CYBER CITADEL

CYBER SECURITY IN THE LOGISTICS SECTOR

Implementing smart integration for smarter business growth

WHITE PAPER | 6 JULY 2022

CONTENTS

LOOKING BACK: CYBER CRIMINALITY IS STILL BIG BUSINESS

In our last white paper on the logistics industry, we focussed on the huge shift in the cybercrime landscape. The paper “The Threat to logistics: Preparing for a New Age of Cybercrime”[1] highlighted the new business-like approach criminal organisations are taking to implementing cyberattacks. We are in the age of the cybercrime marketplace: ransomware can be bought and sold as a service, cryptocurrency makes transactions virtually anonymous, and the dark web provides a ‘trading floor’ where buyers and sellers alike make their money in a shady business underworld.

Some of these landscape changes will be discussed again here, in the context of building a better community response, but it is highly recommended to read our previous paper to familiarise yourself with these concepts.

We also talked about how motivation could not be considered singular in this new business-like regime. The freelance hacker who breaches your network may have no specific motivation for attacking your company at all. More likely they are either looking to build their reputation within the hacking community, or they are looking to make money from selling their software or the data they exfiltrate on the dark web. The latest Verizon report, which analysed over 23,000 incidents and 5,000 breaches, backs this up: personal vendettas accounted for just 1% of all breaches to organisations[2]. Financial motivation however, accounted for 96%.

The question is, what motivates the buyer? This is also likely to be financial, but other motives might include political or industrial espionage, a protest or disagreement, or even just anarchic fun. Fun or curiosity actually accounted for 26% of breaches against larger organisations.

Network security enforcement & trust

At the time of our last white paper, a number of new legislations were being tabled worldwide. Of course, everyone is familiar with GDPR, and in 2020 guidance updates were published. But in addition to that, several regions in 2020 had begun operating a Notifiable Data Breaches (NDB) Scheme including Australia and New Zealand, and others had shiny new privacy acts awaiting passing into law. Most notable were the California Consumer Privacy Act and attempts by South Korea and Brazil to replicate GDPR-style legislation.

We also noted that industries themselves had begun increasing their minimum cyber-standards and data privacy requirements. This was being led by the International Maritime Organisation (IMO) and International Air Transport Association (IATA). Obtaining and maintaining trust is key in today’s world. Trust is severely lacking, whether it be business, politics, or even science, and it will be critical to companies wishing to be the premier operator that they strive to establish trust with their clients.

In this white paper we will once again review the latest in Data Privacy law and enforcement of network security, from both local and regional government as well as from industrial regulators. **We will focus on the relationship between different enforcement entities as well as their relationships with businesses** themselves, and how they can work together in mutually beneficial ways to create a more vigilant, more cybersecure community. We will also **emphasise the risk of cyberattacks to critical infrastructure,** which is high on the cyber security enforcement agenda of many nations, and the solution for which will rely heavily on **governments and regulator cooperation.**

[1] The Threat to the Logistics Industry - Cyber Citadel

[2] Verizon Data Breach Investigations Report, 2022: 2022 Data Breach Investigations Report | Verizon

Prevent cyberattacks for smarter business growth

Say “smart growth” to a business, and they will probably immediately think of new tech: implementing Internet of Things (IoT) devices, remote operations, AI-driven procedural improvements, the list goes on. But in our previous white paper we investigated how this type of growth was a double-edged sword and made businesses increasingly vulnerable to cyber-attacks. So, when we say “smart growth”, it would be better if businesses thought about growing *in a smart way*. Technology is amazing, and it can boost productivity, seek out new target markets, and improve safety. But it needs to be introduced and integrated in a careful, considered way.

We pointed out that the logistics sector has always been vulnerable, due to its reliance on digital communication, the gradual build-up of networks over many decades – which often encompass legacy technology – and the industry’s constant drive for automation and enhanced productivity. It’s also difficult to manage the cyber security of the workforce in the logistics sector. Staff are often transient: changing location, changing teams, working with different third-party providers. These all increase cyber risk and exemplify the importance of cyber-awareness training and cultivating good cyber practice.

