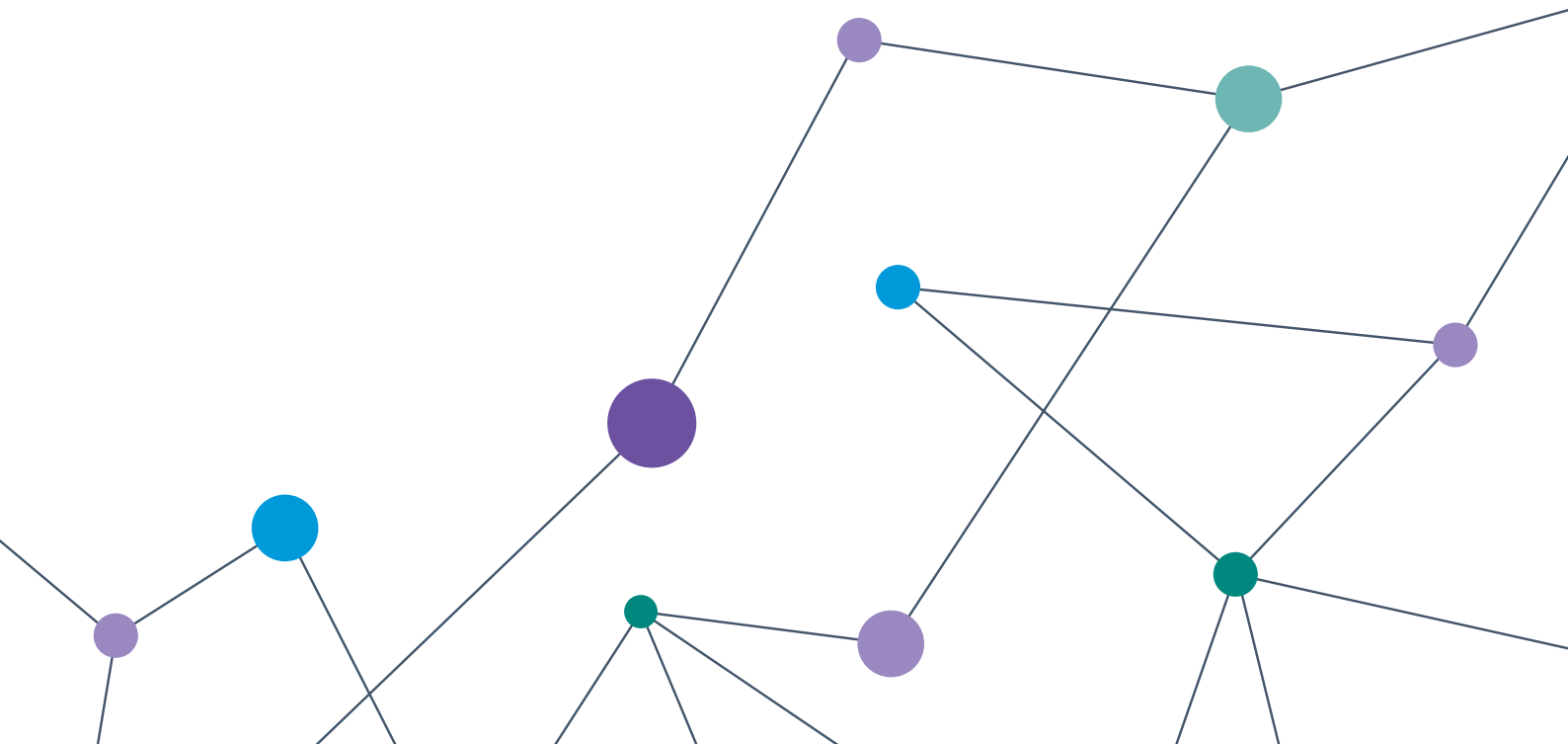
ATKINS

Cyber resilient infrastructure

Securing our critical national infrastructure and defence capabilities


ATKINS
Cyber supplier to
HM Government

Contents



Foreword

Martin Chalmers

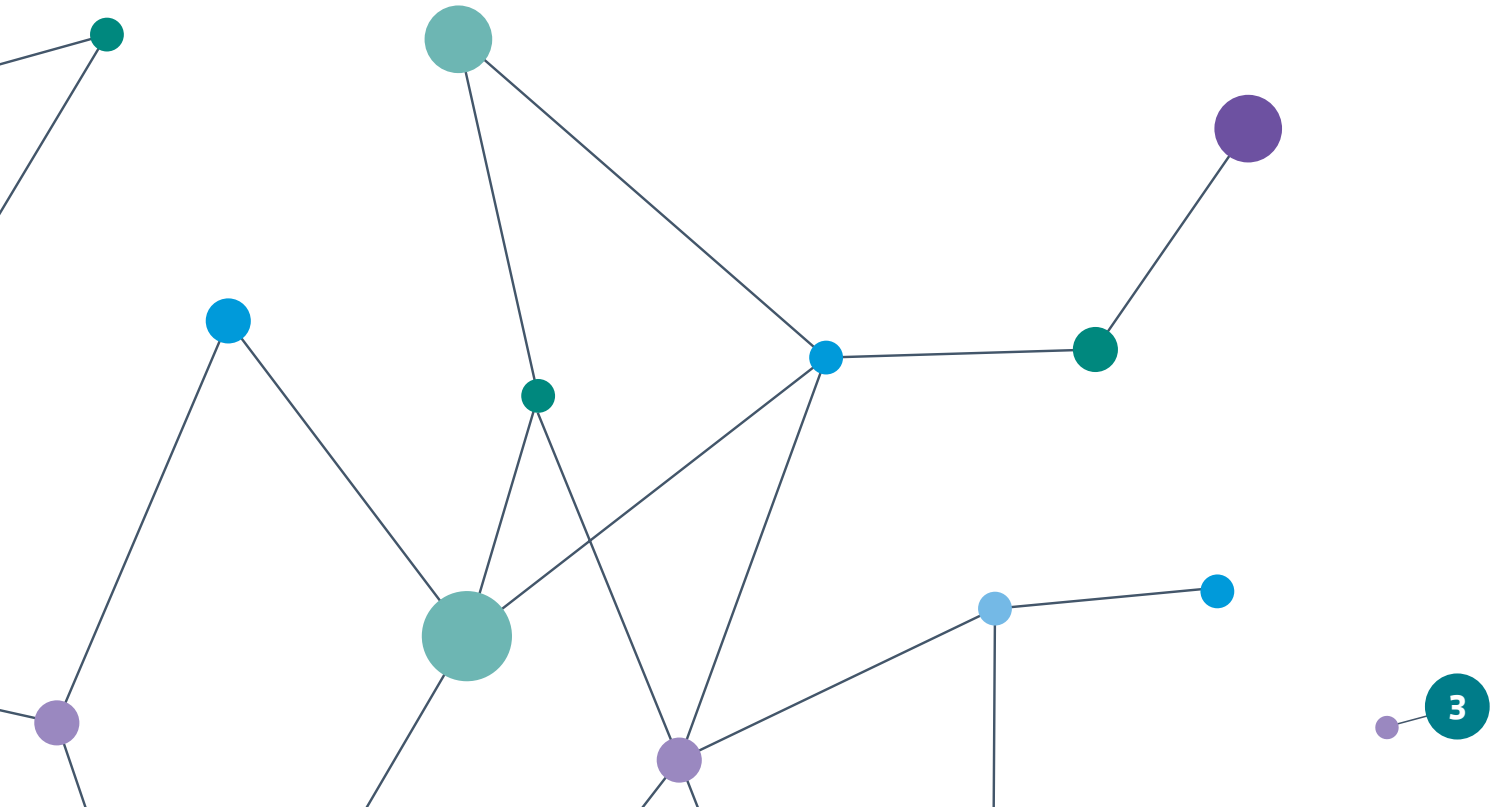
Digital technology is increasingly part of the fabric of everyday life, manifested in smartphones, internet-enabled household equipment, even in our cars. Beyond this, technology is also rapidly pervading the industrial infrastructure that keeps our modern society operating. This is resulting in a convergence between Information Technology (IT) and Operational Technology (OT) – linking previously separate worlds across the internet.

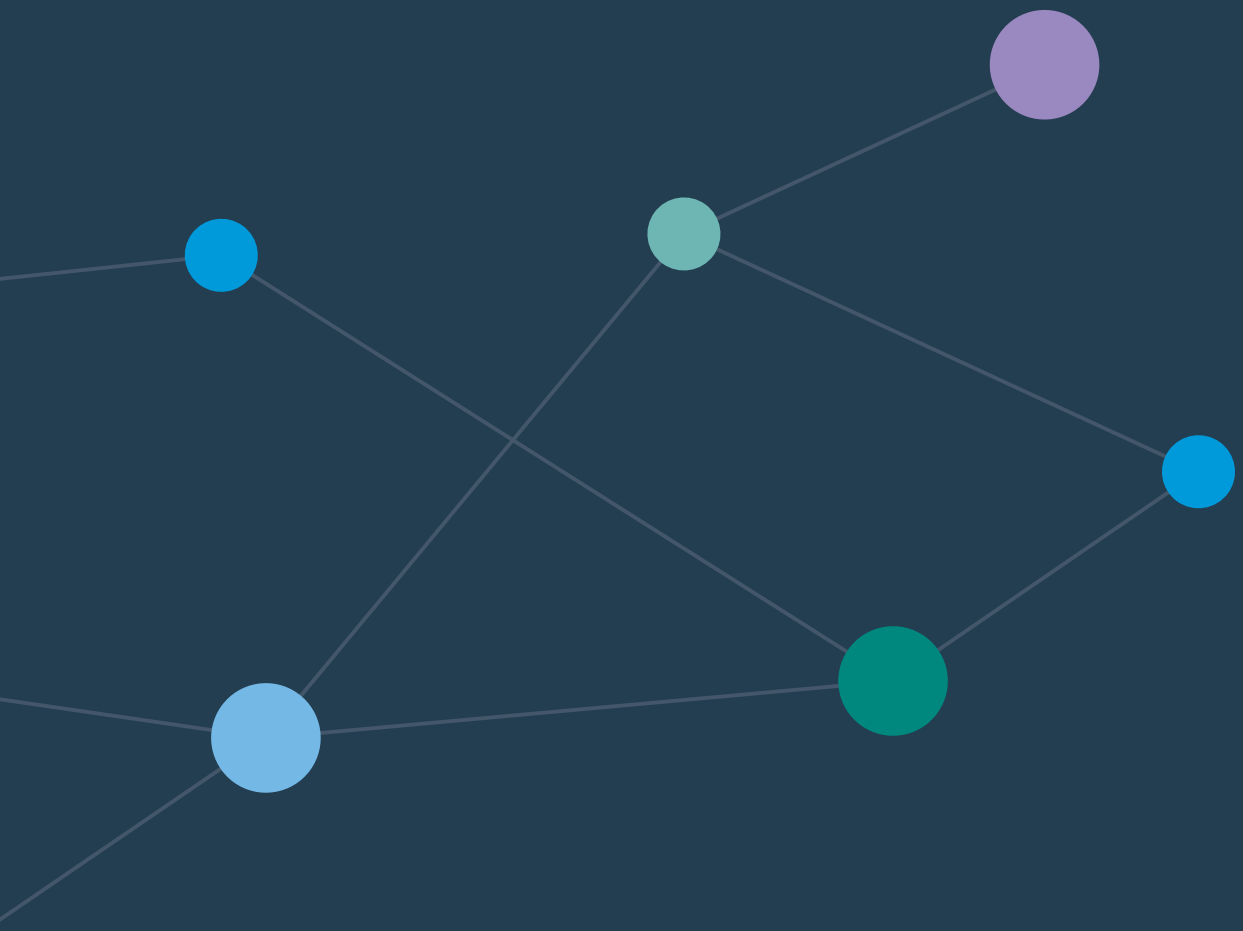
This technology is under threat from cyber-attack with potentially disastrous consequences for society. While some organisations are beginning to respond to these threats to industrial and process control systems, industry as a whole is behind the curve. These operational technologies are still considered by malicious attackers to present softer – but high value – targets, particularly at the point of IT network convergence.

The business risks from this threat – financial, reputational and safety-related – are significant and potentially existential. The response demanded is not just a matter of technology but of culture, organisation, process and governance. The scope of the response is not limited to an isolated function but extends to the whole of an organisation and its supply chain.

Against this backdrop, leadership is critical. The people who are responsible for running and leading an organisation, regardless of size, should be focusing on this challenge, driving the full spectrum of measures required to enable their staff to secure business operations.

This report is for those leaders, to help them develop a better understanding of the cyber world and the challenges it presents. It also aims to show them that there are ways to embrace with confidence the great benefits that digital technologies can bring by ensuring that their operations are cyber-resilient.





Cyber resilience in context

What is cyber resilience?

In recent years we've all witnessed greater convergence of IT, enterprise technology and operational technology within our organisations. The pace of change has been dramatic and shows no sign of slowing down anytime soon. It's this connection between hardware and software that is making cyber-attacks easier and more dangerous, penetrating to the core of our operations.

The news is full of companies being hacked, such as the high-profile cyber security breach of telecoms company TalkTalk in October 2015. However, what's more worrying from an engineering industry and UK security perspective is the potential impact of an attack on some of our critical national infrastructure. This infrastructure includes utilities, power networks, public transport, and defence facilities.

In the face of this ever-evolving threat, and in line with the UK Government's national cyber security strategy, every organisation should have a strategy for cyber security, not only aligned with business needs and budgets but also focused on an organisation's cyber resilience. It is only through such planning and governance that organisations can protect their business operations from an inevitable attack.

We view cyber resilience as the ability of an organisation to understand the cyber threats it's facing, to inform the known risks, to put in place proportionate protection, and to recover quickly from attack. Depending upon the client, robust cyber resilience ultimately provides cost-effective business or service continuity, sustained revenue, or the uninterrupted delivery of military effects. It also contributes toward the ongoing protection of the UK.

Nick Roberts, Atkins UK & Europe CEO

"Technology is impacting the shape of our industry as we know it, breaking down traditional hierarchies and transforming what we deliver, how we deliver it and who we deliver it for.

