threat Horizon 2019

Premeditated internet outages bring trade to its knees

BBC, "Could Russia cut undersea communication cables?", 15 December 2017, https://www.bbc.co.uk/news/world-42365191

K. Townsend, "U.S. Cyber Command launched DDoS attack against North Korea: Report", *SecurityWeek*, 02 October 2017, https://www.securityweek.com/us-cyber-command-launched-ddos-attack-against-north-korea-report

Ransomware hijacks the Internet of Things

A. DeNisco Rayome, "As IoT attacks increase 600% in one year, businesses need to up their security", *TechRepublic*, 21 March 2018, https://www.techrepublic.com/article/as-iot-attacks-increase-600-in-one-year-businesses-need-to-up-their-security/

J. Sattler, "Wake-up call: the time to secure the IoT is now", *F-Secure*, 22 January 2018, https://blog.f-secure.com/wake-up-call-the-time-to-secure-the-iot-is-now/

Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", 2018, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Privileged insiders coerced into giving up the crown jewels

B. Jensen, B. Valeriano, R. Maness, "Cyber Compellence: Applying Coercion in the Information Age", *Marine Corps University, American University, Cardiff University, Northeastern University*

T. Seals, "17% of workers fall for social engineering attacks", *Infosecurity Magazine*, 09 April 2018, https://www.infosecurity-magazine.com/news/17-of-workers-fall-for-social/

Automated misinformation gains instant credibility

E. Durkin, "Almost 350 news outlets to publish editorials denouncing Trump's 'dirty war' on press", *The Guardian*, 16 August 2018, https://www.theguardian.com/us-news/2018/aug/15/trump-press-editorials-defence-fake-news-media-attacks-us

J. McCarthy, "'The time for self-regulation is up': ICO takes aim at Facebook, Leave EU and data misuse", *The Drum*, 06 November 2018, https://www.thedrum.com/news/2018/11/06/the-time-self-regulation-up-ico-takes-aim-facebook-leave-eu-and-data-misuse

R. Nieva, "Google is a no-show at DC tech hearings, stoking anger in Congress", *CNET*, 05 September 2018, https://www.cnet.com/news/google-is-a-no-show-at-the-washington-dc-tech-hearings-stoking-anger-in-congress/

Falsified information compromises performance

K. Costello and S. Hippold, "Gartner forecasts worldwide public cloud revenue to grow 17.3 percent in 2019", *Gartner*, 12 September 2018, https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019

McAfee, "Cloud Adoption and Risk Report 2019", https://mscdss.ds.unipi.gr/wp-content/uploads/2018/10/Cloud-Adoption-Risk-Report-2019.pdf

Subverted blockchains shatter trust

J. Leonard, "Blockchain update: Blockchain too immature for government use, finds Australia's DTA", *Computing*, 23 October 2018, https://www.computing.co.uk/ctg/news/3033006/blockchain-update-blockchain-too-immature-for-government-use-finds-australias-dta

A. Orlowski, "Blockchain study finds 0.00% success rate and vendors don't call back when asked for evidence", *The Register*, 30 November 2018, https://www.theregister.co.uk/2018/11/30/blockchain_study_finds_0_per_cent_success_rate/

Surveillance laws expose corporate secrets

S. Carey, "The Snooper's Charter: everything you need to know about the Investigatory Powers Act", *Computer World UK*, 04 December 2018, https://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/

Privacy regulations impede the monitoring of insider threats

L. Irwin, "The GDPR: can your organisation monitor employees' personal communications?", *IT Governance*, 27 September 2017, https://www.itgovernance.eu/blog/en/the-gdpr-can-your-organisation-monitor-employees-personal-communications

A headlong rush to deploy AI leads to unexpected outcomes

J. Seidel, "CIMON, the International Space Station's artificial intelligence, has turned belligerent", *News*, 05 December 2018, https://www.news.com.au/technology/science/space/cimon-the-international-space-stations-artificial-intelligence-has-turned-belligerent/news-story/953a84bc8c4fe414eed2d0550e1d8bf4