In this report we will drive home the importance of ‘smart integration’. And we will place a spotlight on one of the biggest issues facing the logistics sector: **IT/OT convergence.** This is the integration of traditional operational technology (OT) – the physical machine world – with new Informational Technology – the digital world of communication and data processing. This integration of technologies is set to become the limiting factor of network security, and whilst the process will be gradual, businesses must get a handle on it before it speeds away and becomes a mess and a cause for serious security concern**. No one wants a hacker to not only be able to steal their data, but also start driving a train, or halt a manufacturing line.**

The picture of that cyber security landscape is not pretty.

Light at the end of the cyber security tunnel

If that all sounded bleak, readers should know that in the last white paper we did also discuss solutions. These centred around comprehensive risk management, the feasibility of zero-trust architecture, and implementing low-cost high-return solutions. Whilst it is the least eye-catching of the three, risk management is perhaps the most proactive, feasible, and cheap start to improving cyber security.

Risk management involves training staff, and it as true now as ever that individual error or social engineering play a significant role in a large fraction of data breaches – another statement the new Verizon report makes quite clear. Making staff more cyber aware *will* pay-off, whether they enjoy the

KEY DEFINITIONS

Cryptocurrency

A cryptocurrency, the most notable of which is Bitcoin, is a decentralised, trust-free currency that exists outside the control of any national government. Anyone can create a unique address from which they can send or receive the currency almost completely anonymously.

The Dark Web

The Dark Web is a (relatively) small network of websites which are not indexed by any search engine and can only be found if the user learns the web address from an existing user. These websites can then only be accessed using the Tor browser, which hides all information about the location or identity of users from the host and each other. This anonymity has been used to create numerous illegal marketplaces, where buyers can contract hackers, purchase stolen information and orchestrate the spread of malware. These marketplaces are very difficult to shut down even by law enforcement, as the locations of the hosting servers are not known, and the anonymised traffic to and from the website cannot easily be blocked by an internet service provider.

compulsory seminars or not. Popular training for the logistics sector is now readily available online from WiseTech Academy, for example this short course on preventing phishing attacks, and sessions are very affordable at just A$32.

Whilst our previous report highlights some excellent and affordable solutions, as well as further resources, **this report will consider a broader, more community-oriented solution.** That is not to say it is not worth reading for individual CEOs or smaller businesses. Far from it! Much like tackling climate change, it will be the collective contributions of individual businesses, regulatory bodies, and governments that will make cyberspace more secure for everyone. **An 'all for one, and one for all' scenario.**

THE CHANGING FACE OF REGULATION

The world lives with Covid, and the rapid changes to business that came with it. After 2 years, it is clear we won't be going back. Over this time, data storage, transmission, and availability have really come to the forefront of business problems (and solutions). Where many businesses previously ran on-site servers accessed via local networks or through web portals, the new world of remote working has seen a colossal shift towards cloud-based storage. Applications such as Google Drive and OneDrive from Microsoft now dominate the data storage market.

Cyber security has had to catch up fast. Now more than ever mitigations such as Multi-factor Authentication (MFA) are essential for keeping data safe. In addition, such globally accessible data makes staff credentials more valuable than gold. If a cybercriminal can obtain one high-ranking set of credentials, a whole cloud world is opened up to them.

The adoption of 5G, the shift to remote working and cloud computing, and the advent of IoT, are just some of the reasons cited by many governments as a driving factor for new cyber-related legislation. It is also interesting to see psychological reasons behind some government thinking. For example, the rapid rise of fake news, the general distrust of the public towards authority or expertise, and the use of fear – whether it be of Covid or something else – as a manipulative tool to initiate attacks. These types of strategies broadly fall into the category of social engineering and reached a recent peak in 2020[3].