When it connects people and infrastructure it can help us respond to issues in real time, to create data sets that enable us to predict and plan, to influence user-centric design, maintenance and optimisation and to ensure investment is made in the right places. However, opportunities also carry risks.

As the designers, builders and operators of infrastructure that millions of people rely on every day we need to ask ourselves if we can honestly say we're doing all that we can to protect ourselves, our clients and the public.

We need to elevate the importance of cyber security to board level, just as safety is considered a top priority amongst senior leadership teams. In many cases this will mean investment, but, like safety, this is a necessity rather than a luxury."

Cyber resilience by the numbers

In order to assess confidence in the cyber resilience of UK defence and critical national infrastructure (CNI) organisations, we undertook some independent research of our clients and partners that operate in this area.

This involved interviews with senior figures across a wide range of CNI, government and defence organisations. These included Airbus Defence & Space, Anglian Water, CREST, Department for Culture, Media & Sport, Ministry of Defence, Qinetiq, and the UK Space Agency.

As well as serving as a confidence barometer, the following results also help paint a picture of the CNI industry's major cyber security concerns, both today and in the near future.

Andy Wall analysed some of the trends behind the research figures:

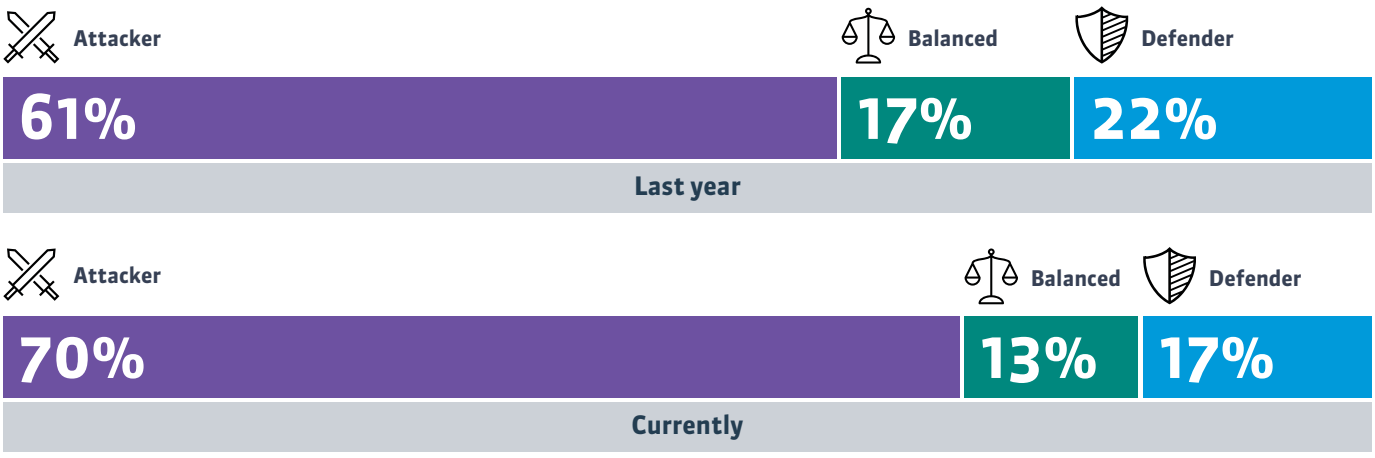
"Respondents believe that the balance of advantage is increasingly in the hands of cyber attackers, and that keeping them all out is practically impossible. It's never been more important to ensure that organisations are **investing** to protect their greatest assets and have well-developed responses to cyber-attack.

"The number one cyber security concern today is vulnerabilities around **people.** These include insider threat, user browsing, board-level awareness, and staff understanding. While awareness of cyber security has improved in recent years, there is still some way to go to properly embed that.

"Another area of concern is the cyber security of CNI supply chains, with almost 60 per cent reporting low levels of confidence and half of those expressing no confidence at all. We talk later in this report about the importance of adopting effective **governance,** industry standards and assessments to address this.

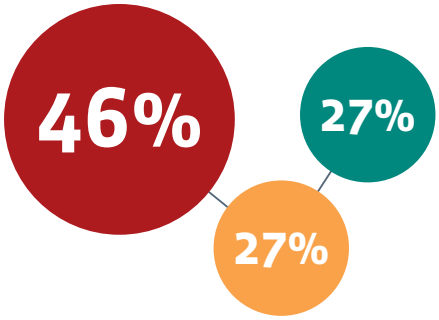
"Finally, **transparency** was raised as an enduring industry challenge. A lack of clear definitions of risk terms and reliance upon confusing technical language to define the threat is switching off senior leaders. This in turn is preventing them from fully understanding the risks and potential mitigation measures. Hopefully this report will help to overcome some of those barriers."

Perception of where the advantage lies between **cyber attacker** and **defender**

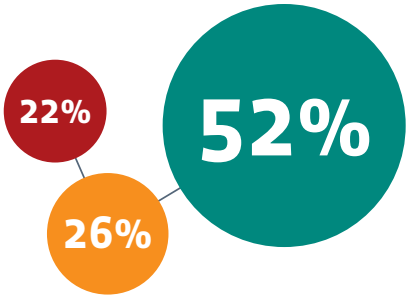


Critical national infrastructure **confidence barometer**

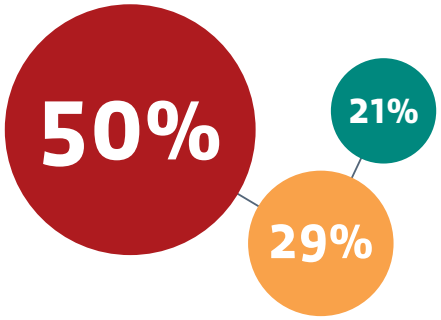
Knowing what information and OT assets are protected from cyber-attack



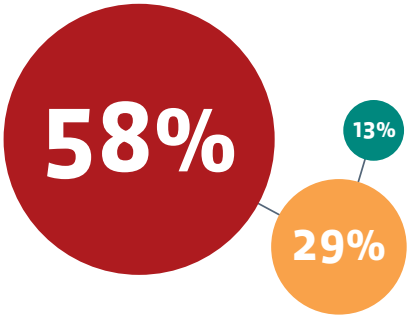
Having cyber security measures that meet regulatory requirements



Employing staff aware of the part they play in protecting their organisation from cyber-attack



Maintaining supply chains that are secure against cyber-attack



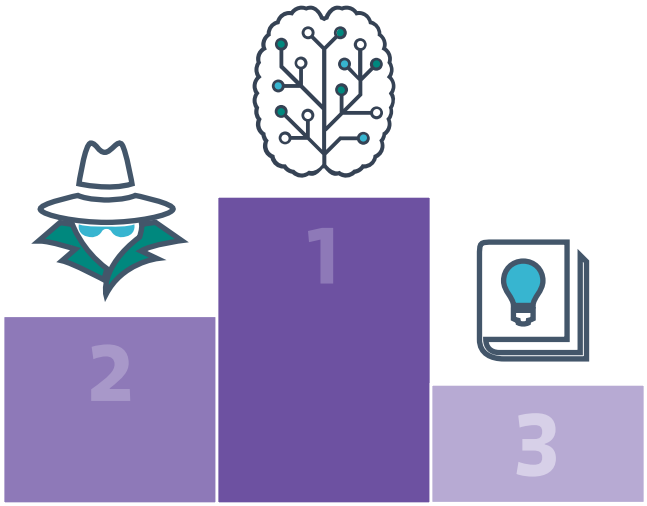
Low confidence Moderate confidence High confidence

Top three cyber security concerns

Currently

1. People
2. Network compromise and legacy systems
3. Organised and state-sponsored cyber crime

Future



1. The rapid advance of technology, especially convergence
2. Organised and state-sponsored cyber crime
3. Shortage of skills required for cyber defence

Defence and security in the information age

General Sir Richard Barrons

What are the changing and evolving military risks to critical national infrastructure in the digital age?

Government, industry and the general public are aware of how much our daily life relies on the safe and efficient functioning of critical national infrastructure (CNI). Although the risks are sometimes exposed by industrial disputes or by the effects of disaster, man-made or natural, we generally still take a constant supply of goods and services for granted.

To these risks we can add a developing recognition of the importance of cyber defence as part of CNI resilience, which tends to focus on individual criminal or terrorist acts. Overall, however, our thinking about the security of our daily life reflects the experience of a comfortable existence since the end of the Cold War and breeds assumptions that the future will be more of the same. It is time for a harder look at what the future may hold for the defence and security of the UK and the place of CNI within it.

There are at least three major sources of potential defence and security risk to the UK and its allies and partners as the 21st Century unfolds:

- The global balance of power continues to change. In the 'Asian Century' economic and, therefore, military potential is shifting to Asia and to China in particular.
- The strategic context in which UK homeland security and our interests abroad must be protected and advanced is becoming potentially more threatening. The UK does not hold the initiative over world events and is at risk from poor outcomes. Terrorism and migration are symptoms of global trends that we cannot ignore.
- In the military sphere, the way conflict is conducted is changing rapidly as a result of new technology and astute investment, especially by Russia and China, specifically designed to overcome the current perceived military advantages of Western forces. This is a combination of new military capability, including offensive cyber, and new methods designed to change the facts on the ground without provoking a military response.

This changing horizon matters to Government and industry. There are vital common interests at stake, such as the food, energy supplies and capital flows that are essential to the UK and its place in an interconnected world. The UK and its industries rely greatly on how a stable, progressive, strategic environment is maintained. Isolation is not possible and there is no guarantee that Europe is somehow now immune to conflict.

The core point for the owners and operators of CNI is that in modern conflict one of the most effective strategies is to attack an opponent's infrastructure in order to bring their daily life to a halt. This could materialise at very short notice in a confrontation as cyber-attack (a daily concern) or in an armed conflict (not an immediate concern). These risks are not widely considered, partly as a result of decades living free from 'existential' risk, partly because they do not feel imminent, and partly because the remedies may be expensive. They should not be ignored.

So how does the UK do better? Doing so in a more difficult world starts with recognising how things have changed and thinking through the implications in an honest and rigorous way. This is the job of both industry and Government, given the spread of expertise and responsibility. Part of the mitigation then lies in exploiting the transformative potential of the Information Age as it profoundly affects our politics, society and commerce. It will be the same for how future military capability is designed, built and operated, and equally vital to how the security of CNI is delivered.

For the military, this is about much more than just cyber defence or the exploitation of social media. It requires the integrated exploitation over time of four major opportunities to build new military capability:

- Seizing the potential of the combination of the expansion in data, processing power, and connectivity – the power of Big Data and the Internet of Things.
- Maximising the capability of existing and planned military space-based capability, combined with harnessing the rapid growth in commercial space investment to support communications and imagery.
- Developing the huge potential of new weapons and sensors built around the growth in range, stealth, precision, choice of effects, and survivability possible in employing emerging technology. In particular, the ability to separate and network complex weapons from their present reliance on sophisticated platforms introduces new ways to achieve mass, deception, and resilience at lower cost.
- Adopting the rapid evolution of autonomous systems and robotics, in order to acquire both greater levels of effectiveness and efficiency, including by reducing manpower costs and logistic footprints.

An information age approach will improve the security of the UK by hardening the resilience of CNI against a broader range of risks.

First, improve the intelligence available to owners and operators about the security context in which their infrastructure is operating. It means much better intelligence collection (from networked open source systems, including projects such as Smart City data), fusion, analysis and visualisation to monitor current operations and to quickly identify risks and anomalies. This understanding will often also lead to efficiency gains and new commercial opportunity.

Second, improve the physical resilience of UK CNI, so that it is harder to interfere with. This is about changing protection levels to mitigate more thoroughly, and to agreed standards, the risks arising from criminality, terrorism and disaster. It must include thinking through how CNI is vulnerable to a range of offensive military or para-military action in a crisis, building in resilience where possible, and understanding and sharing the implications where not. Surprise is an effect best inflicted only on an opponent. Future physical security will include the use of robotics to replace people in dull, repetitive and dangerous roles.

Third, improve the digital resilience of UK CNI, comprehensively protecting equipment, control systems and the networks that connect them. This requires an holistic cyber defence though a combination of design, engineering, information resilience, planning, education, training, culture and behaviour – now with both state and non-state adversaries in mind.

Fourth, to improve the ability of infrastructure and the communities reliant on them to withstand a strategic shock. In order to achieve this we need to invest in:

- What 'strategic shock' may look like so people are conceptually better equipped to react should it occur.
- Quality contingency planning and preparation, drawing in all the affected agencies and institutions.
- Improved 'command and control' capability so that CNI leadership's response to a crisis is efficient and effective.

It rests on information and intelligence, but also requires better decision support tools, robust communications capability with which to disseminate instructions and receive reports, and a full set of media tools with which to inform government, customers and communities about what is going on and what they should do. Social media (in a variety of languages) is at the heart of this, but other channels still matter.

Operational technology cyber resilience trends

Dr Richard Piggin

What do the events of the last two years reveal about the growing sophistication of cyber-attacks against operational technology and critical national infrastructure?

Until recently, the prospect of a cyber-attack impacting the delivery of public services, such as energy provision, was largely theoretical. However, it became a reality on 23 December 2015, when Ukrainian media reported that a cyber-attack had left half the homes and 1.4 million people in the Ivano-Frankivsk region without electricity.