Appendix D: Assessing predictions from Threat Horizon 2020

Cyber and physical attacks combine to shatter business resilience

J. Lynch, "How the Army is virtually prepping real cyberattacks", *Fifth Domain*, 22 June 2018, https://www.fifthdomain.com/dod/army/2018/06/22/how-the-army-is-virtually-prepping-for-real-cyberattacks/

A. J. Martin, "UK infrastructure being targeted by hackers", *Sky News*, 06 April 2018, https://news.sky.com/story/uk-infrastructure-being-targeted-by-hackers-11319033

Satellites cause chaos on the ground

A. Chrisafis, "'Act of espionage': France accuses Russia of trying to spy on satellite data", *The Guardian*, 07 September 2018, https://www.theguardian.com/world/2018/sep/07/france-accuses-russia-spying-satellite-communications-espionage

The Economist, "It will soon be possible to send a satellite to repair another", 24 November 2018, https://www.economist.com/science-and-technology/2018/11/24/it-will-soon-be-possible-to-send-a-satellite-to-repair-another

G. Falco, "Invaders from space – hacks against satellites threaten our critical infrastructure", *San Francisco Chronicle*, 24 August 2018, https://www.sfchronicle.com/opinion/article/Invaders-from-space-hacks-against-satellites-13175362.php

J. Foust, "'No encryption, no fly' rule proposed for smallsats", *SpaceNews*, 09 August 2018, https://spacenews.com/no-encryption-no-fly-rule-proposed-for-smallsats/

J. Seidel, "Killers or fixers? Russia's 'space apparatuses inspectors' raise US fears of satellite sabotage", *News*, https://www.news.com.au/technology/innovation/military/killers-or-fixers-russias-space-apparatuses-inspectors-raise-us-fears-of-satellite-sabotage/news-story/9a71d406635150819eeeb29ce927ee1c

Weaponised appliances leave organisations powerless

The Economist, "Air-conditioners do great good, but at a high environmental cost", 25 August 2018, https://www.economist.com/international/2018/08/25/air-conditioners-do-great-good-but-at-a-high-environmental-cost

M. Hongoltz-Hetling, "Hackers are attacking the electric grid", *Popular Science*, 18 January 2018, https://www.popsci.com/hackers-are-attacking-electric-grid

A. Muravitsky, V. Dashchenko, R. Sako, "IoT hack: how to break a smart home… again", *Kaspersky Lab*, 27 February 2018, https://securelist.com/iot-hack-how-to-break-a-smart-home-again/84092/

Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", 2018, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Quantum arms race undermines digital economy

The Economist, "The race is on to dominate quantum computing", 18 August 2018, https://www.economist.com/business/2018/08/18/the-race-is-on-to-dominate-quantum-computing

C. Hammerschmidt, "Infineon preparing post-quantum cryptography for cars, infrastructure", *Electronic Design*, 02 October 2017, https://www.electronicdesign.com/automotive/infineon-preparing-post-quantum-cryptography-cars-infrastructure

M. Giles, "Quantum computers pose a security threat that we're still totally unprepared for", *MIT Technology Review,* 03 December 2018, https://www.technologyreview.com/s/612509/quantum-computers-encryption-threat/

J. Kahn, "IBM ups pressure on Google and other rivals with quantum computer prototype", *Financial Post*, 10 November 2017, https://business.financialpost.com/technology/ibm-ups-pressure-on-google-and-other-rivals-with-quantum-computer-prototype

F. Lardinois, "IBM unveils its first commercial quantum computer", *TechCrunch*, 08 January 2019, https://techcrunch.com/2019/01/08/ibm-unveils-its-first-commercial-quantum-computer/

Artificially intelligent malware amplifies attackers' capabilities

P. Tucker, "Tomorrow's intelligent malware will attack when it sees your face", *Defense One*, 14 August 2018, https://www.defenseone.com/technology/2018/08/tomorrows-intelligent-malware-will-attack-when-it-sees-your-face/150550/

Attacks on connected vehicles put the brakes on operations

P. McGee, "Electric driverless vehicles set to gain approval for public roads", *Financial Times*, 02 December 2018, https://www.ft.com/content/f76ef090-f47f-11e8-ae55-df4bf40f9d0d