[3] Verizon Data Breach Investigations Report, 2022

KEY DEFINITIONS

Credentials

These are a set of proofs of the identity or right of access for a user. Credentials may include a username, password, fingerprint, face scan, or one-time access code sent to a mobile phone.

Multi-Factor Authentication (MFA)

MFA is a security authentication method used to verify a user's identity by requiring two or more credentials. Only if users can successfully provide multiple sets of credentials are they then granted access to the computer or authentication system.

Many cloud-based services such as Office 365 now offer this as an easily activatable setting, making its roll-out both fast and simple.

Cloud Computing

The delivery of computing services such as storage, data processing, and server access over the internet, improving task speed, accessibility, and financial cost through the use of shared resources.

Cloud-based storage from providers such as Microsoft (OneDrive) and Google (Google Drive) are now incredibly popular, and both can enforce MFA.

SPOTLIGHT: NEW LEGISLATION

Worldwide

- 80% of countries now have some form of cybercrime legislation
- 71% of countries now have data privacy laws[4]
- African countries make a determined effort to improve cyber security laws with a second Africa Forum on Cybercrime
- The Brazilian Data Protection Law (LGPD) came into effect August 2020, and increased penalties for cybercriminals were introduced a year later

USA & Canada

- 35 states in the USA passed bills of or related to cyber security, cybercrime, or data privacy, with more in revision or pending final decisions[5]
- In June the Canadian government introduced the Act Respecting Cyber Security (ARCS) Bill, which also contained a Critical Cyber Systems Protection Act (CCSPA)[6]; long awaited legislation to bring Canadian security law into the 21st Century

Australia & New Zealand

- In Australia, the new Security Legislation Amendment (Critical Infrastructure Protection) or SLACIP Act came into force on 2nd April 2022[7]
- The Australian government is also considering legislative reforms in transport and logistics, captured in a new Transport Security Amendment (Critical Infrastructure) or TSACI Bill
- New Zealand is seeking to follow Australia in signing the Budapest Convention on Cybercrime, this will come with further enhancements to their cyber and data privacy laws

UK & Europe

- The UK leads with a Product Security and Telecoms Infrastructure (PSTI) Bill addressing the security of smart devices[8]
- The EU is set to revise their cyber security legislation in a Network and Information Systems (NIS) 2 Directive this year[9]
- As part of Digital Spain 2025, the government has introduced a Digital Rights Charter to propose a framework for future legislation

[4] United Nations Conference on Trade and Development (UNCTD) Global Cyberlaw Tracker
[5] National Conference of State Legislature (NCSL)
[6] Public Safety Canada
[7] Australian Cyber Security Centre
[8] National Cyber Security Centre, UK
[9] The Law Reviews

Changes to the law

The USA has made huge steps forward from a former position of relatively few cyber security, cybercrime, and data privacy laws. This is likely due to the terrifying recent attacks on government systems and critical infrastructure, such as the SolarWinds hack which affected public and private systems alike and the Colonial fuel pipeline attack which breached the IT network but caused significant operational downtime.

Incidents such as these also highlight the growing need for both corporate businesses and government agencies to work together to not only try and prevent cyber-attacks but also respond to them when they happen. The attack on the fuel pipeline was obviously disastrous for the company who own and manage it, but equally it had a real effect on the US economy.

These huge steps forward included the consideration of over 250 bills or resolutions across the country. From requiring agencies to implement cyber training, to formalising security standards and practices, to regulating cyber security within the insurance industry. The bills covered an enormous range of measures seeking to comprehensively improve the cyber security outlook of the public and private sectors.

Any businesses trading or looking to trade within the USA should make a point of familiarising themselves with the array of new legislature which differs state-by-state.

Another poignant example of attacks affecting both private and public sectors was the attack on the New Zealand Exchange (NZX). This basic Denial of Service (DoS) hack inhibited trading for hours and resulted in an initial fall in the NZX 50 index by 0.24%. Whilst the attack did not affect public systems directly, a fall in stock exchange index values has real implications on national economies and the confidence investors have in a domestic market.