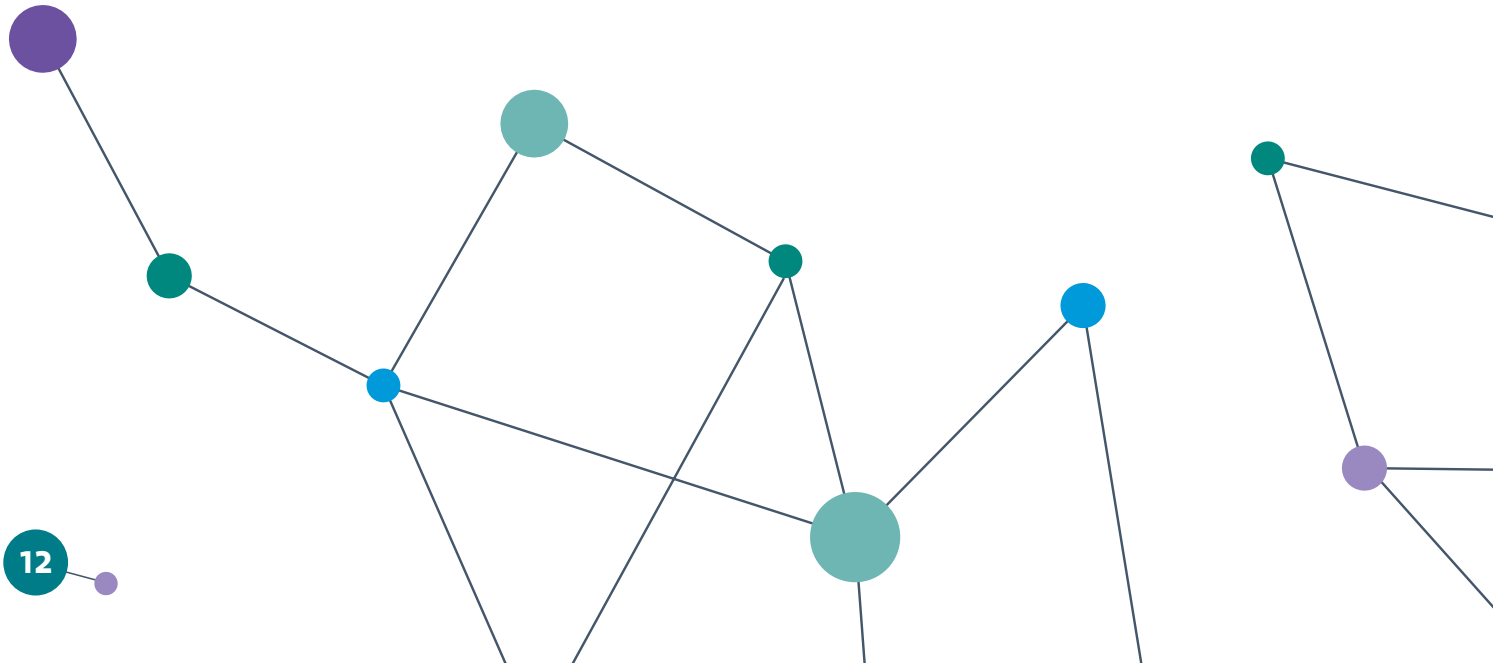
Although services were restored within a few hours, it was the extent of the attack that was cause for concern. Further investigation revealed that the incident was not isolated and that multiple electricity companies had been affected simultaneously. Similar malware had even been found in IT networks at Kiev's Boryspil Airport, including a network used for air traffic control. Ukraine blamed Russia for the incidents.

Later, the presence of Black Energy 3 malware was confirmed, as well as the fact that the power outages were caused by remote cyber intrusions at three regional electric power distribution companies. Three other organisations, some from other critical infrastructure sectors, experienced intrusions but were thankfully unaffected. The cyber-attack was synchronised and coordinated, following extensive reconnaissance of the victim networks.

Although this represents the first confirmed attack against the electric power grid, there has been much widely reported reconnaissance, such as the Havex malware of 2013 and 2014.

The Havex Trojan and Black Energy perpetrators have been described as 'sophisticated actors' by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). These actors have deep knowledge of industrial software and protocols, and advanced expertise in developing ICS malware for reconnaissance, compromise and potentially physical damage.

Physical losses are a growing concern in terms of severity and frequency. The new generation of control systems are based on openness and interoperability, and use open networking and commodity technologies. These expose organisations to a host of cyber security risks that are only just beginning to be understood.



The new generation of control systems are based on openness and interoperability... these expose organisations to a host of cyber security risks that are only just beginning to be understood.

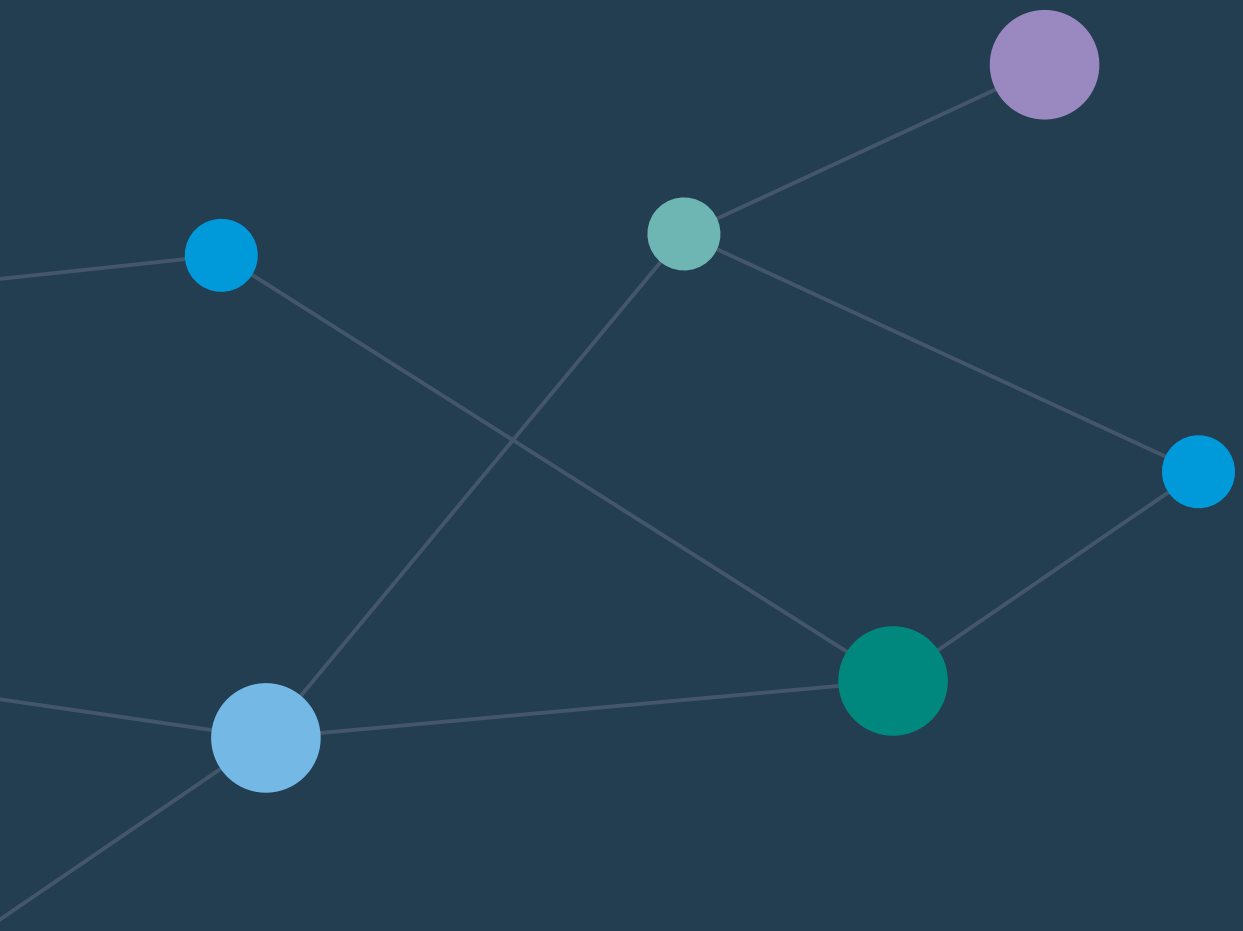
An example of a physical loss resulting from a cyber-attack occurred at a steel mill in Germany in December 2014. The attack used a sophisticated spear phishing and social engineering campaign to obtain initial access. The attackers then moved from the corporate to the production networks to locate and compromise the mill's industrial control systems. Over time, failures leading to the loss of plant control occurred. These ultimately caused the unscheduled shutdown of a blast furnace in an unsafe manner, resulting in extensive damage and loss of production.

That adversaries are becoming more knowledgeable and launching more sophisticated attacks in increasing numbers is a grave concern. The tools and techniques of nation states are now being increasingly used by organised crime.

Meanwhile, many companies use legacy systems running on old operating systems and control equipment with known vulnerabilities. This toxic combination has the potential for companies to incur legal liability and degrade their credit ratings and insurability, along with market valuations and mergers and acquisition attractiveness.

Ultimately, if severe attacks are actually realised, the consequences to organisations – in terms of human casualties, property loss, litigation, reputational damage and stock price plunges – could be overwhelming. This should galvanise boards to do all they can to ensure that their organisations will withstand the highly-sophisticated targeted cyber-attacks that are bound to come.

The 13 national infrastructure sectors defined by the UK Centre for the Protection of National Infrastructure



Cyber resilience challenges

A machine for living?

Andy Wall

Can a look back into the history of art and architecture teach us something about modern security and the human approach to securing infrastructure?

In the 1920s avant-garde international art and design brought a new, radical tenet: 'form follows function'. Walter Gropius and Bauhaus put architecture at the heart of design where practicality, purity of form and being true to the materials of construction were the foundations of their approach. Le Corbusier took this a stage further with his 'a house is a machine for living in'.

Ninety years later, with the Internet of Things connecting household appliances, smart meters and Internet-controlled heating systems, it's proving to be pretty accurate as predictions go. What happens in the home inevitably spreads into the office and then into industry.

There appear to be many parallels between the ideals of Gropius and Le Corbusier to our current concerns about securing infrastructure, particularly within critical national infrastructure environments. The fundamental unity underlying all branches of design that Gropius spoke of is our holistic security approach of today. Le Corbusier's efficient, productive and comfortable house-machines are our practical and appropriate security controls that keep the machine running.

Holistic security is an approach that does not focus on the traditional organisational or functional silos. A cross-cutting, multi-discipline approach where the underlying unity is brought out in design terms gives us a security version of 'form follows function' in a resilient way.

Interconnected critical national infrastructure is our industrial machine for working in - a 'system of systems'. Securing this from attack or failure is therefore not just a technical issue. Humans interface with control systems, even remote, automated ones, so personnel controls are needed – skills, training and screening clearances. Organisations need governance so we need management controls to keep this machine working – policies, procedures, audits and reviews.

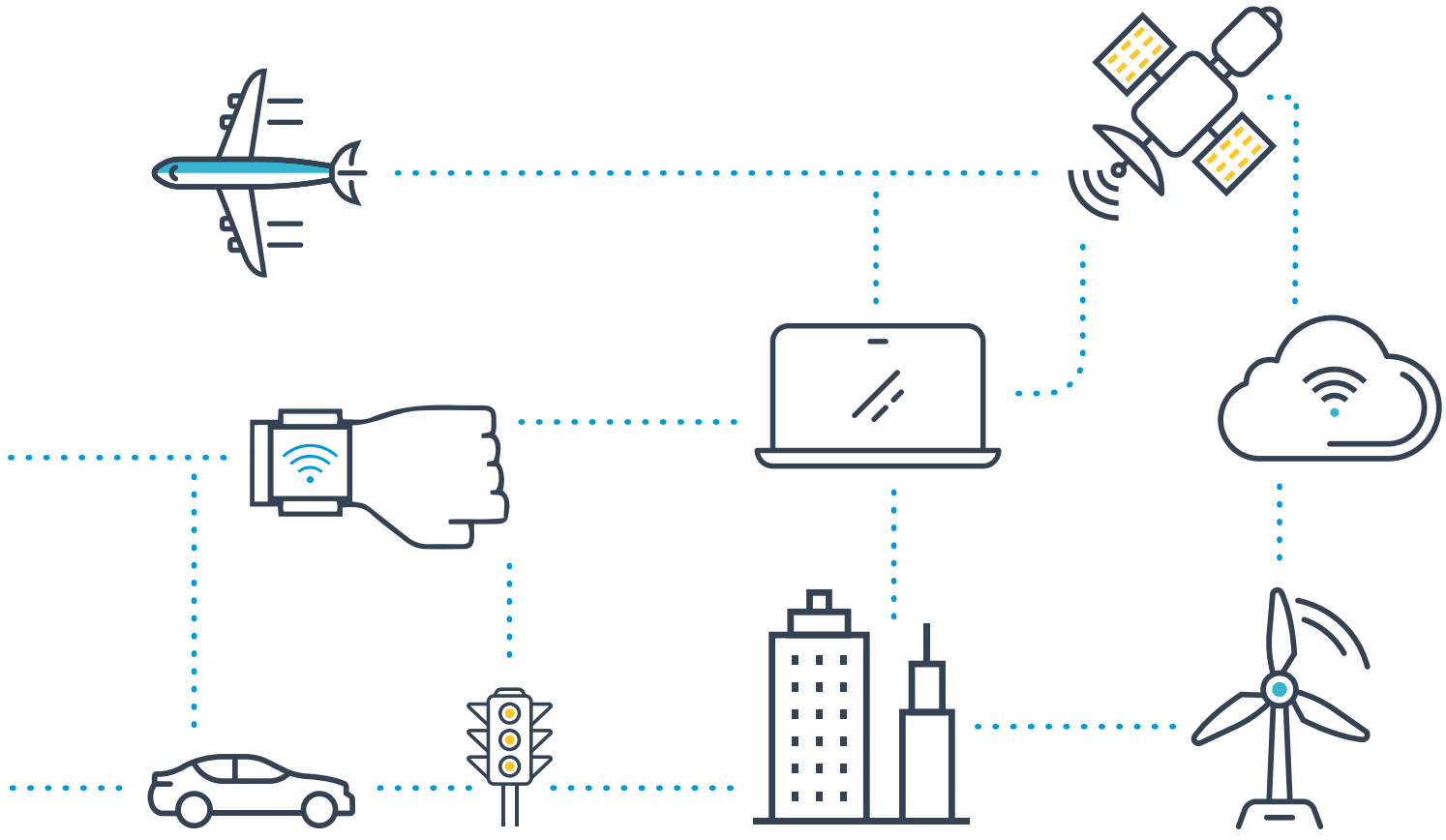
We should not over-engineer our security systems as that inevitably results in a more difficult and costly maintenance regime. We should instead design and implement only those controls we need to protect the assets that value, based on the threats to those assets.

All of these controls need to be integrated into our efficient and productive machine.