J. C. Reindl, "Car hacking remains a very real threat as autos become ever more loaded with tech", *USA Today*, 15 January 2018, https://eu.usatoday.com/story/money/2018/01/14/car-hacking-remains-very-real-threat-autos-become-ever-more-loaded-tech/1032951001/

Biometrics offer a false sense of security

W. Ashford, "Superdrug denies data breach", *ComputerWeekly*, 22 August 2018, https://www.computerweekly.com/news/252447313/Superdrug-denies-data-breach

H. Williams, "Facial recognition technology: what are the dangers?", *TechWorld*, 18 December 2017, https://www.techworld.com/security/facial-recognition-technology-what-are-dangers-security-preventions-3669268/

New regulations increase the risk and compliance burden

Consultancy UK, "GDPR preparation has cost FTSE 350 businesses around $1.1 billion", 23 May 2018, https://www.consultancy.uk/news/17226/gdpr-preparation-has-cost-ftse-350-businesses-around-11-billion

Legal ICT, "Privacy and monitoring at work under the GDPR", 2018, https://legalict.com/factsheets/privacy-monitoring-work-gdpr/

Trusted professionals divulge operational weak points

U. Hassan, "Insider threats rise as businesses struggle with cybercrime", *Computer Business Review*, 25 July 2018, https://www.cbronline.com/news/insider-threats-cybercrime

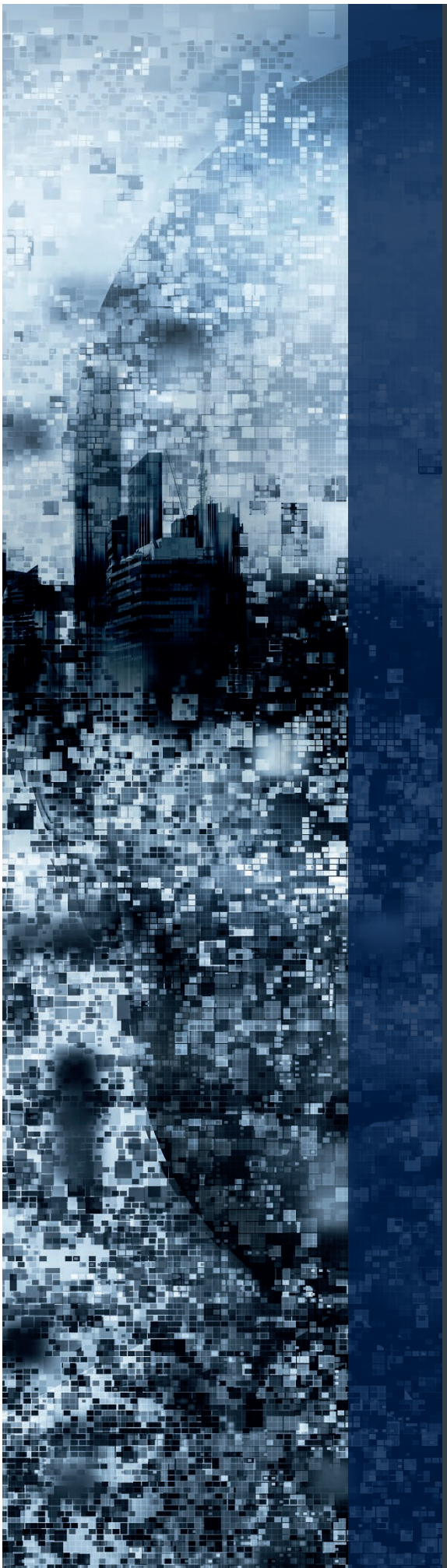
ACKNOWLEDGEMENTS

The ISF thanks all Members and external experts who contributed to the information gathering and validation phases of this report, as well as those who reviewed pre-publication drafts. We are grateful to the ISF Advisory Council and those who participated in discussions at ISF Chapter meetings and the ***ISF Annual World Congress 2018*** in Las Vegas. Members often contribute research information related to their own organisations and those contributions have been anonymised by default. The views, opinions and comments in this report are not necessarily of work group participants or Member organisations.

ABOUT ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.



FOR FURTHER INFORMATION CONTACT:

Information Security Forum
+44 (0)20 3875 6868
info@securityforum.org
securityforum.org

Information Security Forum

REFERENCE: ISF 19 01 01