But, in an increasingly complicated infrastructure environment, the modernity and simplicity evangelised by Gropius and Le Corbusier is needed more than ever in security terms to protect the machine and keep it resilient. Very complex threat and operational environments, huge security product choice, competing vendors and contrasting professional views muddy the waters. As a result many organisations buy and implement a massive range of products, often without really understanding how these protect assets collectively. This is particularly true thanks to the proliferation of security, information and event management (SIEM), boundary, identity and malware tools.

Do these products, tools and elements all work together smoothly? How do they integrate into our systems beyond the technical? These are all tough challenges that we must overcome. We should not over-engineer our security systems as that inevitably results in a more difficult and costly maintenance regime. We should instead design and implement only those controls we need to protect the assets that value, based on the threats to those assets.

Without a holistic approach to bringing our different security regimes together, something is either duplicated or missing, and the resilience we seek won't exist - architecture needs to be at the heart of modern security design processes – just ask Gropius.



The realities of nuclear cyber security

Dr Richard Piggin & Dr Ian Buffey

How do civil nuclear power organisations approach cyber risk and what lessons could other critical national infrastructure organisations learn from their example?

By its very nature, the civil nuclear power industry is responsible for operating some of our most critical national infrastructure. Consequently it represents a compelling target for malicious cyber-attack. Of course, a single incident in the nuclear sector carries greater consequences than other sectors and therefore generates greater public concern.

However, what is less understood by the public is that the systems used to control industrial plant are not the same as those used for safety critical control. The latter tend to be isolated systems, with rigorous access control, monitoring and working practices, not purely dependent upon digital technology for protection.

Having had the opportunity to work with all of the existing UK nuclear power generators and nuclear new-build companies, it's our experience that these organisations are 'designing security in' and developing best practice technical solutions to tackle potential threats.

Last year Chatham House published a report - Cyber Security at Civil Nuclear Facilities: Understanding the Risks - which considered the major cyber threats to civil nuclear facilities. The report highlighted some key challenges for the global energy industry, which are just as relevant for other industrial sectors using control systems. These included:

Disclosure

Low levels of cyber incident disclosure, creating a false sense of security stifling appropriate security investment. However, full disclosure can lead to copying of tactics or techniques, thereby increasing risk.

Risk assessment

Unsuitable risk assessments can lead to insufficient spending on cyber security or the incorrect targeting of that spend. The issue of improving risk understanding at board level is a critical one. Our experience is that, in the UK, the nuclear industry is leading the adoption of good practice and boards are taking security and safety risk assessments very seriously. Integrating control system security and safety risk assessment and treatment is now a focus for good practice development and international standards committees.

The nuclear industry has traditionally focused on safety to provide resilience and security

Cultural challenges

Including the difficulty in communications between plant engineering (operational technology) and information technology personnel, addressing the need for greater appreciation of cyber security, training and skills development. We have seen that this human element is already being addressed in the nuclear industry, particularly the cultural aspects of integrating formerly disparate disciplines, as well as ensuring security roles and skills are developed to meet current and future needs.

Technical challenges

Including control systems which were not initially designed securely. Standard IT security approaches are often difficult to implement in plants, due to technical validation requirements, potential downtime and the commercial imperative to remain operational. Yet, these generic findings do not illustrate the secure design developments and practices being undertaken by the UK nuclear industry and the supply chain.

The Department for Business, Energy & Industrial Strategy is the first government body to launch a five year sector cyber security strategy. This sets expectations for industry, government, and regulators in light of increasing cyber threats and significant technological change. It's transformational, and has substantial implications for the nuclear sector, particularly in the supply chain.

The Civil Nuclear Cyber Security Strategy sets stretch goals, in consultation with industry, to address the risks to the safe and secure operation of new civil nuclear facilities and the management of legacy and waste facilities. Delivering this transformation will require greater understanding of the threat and focus upon outcomes as part of a holistic security posture. This work is already ongoing.

The nuclear industry has traditionally focused on safety to provide resilience and security. However, as the implementation of new operational technology potentially increases opportunities for malicious intent, more dynamic approaches are required to stay ahead of the continuously evolving cyber threat.

The strategy reinforces key themes essential to successful cyber security implementation; dealing with the increasing threat, board awareness, governance, OT and IT, and the interdependence of safety and security. Successful delivery will require all sector participants to be fully engaged, especially in the supply chain, and beyond the regulator's relationship with licensed nuclear sites. This will entail closer relationships with partnering companies, contractors and suppliers to provide the proportionate cascaded risk ownership, understanding and mitigation. The supply chain will also be called upon to develop capacity and capability where there are skills shortfalls.

No organisation or industry can afford to rest on their laurels when it comes to cyber resilience, especially those delivering critical national infrastructure. However, by considering these challenges, striking a careful balance between regulation and self-determined actions, and by recognising the need for risk-based approaches and innovation, the nuclear power industry will remain world-leading in its approach to addressing cyber security threats. Other sectors can learn from these developments, and some are already taking a keen interest.

Cyber vulnerabilities in the defence procurement lifecycle

John Connolly

What are the common cyber touch points throughout the defence procurement cycle and what can organisations within the supply chain do to manage these risks?

Military platforms are becoming more sophisticated, with each one now relying on supporting infrastructure and systems. Depending upon the missions they perform, they are also interacting with other platforms and combat systems on an almost constant basis. This increased level of sophistication can lead to a higher volume of cyber-attacks with even greater potential impact.

The defence procurement lifecycle has a variety of cyber 'touch points', as well as corresponding opportunities to implement practices and measures that ensure military systems are cyber resilient. At each point in the lifecycle different stakeholders will have primary responsibility for maintaining effective cyber security controls. Robust governance is therefore required to ensure that this is handled effectively.

A typical procurement lifecycle contains the following phases: Feasibility (or Concept and Assessment, as the MOD define it), Design, Manufacture, In-Service and Disposal.

Feasibility

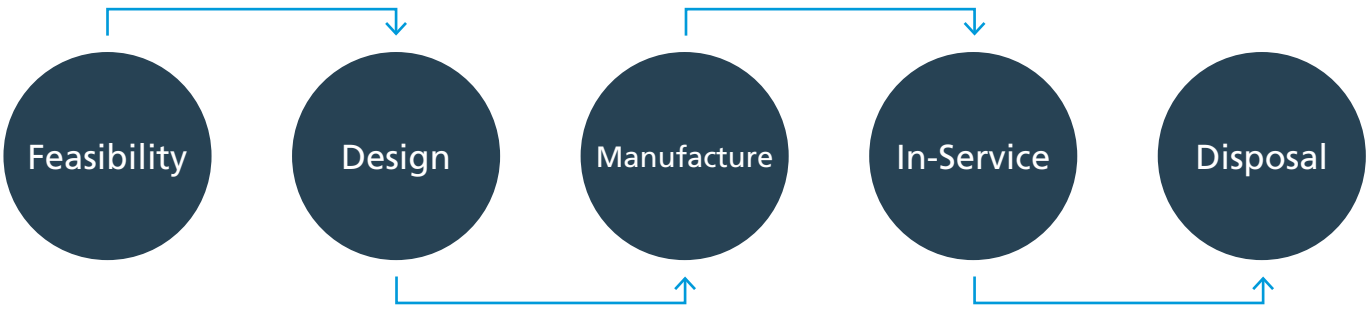
Potential cyber risk might include the compromise of initial concepts of operation, supplier details and/or strategic intent. Adversaries might also better position themselves to disrupt, influence or steal intellectual property (IP) as it develops during the late concept phases into the design phase. Military clients are particularly concerned about concepts of operation and desired performance characteristics being compromised. The ownership of the development risks from a cyber risk perspective is managed by the customer.

Design

In this phase the level of innovation and IP developed is at its highest. This information is not only vital to the customer but its loss could significantly damage the supplier. Other risks could result from the injection of vulnerabilities while in software development which may potentially leave the system open to attack during the In-Service phase. This is a concern for the customer, but given the contractual boundaries in place with the supplier, their direct influence is limited to assurance and accreditation processes.

Manufacture

The supply chain broadens and deepens to include manufacturers and service providers that may not have security at the forefront of their minds. These companies may hold sensitive environmental or contract information which, if compromised, could cause significant reputational damage throughout the supply chain. The primary responsibility for addressing the cyber supply chain risk lies with the prime supplier, while assurance and standards setting responsibilities remain with the customer.



In-Service

In this phase, any equipment or system in the procurement lifecycle is subjected to increasing levels of cyber-attack. These attacks might impact the asset's ability to perform its role, or even to be used as a 'lily pad' for more extensive attacks on other targets. In this phase the responsibility for countering the cyber risk has moved from the supplier to the customer, or more specifically the user. The supplier may at this point be a service provider for maintenance, training and/or warranties. They have a part to play in identifying and helping manage the cyber risks but are unlikely to do so unless adequately incentivised.

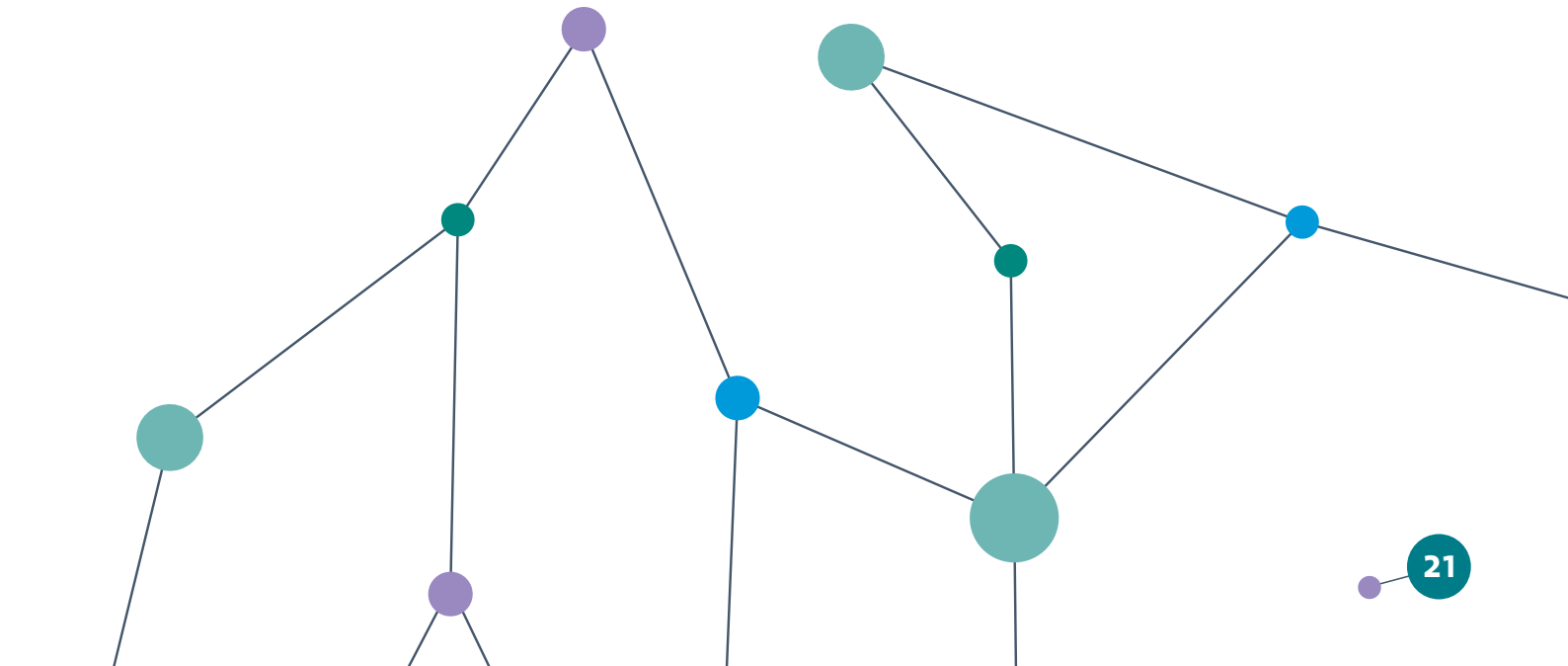
Disposal

While in the final phase of any equipment or systems lifecycle the disposal processes can pose potential risks. These systems often hold sensitive information, are based on innovative technologies or are subject to export controls (particularly with respect to military capabilities). There are a number of practices and processes that need to be adhered to, so that information is adequately safeguarded as systems are disposed of. The responsibility for managing the cyber risks in this final phase sits with the customer.

The supply chain for almost any procurement activity can be the target of cyber-attack; whether attacking the supply chain itself, the products developed, or the systems once integrated. While many of these attacks prove to be benign or are thwarted with simple security controls, more sophisticated attacks are often left undetected or unreported, creating the potential to be more damaging in the end products.

To counter this risk, defence supply chain organisations should embrace effective governance, adopt appropriate industry standards and good practice, undertake a maturity assessment and promote collaboration across the whole supply chain.

“The supply chain for almost any procurement activity can be the target of cyber-attack; whether attacking the supply chain itself, the products developed, or the systems once integrated.”



The end for off-grid automation?

Andy Wall

Connecting previously off-grid control systems to the network enables more efficient operations, but how does this impact operational risk?

Is the increasing automation of our transport systems a car crash waiting to happen, so to speak? Over the last few years we've had a growing awareness of the issues and risk associated with transferring human control to automated systems within intelligent mobility and transportation. The rail industry is replacing traditional mechanical signalling systems with computer networked systems, the vehicles we drive daily can almost drive themselves, and pilots can take a break mid-flight while the aeroplane handles the flying.

While there are clear benefits to this trend there are also significant concerns that need to be addressed. Humans make mistakes. We are, in fact, good at it. Automation has immeasurably improved our safety from the industrial revolution to the modern day as our technology has advanced and become more widespread. Automation also offers improved redundancy and considerable capacity enhancement for better exploitation of our transportation grids. Humans are also outward looking. What used to be employed in big industrial facilities in the 1970s is now commonplace in our home. The Internet has extended this reach even further.

For all the benefits of automation, there are also significant risks from the software logic itself. Many of us remember the shock of Air France Flight 447 where inconsistent flight speeds were being reported to on-board control systems resulting in the autopilot being turned off. This year the Google automated vehicle had its first crash blamed on its on-board control system. Decision-making software is clearly not infallible.

Is the increasing automation of our transport systems a car crash waiting to happen?

The challenges for good security design in on-line automated systems are immense but the key threats and risks can be mitigated.

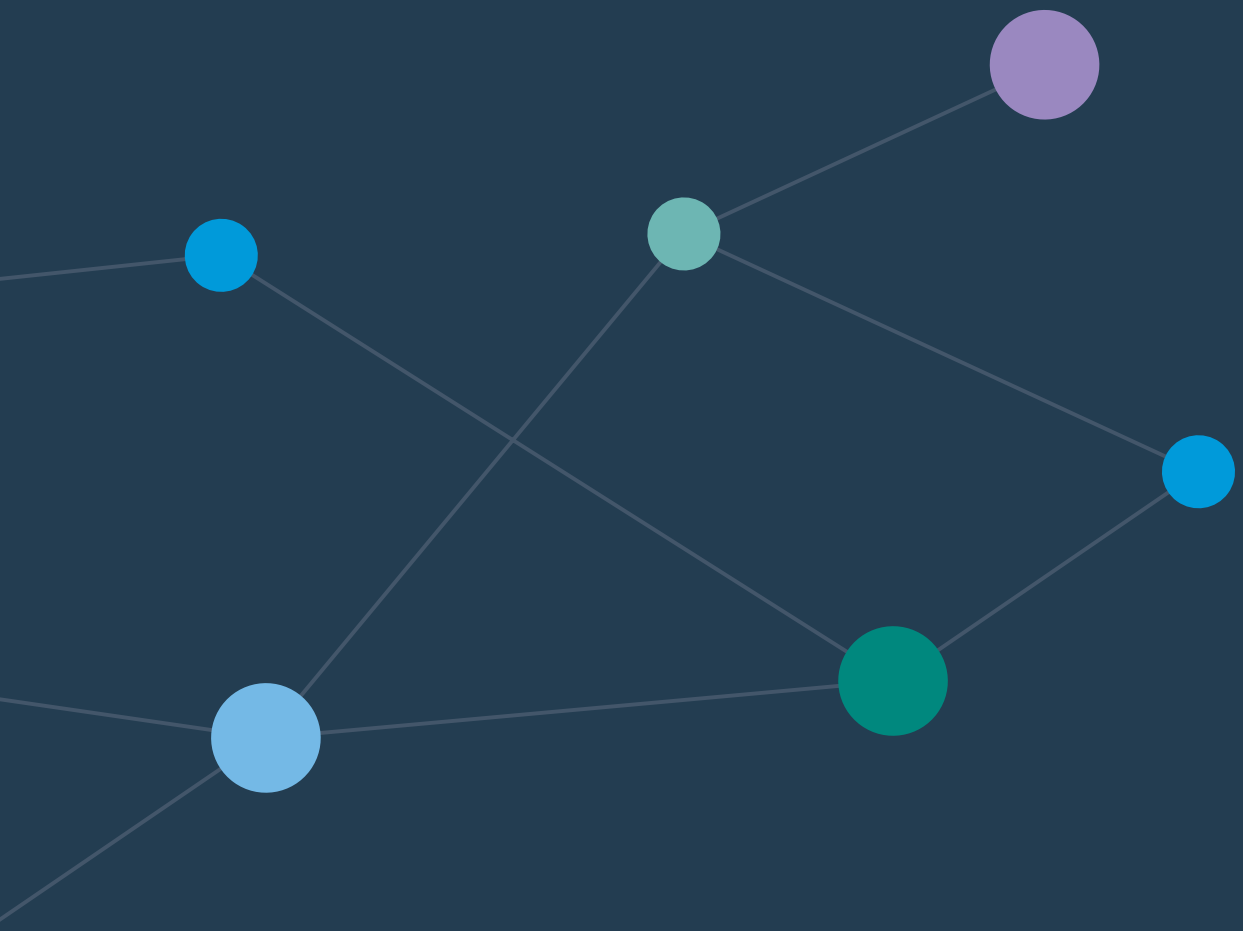
Furthermore, in connecting control systems to a computer network there are going to be risks of compromise as these networks themselves are likely to be connected to the Internet. There are many examples where this could be dangerous: connecting remote aging water treatment sites to networks opens up old control software to modern cyber-attack. The same applies for electricity substations, oil and gas platforms and many other utilities.

Malicious attack might come from a variety of sources, whether from hobbyist hackers, disaffected travellers, insiders or state-sponsored terrorists. New networked rail signalling technology raises fears that insiders can attack the system and cause an accident or major rail disruption. Interconnected and shared aircraft control and entertainment systems with ground communication links create the risk that aircraft can be brought down. Connected systems within road vehicles face the same problem. These attacks could be catastrophic. No sane person wants to see explosives packed into automated vehicles controlled by terrorists. Yet, as cyber testing across the world has shown, current automated vehicle designs are vulnerable to attack.

These concerns are why security is so important. Our inability to post on a social network, watch a TV programme or book a holiday is truly insignificant when compared with protecting human life. The challenges for good security design in on-line automated systems are immense but the key threats and risks can be mitigated. Good design lies at the heart of security and needs to consider technology, people and process.

There is, however, no going back. The benefits of controlling modern, or even aging, infrastructure outweigh the potential consequences but only if the risks are understood. Realistic threat and risk assessments are needed together with a programmatic approach to implement mitigations.

New networked rail signalling technology can open the system to potential attack



Cyber resilience in practice

What does good cyber security design look like?

Andy Wall

How do security professionals achieve effective cyber design and what factors impact our ability to build it into the heart of our organisations?

We have seen earlier in this report that business operations, and the technology that supports it, are increasing in complexity. Securing these operations is becoming more difficult, in no small part due to the continuing demand to create more modern, efficient and effective infrastructure.

What we therefore need is better design. Design that is undertaken up front and early in the process. We believe that existing industry approaches only go so far. As an organisation that designs and engineers some of the most complex infrastructure on the planet, we have some views on securing this – the security design challenge.

Technology and security professionals are used to designing technical approaches by using shapes on network maps and schematics – typically detailing many layers, boxes and connections. We adopt a different approach. Although we start with an idea and develop it into a detailed set of requirements, our approach is based on a different form, one which can address diverse levels of analysis, encompass an organisation's strategy and objectives, and focus on the people, processes and technology required to realise those objectives.

A fundamental aspect to this approach is our belief that security is probably misunderstood in many organisations. To us it is a process and not a product. It should exist to protect assets of value, meaning that it is a relative concept and has no intrinsic meaning outside the asset view. As an asset changes then so does the security around it based on organisational risk approaches.

If security design is so important what can hinder it? In our experience the key elements are:

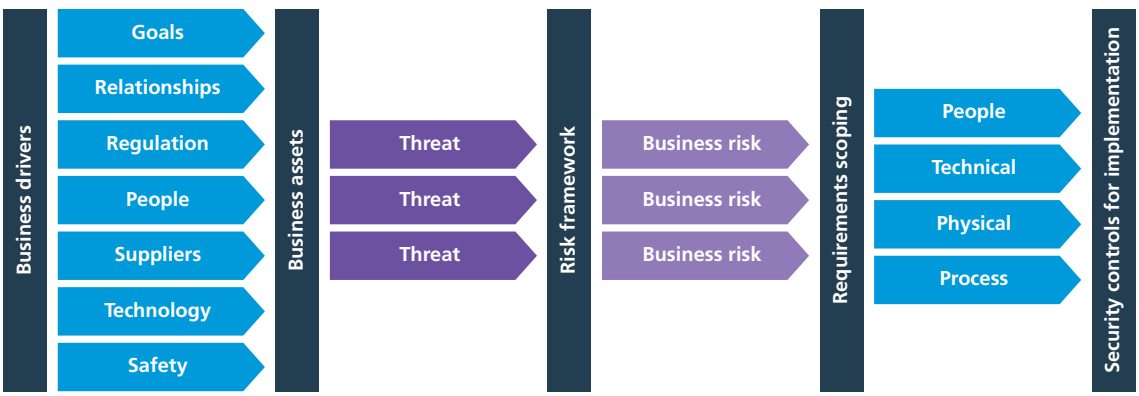
- A misunderstanding of the threat as a fixed 'thing' when it has many components – sources, agents, motivation, capability, resources – any of which can change at any time.
- Too much focus on technology that sits in organisational silos as the single solution to cyber. This inevitably leads to people and processes being overlooked, especially when most cyber incidents involve human error.
- Little common language across organisations. Despite the fact that 'security is everyone's responsibility', every industry, sector and technology is different. Just think of the same and different needs of information technology and operational technology.
- Cyber is borderless. It does not matter what country, organisational or functional boundaries exist, so security governance needs to span across these areas to avoid gaps in security posture.
- We have an unbalanced workforce. Yes there is a cyber skills shortage, but it's worse than that: the workforce is dominated by IT, yet we needs skills from across a business to provide for effective cyber e.g. business change, process analyst, human factors specialist; it's not all about technology.
- Over time the business and countermeasures lag behind technology and the threat. With this in mind we must ask ourselves 'is this a battle we can win?' This means organisations should decide what risks they are willing to accept.

So what does 'good' look like? Security needs to be built in at every stage of engineering design and fully aligned to business requirements. It is therefore about:

- Understanding the business goals and objectives.
- Determining the assets and their criticality to the business.
- Understanding the threats, risks and opportunities related to the business operations and assets.
- Developing the strategies, processes, mechanisms, standards and tools that will underpin the goals and risks.
- Developing the governance, management, roles and responsibilities that will underpin the processes and mechanisms.
- Understanding the geographies, sites, business units and infrastructure where security needs to be implemented.
- Understanding the business time aspects, calendars, processing schedules and sequences.

Design though is not a one-off activity. We can't pat ourselves on the back and walk away happy once it's delivered. Technology evolves, threats adapt and business needs change. Our designs need to evolve with this and security needs to be lived and operated – it should be the oil in the cogs of your machine.

This approach provides traceability from the business to the security requirements so that security controls exist to serve a specific business purpose:



Identifying the right cyber security standards for your supply chain

John Connolly

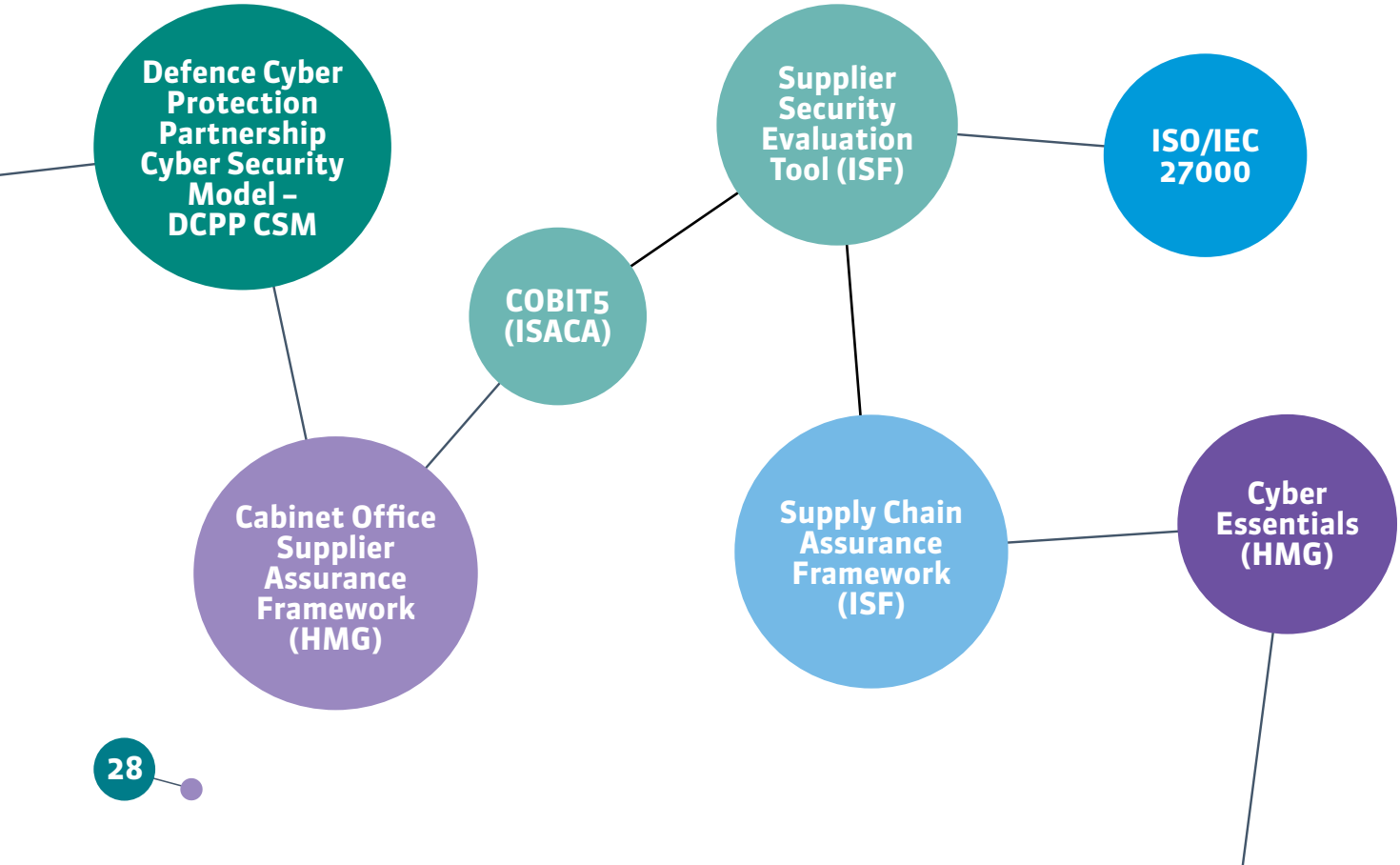
Which standards, policies and frameworks should be applied to an integrated supply chain to minimise cyber security risk?

A supply chain that does not have a clear set of standards to follow is likely to be fragmented and inconstant in its approach to cyber security. This may leave it open to attack through the weakest link.

Not all standards, or implementations, are the same. As a result, standards for specific industries and functions are needed. Some standards, such as information handling, are core and persistent in all phases while others only apply to one part of the lifecycle.

There are a number of common cyber security standards which are applicable to all industries, including those that are regulated. COBIT5 (ISACA), Cyber Essentials (HMG) and ISO/IEC 27000 are three popular ones applicable to any industry group. These provide organisational and information system controls that ensure information risks are managed appropriately.

A supply chain assurance framework, such as the one developed by the Information Security Forum (ISF), helps pull the variety of different standards in to a single framework. The benefits for a specific supply chain maturity model mean a customer could provide specific assessments for given types of procurement or as a precursor to any contracted supply arrangement.



However, introducing cyber supply chain risk management requires a level of understanding and co-operation. That understanding comes from a capability and maturity assessment. This scoring not only tells the buying authority and fellow suppliers the level of cyber competence but also gives it markers to improve and use cyber risk management as a competitive advantage. Supplier assessments, such as the ISF's Supplier Security Evaluation Tool (SSET), help organisations in a supply chain to evaluate who is strong or weak with respect to cyber security.

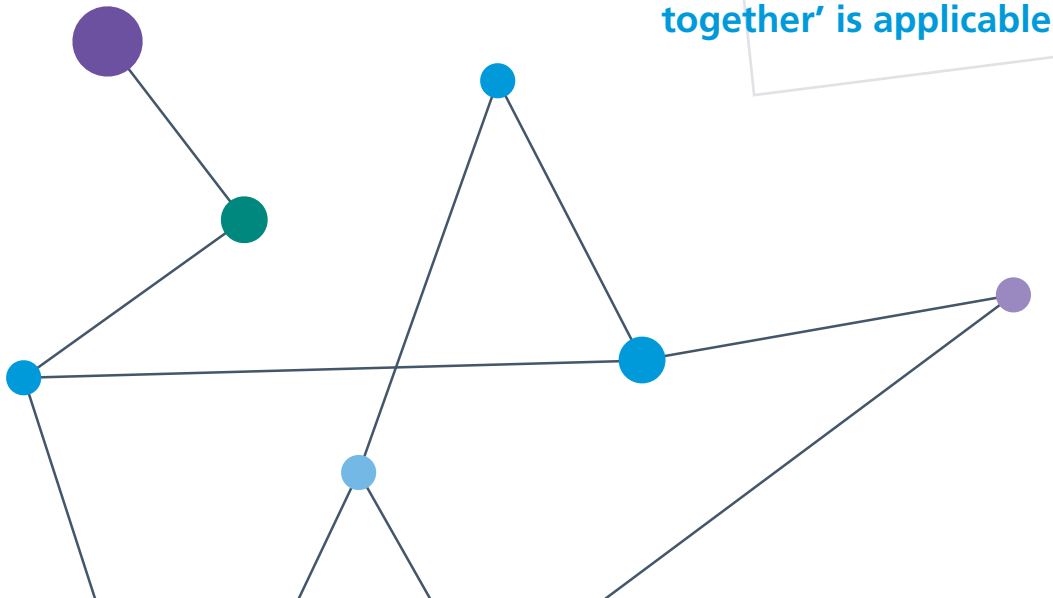
From a co-operation point of view, supply chain members need to be prepared to share their understanding of emerging threats and offer best practice ideas to strengthen collective capabilities. The old adage 'we are all in it together' is applicable here, as the threat from cyber-attack could come from any one supply chain member.

Capability and maturity assessments aid both the supplier in its self-improvement and the customer in the level of trust they hold in a given supplier. Maturity is not all about how an organisation complies with a standard but also how they learn and share experiences. Collaboration is a good way of improving how the organisation addresses the cyber risk, and through collective experience, that learning has the potential to be accelerated, increasing the maturity of the sector.

Maturity models exist across the cyber management space. Cyber Capability Maturity Model (C2M2) and ISF Maturity Model are two examples. However, these are not adaptable at each stage of the development lifecycle, meaning they won't effectively integrate with a supply chain. As such, blending the maturity assessment, standards and supply chain processes means cyber security is required to successfully embed the required culture, systems and structures of the supply chain members.

As the complexity of the supply chain increases, so does the probability of a significant cyber-attack. By using the right standard at the right time and undertaking a maturity assessment to feed a collaborative approach to improvement, these issues can be addressed at all stages of the development lifecycle.

Supply chain members need to be prepared to share their understanding of emerging threat and offer best practice ideas to strengthen collective capabilities. The old adage 'we are all in it together' is applicable here.



Organisational cyber resilience – the case for Defence

Chris Jones

How can Defence users and their suppliers become truly cyber resilient?

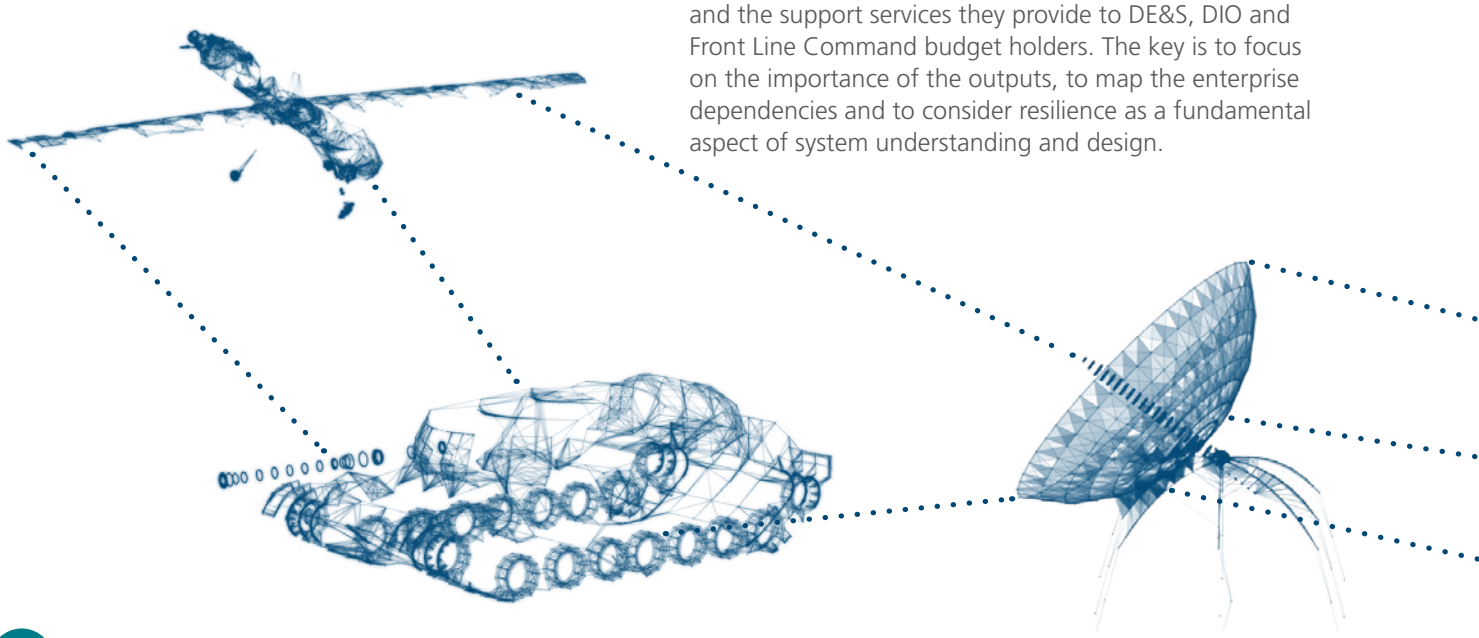
The Defence industry faces unprecedented challenges to the assurance of capabilities, products and systems in an increasingly digital world. Against a backdrop of growing threat sophistication, designers, suppliers and users need to acknowledge that their defences are not impervious and that a shift toward intrusion tolerance and mission assurance may offer the best return-on-investment. To unlock this return, a balance is required at the capability level between platform cyber security and system cyber resilience.

We know that the delivery of military capability requires the integration of inputs from across each of the Defence Lines of Development (DLODs): training, equipment, people, infrastructure, doctrine, organisation, information, logistics and interoperability. In the Information Age, countering and creating effects requires alignment and coordination across these DLODs to simultaneously exploit and protect the digital interdependencies that build the capability.

The Defence industry group Niteworks has stressed that this alignment, or 'capability coherence', occurs across the overlapping domains of strategy and finance; programmatic management; and operational and technical solutions. Cyber threats permeate each and the traditional platform and system security protection measures that rely on in-built redundancy, supported by reversionary or business continuity concepts, may therefore be insufficient. Resilience, seen in this sense as merely the response required to counter vulnerabilities, may be too narrow a definition.

Of course, it is not wrong to take a reactive standpoint that draws upon situational awareness and freedom of manoeuvre at the solution or platform level; particularly if this allows decision-making based on operational or business outputs. But, with increasing system complexity, there should be more emphasis on placing these elements within a more holistic or organisational approach across all the domains of coherence. This way cyber resilience can be designed-in from the outset to combine individual security investments at the technical, physical, people and process levels.

This can work as well for operational commanders and their warfighting capabilities, as it can for business leaders and the support services they provide to DE&S, DIO and Front Line Command budget holders. The key is to focus on the importance of the outputs, to map the enterprise dependencies and to consider resilience as a fundamental aspect of system understanding and design.



Defence requires particularly high standards of assurance due to the safety, security and mission criticality of the capabilities, within a complex, competitive and adversarial operating environment. Fortunately, advantage can be considered contextual (dependent upon the success criteria of the scenario), temporal (existing for long enough to succeed) and subjective (success determined by decision makers). If mission assurance is the desired outcome, consideration of these factors allows for a more agile response.

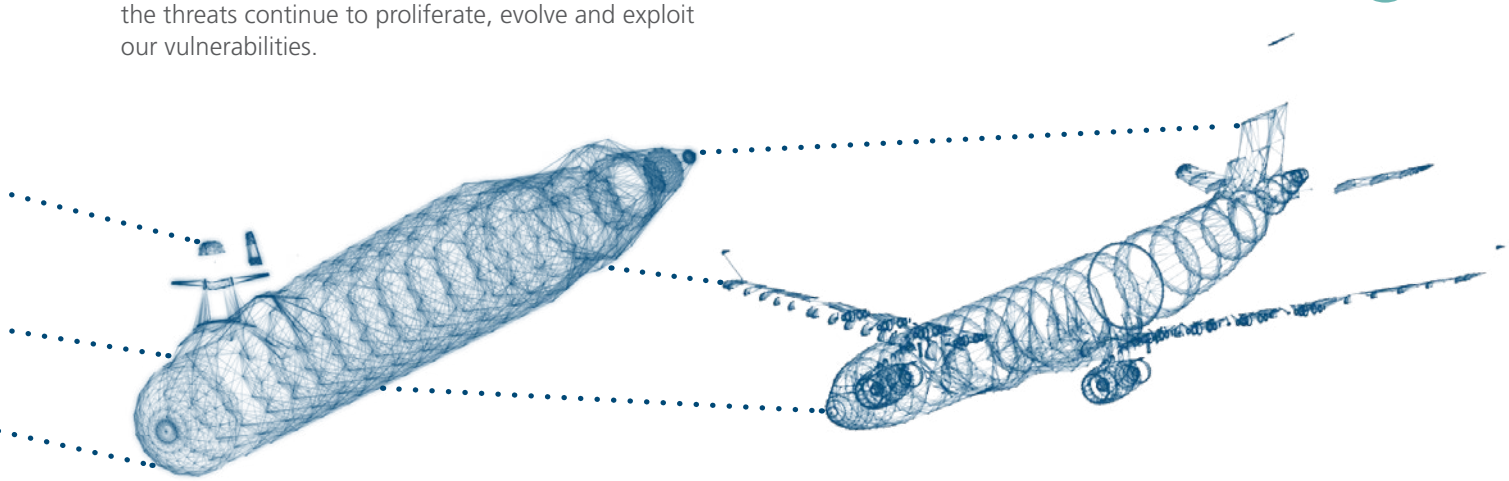
Ultimately, mission assurance is driven by commanders and business leaders who draw on the benefits that technical solutions can offer, and then make decisions on what is good enough. This is a risk-based approach that creates choice and alternatives (mitigations) through confidence in the visibility and assessment of threats and an understanding of the impact on the outputs that create advantage or success.

The concepts and challenges outlined here are magnified by the mission critical nature of Defence capability, but they are broadly replicated across critical national infrastructure (CNI). The risk is that Defence becomes fixated with platform cyber vulnerabilities as the input to addressing the threat. The utility, energy and transportation sectors focus more on the outputs required from the process, recognising that it is context-dependent, risk-based, system coherence that provides true cyber resilience. Taking too long to develop this viewpoint may put Defence too far behind the opposition as the threats continue to proliferate, evolve and exploit our vulnerabilities.

Lessons on resilience from CNI are important to Defence. Getting the right balance of systems engineering, holistic security, information assurance, risk management, programme controls, operational requirements and human factors places a responsibility on the platform OEMs, product suppliers and independent technical advisors to collaborate, not compete, on cyber resilience.

The cyber threats that our Defence capabilities face are so great, and the outputs of their mission so important, that this is not the time for any single part of the Defence enterprise to be 'marking their own cyber homework'. Mission assurance and intrusion tolerance demand an open-system approach to cyber resilience that may be uncomfortable for industry – but it is an absolute must in the delivery of the critical operational capabilities that keep the nation safe.

“Defence requires particularly high standards of assurance due to the safety, security and mission criticality of the capabilities, within a complex, competitive and adversarial operating environment.”



Implementing effective cyber resilience

Andy Wall

As the risk of cyber-attack against both critical national infrastructure and the defence supply chain grows, what can organisations do to help protect themselves and ensure that they are cyber resilient?

The key challenge for many organisations is understanding exactly what they need to protect – those assets that are most valuable to business operations. The security industry has a long history of focusing on technical issues and environments rather than on the business. Failing to understand the business' problems or talk their language, creates weaknesses in effective security.

Atkins offers a different approach, one that links and aligns security to the business through a stepped process: identify, assess, design, adopt and evolve.

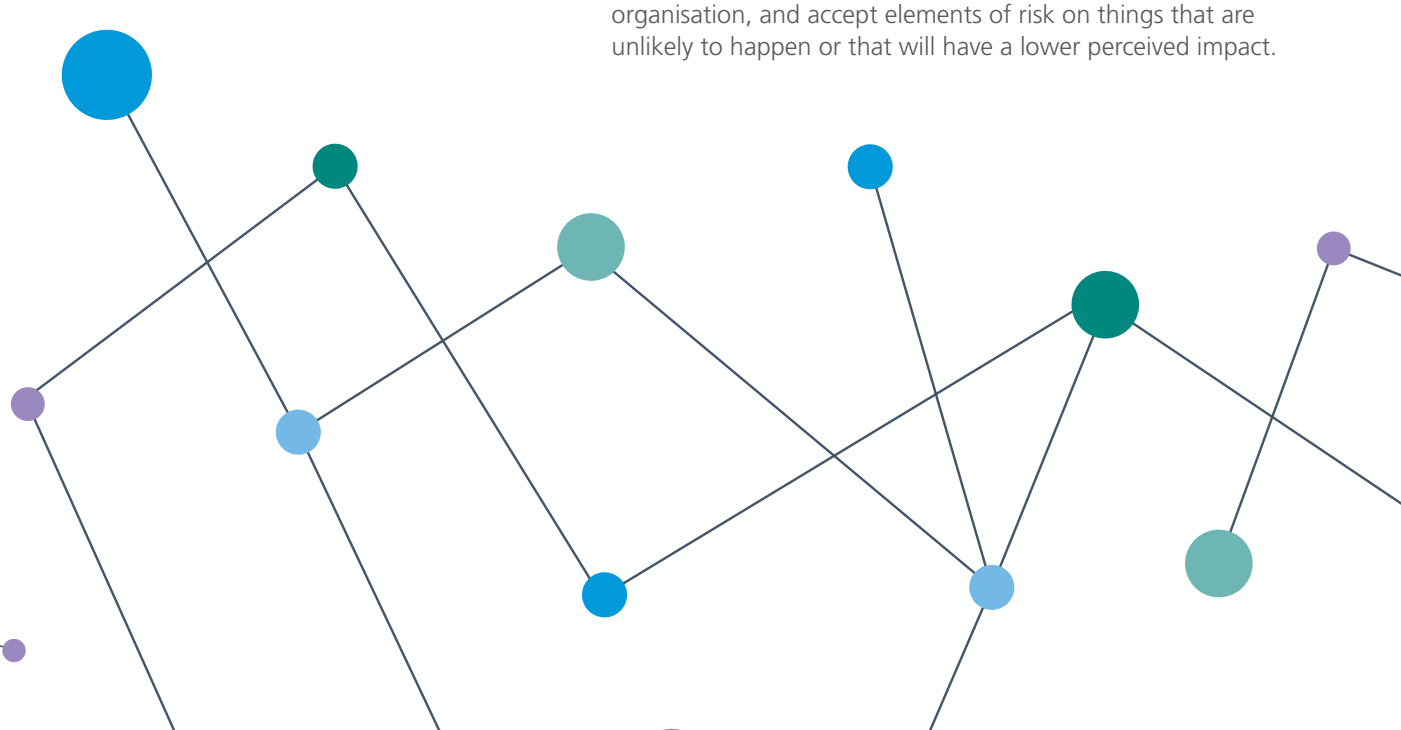
Identify

From the outset, your organisation should analyse its goals and drivers and then see how this translates into a security response. What security concerns keep your CEO awake at night? What do you understand about your assets and how critical are they to your operations? During this stage it's important to develop a common understanding of the business as a platform for a new cyber approach. In the majority of cases there will be a gap between what the business does and what security does.

Assess

Next comes the assessment process where you determine the maturity, or 'as-is' view, of the business from a cyber security perspective. This assessment can be measured against cyber security standards or industry best practice, depending on what is best for your culture and organisational style. From this assessment you will gain a better sense of your organisation's strengths and weaknesses, providing you with potential strategic direction for security investment.

You also need to understand your organisation's appetite for risk, particularly what the business is willing to tolerate as a loss or compromise. It's better to spend 80 per cent of your investment on the risks that are most important to your organisation, and accept elements of risk on things that are unlikely to happen or that will have a lower perceived impact.



Review

That then leads on to reviewing the threat environment that your organisation faces, as well as what can be done to mitigate that risk. Who are the most likely attackers and what will they be after? Armed with this information you can then plan your defence strategy against a realistic view of threat to really focus on what you want to do about it and where you should make any investment. This could be technical, people, process or physical.

Effective cyber security needs to build it in at every control stage, so it's not just an issue for IT or Security. HR will need to be engaged to screen staff during recruitment and your training team will need to keep raising security awareness across the organisation. People are the biggest security threat to a business, but also their greatest strength if they understand what they need to do and are encouraged to do it.

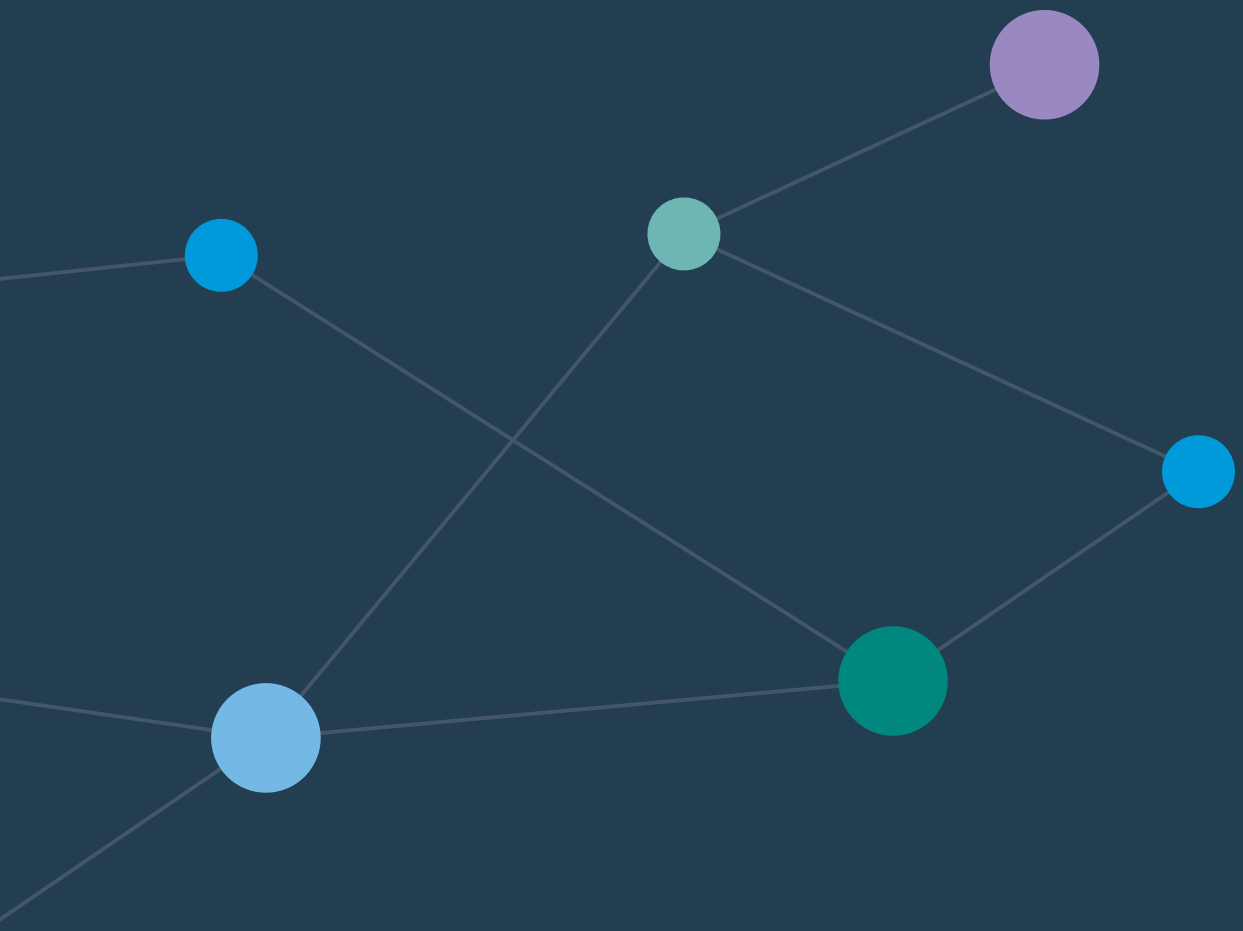
Adopt

Reviewing the outputs from the previous stages will then reveal what is missing to achieve your business objectives. This is then used to develop a programme of work aimed at securing critical assets, reducing the risk to your business.

Cyber security standards and the best practice you select allow you to make informed decisions about where to invest resources, where to realign organisational goals and processes, and what policies and procedures will support core missions and business functions.

Evolve

Once you've put your cyber resilience strategy in place, you can't rest on your laurels. Cyber attackers continually evolve their means and routes of attack. Therefore, an effective cyber strategy needs to be resilient and enable continuous improvement to meet this evolving threat.



Conclusion

The future of cyber resilience

Dr David Butler & Russell Cameron

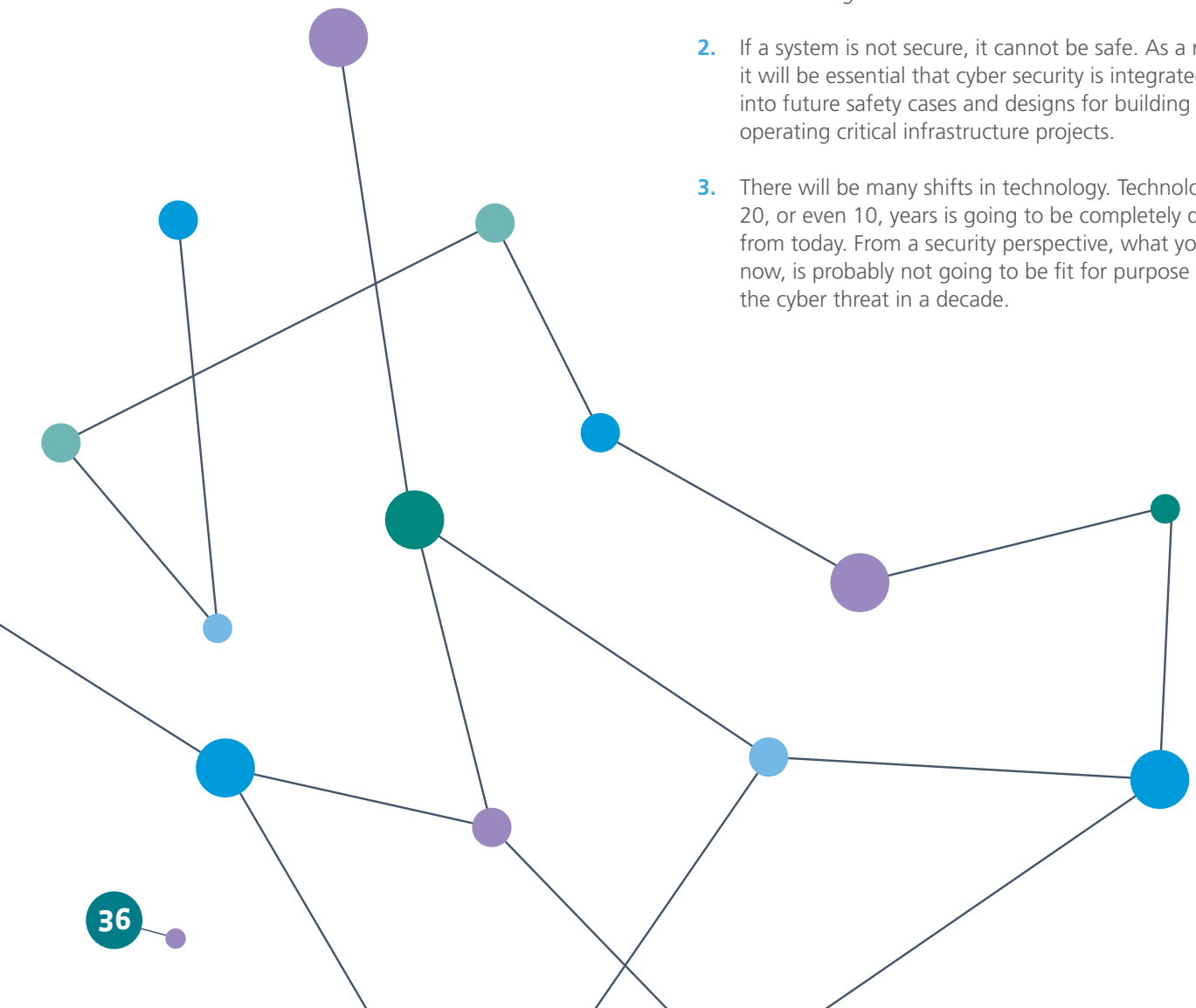
What will cyber resilience look like tomorrow, and how can organisations ensure they are future-proofed against an ever-evolving threat?

Each of the articles in this report outline the current threats organisations face, as well as approaches that can be adopted to mitigate them. But how will these threats change over time? While we cannot predict the future, we can imagine some of the key themes we should expect. These include:

1. Corporate and industrial control networks will continue to converge due to cost, flexibility and support requirements. Each of these benefits will need to be balanced against the potential security risks created by this convergence.

2. If a system is not secure, it cannot be safe. As a result it will be essential that cyber security is integrated into future safety cases and designs for building and operating critical infrastructure projects.

3. There will be many shifts in technology. Technology in 20, or even 10, years is going to be completely different from today. From a security perspective, what you design now, is probably not going to be fit for purpose against the cyber threat in a decade.

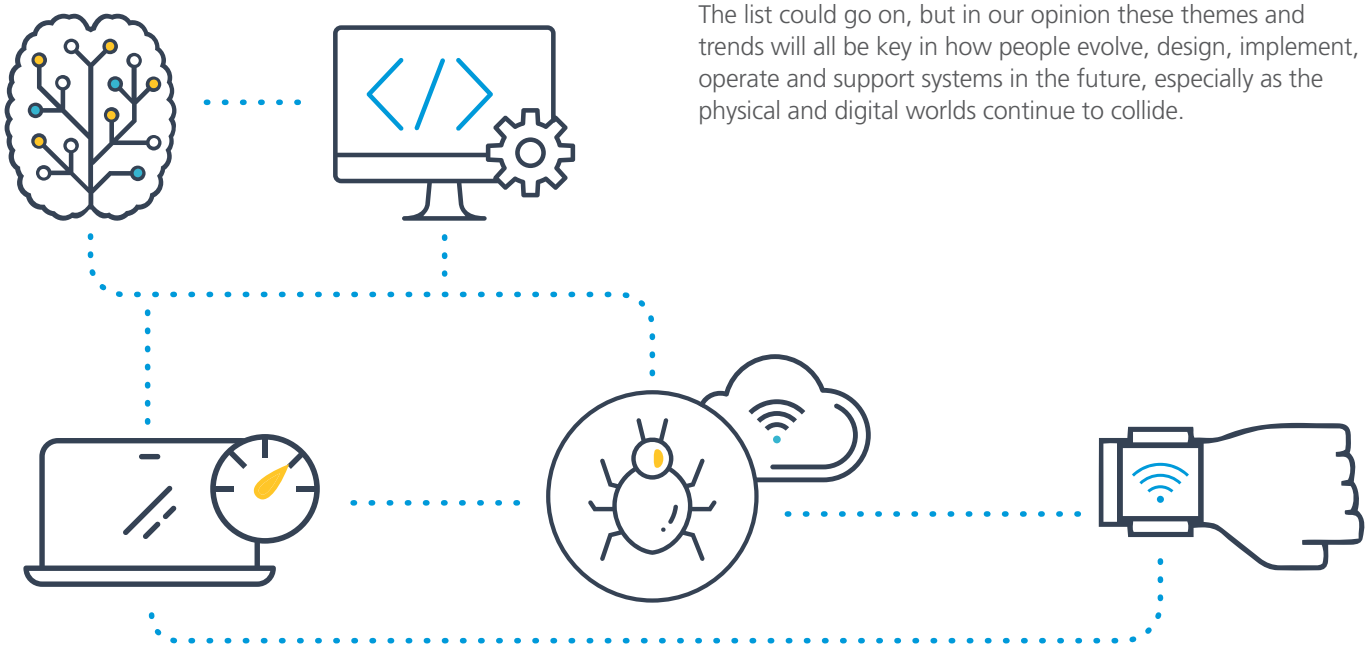


Examples of what the future cyber-threats may look like include:

- Access to cheap, or free, ubiquitous technology that will make it easy for a threat-actor to innovate and attack infrastructure.
- Artificial intelligence threat-actors that can be provided with some basic parameters and an end objective and just left to find ways in.
- Quantum computing will introduce a paradigm shift that will compromise the currently robust security offered by Public Key Infrastructure (PKI) encryption.
- Extensive penetration of mobile and wearable technologies that will make it nearly impossible to set up strong geographical 'security boundaries'.

4. The controversial view that the currently essential role of Chief Information Officer (CIO) will begin to decline as IT becomes fundamental to business operations and therefore intrinsic to other board roles. Conversely, due to greater awareness of the growing security threat, the role of Chief Information Security Officer (CISO) is on the rise.
5. The reality that, as a result of technological shifts, everyone will be 'hacked' at some stage. As a result we must be prepared and have proven plans in place to deal with this eventuality, both from an external and internal perspective.
6. That regardless of technological advances, the greatest strength and weakness in cyber protection will remain an organisation's people. As such, an increased focus on creating a better educated, more cyber-aware culture will be crucial. Key to this will be emphasising personal, rather than organisational, accountability to help drive the right behaviours.

The list could go on, but in our opinion these themes and trends will all be key in how people evolve, design, implement, operate and support systems in the future, especially as the physical and digital worlds continue to collide.



Closing words

Martin Chalmers

In this report we have outlined the realities and challenges facing organisations like yours seeking to defend themselves, and those who depend on them, in a digitally connected world.

As General Sir Richard Barrons observes, the threat to our critical national infrastructure, not just from criminals and terrorists but now from state actors, is growing. Through cyber-attack, an adversary can bring normal daily life to a halt. Vulnerability is increased by such trends as the connection to the web of hitherto off-grid operational technologies and the increasing complexity of supply chains, which may include organisations for whom cybersecurity is not a priority. The reality of the threat is demonstrated by the attacks in Ukraine and Germany described by Richard Piggin.

Andy Wall and our other contributors have vividly depicted the sweeping scope of the holistic response demanded by this challenge:

- covering all dimensions: technical, physical, people and process.
- considering security as an integral part of all stages from inception and design through to operation.
- ranging across the whole supply chain.
- embedding appropriate awareness at all levels of the organisation, from the board downwards.
- considering not just the prevention of attacks but also the response and recovery measures required to provide true resilience.

Based on our experience of working with all of the existing UK nuclear power generators and nuclear new-build companies, we have highlighted the nuclear industry as a leading exemplar in the breadth and depth of its approach to cyber security, reflecting an appreciation of its safety criticality on the part of both government and industry.

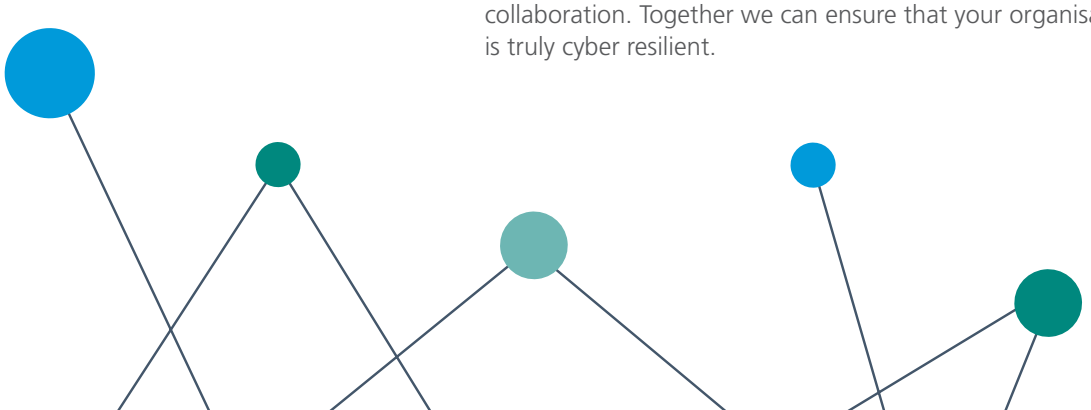
We have also provided an overview of the factors that organisations should consider in maximising the return on investment from cyber resilience. These include focusing investment on the right areas to protect your organisation's 'crown jewels' and developing agile approaches to cyber resilience that can evolve over time to keep pace with the ever-developing threat.

It is often difficult to look objectively across one's organisation to identify areas of weakness or potential vulnerability, to ask challenging questions regarding culture or working practices or to implement the changes required.

This is where advisers like Atkins can offer solutions and approaches to smooth the journey. We work in collaboration with our clients throughout the design and implementation of their cyber resilience strategies and offer assurance for live system service running.

Part of that assurance is to check that governance and risk management are optimally aligned with an organisation's needs and priorities. This will ensure that any investment made is used effectively and that the return on that investment, measured against agreed key performance indicators that reflect the nature and needs of the specific business, is maximised.

Leadership in our evolving digital world is essential, but so is collaboration. Together we can ensure that your organisation is truly cyber resilient.



Report Contributors

Andy Wall
Head of cyber security

Andy is a specialist advisor in security risk with over 25 years' experience in the industry. He has led and delivered multiple security projects in the UK, Europe and the Far East. Andy currently consults across UK Government and critical national infrastructure enterprises, architecting business-driven security solutions.

Chris Jones
Defence client director

Chris is a client director with Atkins, responsible for cyber security and resilience strategy in the Defence market. A retired Royal Air Force officer, he has many years of senior experience as an operator and capability manager in Defence intelligence and information systems. His current focus is on business growth and capability development in support of Atkins' digital enterprise propositions.

Daniel Gray
Report editor and PR manager

Daniel manages the public relations and thought leadership programme for Atkins' Aerospace, Defence, Security and Technology (ADS&T) division. He is a marketing and copywriting specialist who has served the aviation, defence, engineering, Government and IT sectors throughout his 17 year career.

Dr David Butler
Technology client director

David is our Aerospace, Defence, Security and Technology (ADS&T) divisional account director. He is responsible for cyber security and resilience business development in the transportation, utility, energy and private sector markets. Since 2001, David has worked in the ICT sector. His current focus is on business growth and capability development in support of Atkins' digital enterprise propositions. In addition, he is project director for several cyber programmes.

Dr Ian Buffey
Technical director

Ian is a technical director who has worked in the operational technology (OT) space for over 30 years, specialising in security since 2004. He has performed a wide range of roles from programming through to system architect and client-side advisor. Over his career, Ian has also worked exclusively on critical national infrastructure systems across a range of industries and is now focussed on helping those industries develop effective approaches to cyber resilience.

John Connolly
Principal consultant

John leads a team working with the Ministry of Defence to establish cyber vulnerability investigations as a core UK capability. He has almost 20 years of experience in designing and implementing security-centric solutions for clients, predominately in the defence, intelligence and security sectors. He fuses technology and business expertise to ensure clients at all levels obtain the best outcomes for their organisation while safeguarding information appropriately.

Martin Chalmers
Managing director, ADS&T

Martin is managing director of Atkins' 1000-strong Aerospace, Defence, Security and Technology (ADS&T) division. His priority is to ensure that ADS&T continues to harness its advanced engineering, digital and cyber, business consulting, and project management skills, in order to help clients address the opportunities and threats created by the convergence of the digital and physical worlds.

General Sir Richard Barrons KCB CBE
Former commander Joint Forces Command

General Sir Richard Barrons served as Commander Joint Forces Command, one of the six Chiefs of Staff leading the UK Armed Forces until April 2016. He was responsible for 23,000 people worldwide and a budget of £4.3 billion, delivering intelligence, Special Forces, operational command and control, information systems and communications, logistics, medical support, and advanced education and training across the Armed Forces.

His ambitions now are to be at the forefront of applying disruptive technology as it revolutionises business, society and government; to find a leading part in addressing the causes of instability, tension and conflict in a rapidly changing world; and to contribute to the continuing evolution of defence and security thinking worldwide.

Dr Richard Piggin
Principal security consultant

Richard is a principal consultant at Atkins. He has an Engineering Doctorate in industrial networking from the University of Warwick and has since focused on networking, technology evangelism, international standards, safety and security. At Atkins, Richard is working with clients to make their Operational Technology resilient against current and emerging threats.

Russell Cameron
Technology director

Russell leads Atkins' Technology Hub. This hub helps our clients to face the threats and opportunities created by the digital world, as well as to drive growth across our technology consulting, solutions, products and services. Russell is a mechanical engineer with over 30 years' experience in senior executive, project management, and consultancy roles. He previously led Atkins' Security and Intelligence business and also set up our security consultancy.

To keep up to date on our latest thought leadership, or to learn more about how we can help make your organisation more cyber resilient, please visit **www.atkinsglobal.com/cyber**

Glossary

Critical national infrastructure – (CNI) The assets, facilities, systems, networks or processes that support our way of life, and whose loss would have a detrimental effect on our nation. This infrastructure includes communications, utilities, power networks, public transport, and defence facilities.

Cyber-physical systems – Cyber-physical systems (CPS) interface the physical world with the logical, enabling the (Industrial) Internet of things, data and services.

Cyber physical system of systems – Cyber physical systems of systems are complex systems that feature partial autonomy. They interact with a large number of distributed computing devices to monitor, control and manage systems by exchanging information between CPS and users. E.g. transport systems, power plants, utilities, pipelines and manufacturing.

Cyber resilience – The ability of an organisation to understand the cyber threats its facing, to inform the known risks, to put in place proportionate protection, and to recover quickly from attack.

Defence (or military) platform – Term used by the Defence industry to describe a particular military asset. Examples of Defence platforms might include specific fighter jets, navy warships, aircraft carriers or armoured vehicles.

Enterprise Technology – Refers to the concept of information technology (IT) resources and data that are shared across an enterprise.

Governance – In a security context, refers to the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements.

Holistic security – The practice of approaching security as a whole, rather than as disparate strands e.g. physical, cyber and personnel security.

Industrial control systems – (Also known as Operational Technology or OT) The systems that control industrial and critical infrastructure. A general term that encompasses several types of control systems used in industrial sectors and critical infrastructure.

Industrial Internet of Things – The use of the Internet of Things (IoT) in an industrial capacity. Industrial IoT systems are bound by specific design functionality, and can therefore be distinguished from (non-Industrial) IoT ad hoc groupings of existing devices sharing data to fill an emergent requirement.

Information assurance – (IA) The practice of managing information-related risk.

Information technology – (IT) The hardware and software used by an organisation to manage and process information. Includes computers, networks, operating systems, databases, storage and servers.

Internet of Things – (IoT) The movement toward connecting physical devices – such as your car, fridge, home heating system, lighting, etc. – to the internet so that they can be controlled, monitored or supported remotely.

Operational technology – (OT) The hardware and software that controls or monitors the state of a physical system. See industrial control systems.

Security, information & event management – Software products and services that combine security information management and security event management. They provide consolidated real-time analysis and alerts of security events generated across the enterprise by network hardware and applications.

Supply chain – A system of organisations, people, activities, information, and resources involved in moving a product or service from supplier to customer.

System of systems – A collection of individual systems that, when interconnected, create a single, larger, more complex system.

Systems engineering – A field of engineering that focuses on how to design and manage complex engineering systems.

Acronyms

CNI – Critical national infrastructure
CPS – Cyber physical systems
CPSoS – Cyber physical systems of systems
IA – Information assurance
ICS – Industrial control systems
IIOT – Industrial internet of things
IOT or IoT – Internet of things
IT – Informational technology
OT – Operational technology
SIEM – Security, Information and Event Management

ATKINS

www.atkinsglobal.com/cyber