Again it highlights the **growing need for different sectors, regulators, and specialists to work together.** Especially when a crisis hits.

Australia has introduced two new bills this year, both target critical infrastructure. The first, which came into force on the 2nd of April this year, is the Security Legislation Amendment (Critical Infrastructure Protection) or SLACIP Act.

The legislation amends the 2018 act by introducing a new obligation for responsible entities to create and maintain a critical infrastructure and risk management program, as well as new enhanced cyber security obligations for operators of systems of national significance[10].

KEY DEFINITIONS

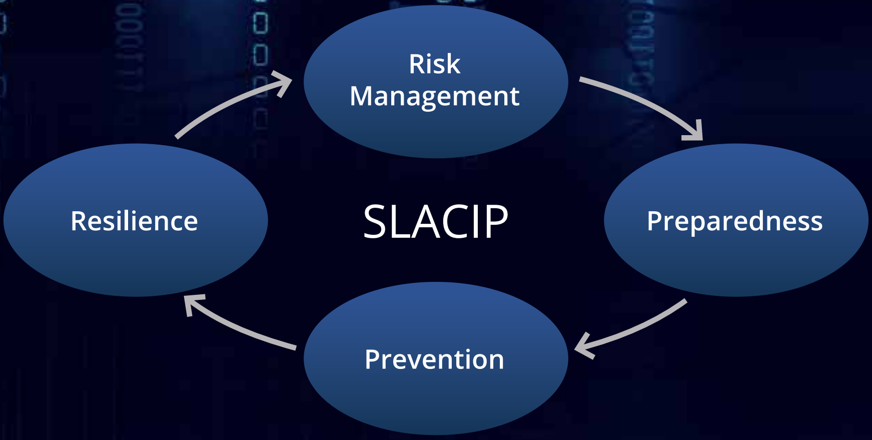
Internet of Things (IoT)

Any device connected in some way to the internet is an IoT device. They are not always obviously computers, and may be thermostats, speakers, smart watches, lights, or other automatic machinery. Many companies employ IoT to run manufacturing processes or transport remotely, and many individuals who own personal IoT devices connect them (intentionally or not) to various private and public networks. They are often exploitable by cybercriminals as weakly defended access points to connected networks.

Social Engineering

A strategy for cyberattacks which uses human interaction to engineer a network vulnerability. It is principally psychological manipulation designed to cause security lapses or obtain sensitive information such as access credentials as result of human error. This approach is much more targeted than spear phishing, and usually involves gathering background information on a victim and using this as part of the deception.

[10] Australian Government Department of Home Affairs



The act also enables the government to assist in the case of an emergency cyber security incident affecting critical infrastructure or systems of national significance (SONS). This means that the government will be able to gather information related to the incident as well as direct actions for the affected entity. In the majority of cases the entity is expected to have sufficient security in place to carry out these actions and readily comply. In rare cases, the government may authorise the Australian Signals Directorate (ASD) to intervene, which gives them the power to provide specified assistance including installing or modifying systems and programs, and altering or deleting data.

Such emergency powers have been the subject of extensive debate. A number of factsheets have been issued to assist with entities understanding their obligations with respect to the new act, these can be found here[11].

The second bill, which is currently still being debated and revised as part of a co-design process between industrial and regulatory contributors, is the Transport Security Amendment (Critical Infrastructure) or TSACI Bill. This bill is specifically aimed at the logistics and transport sectors and is a set of amendments to the previous Aviation Transport Security Act (2004) and Maritime Transport and Offshore Facilities Act (2003). The main aim is to expand the regulatory framework to include all hazards where currently the focus is just on unlawful interference, typically characterised as acts of terrorism which risk the physical safety of goods, people, and infrastructure[12]. **The new 'All Hazards Framework' will include all relevant operational interference, physical or otherwise**; the new categories of hazard are summarised in the schematic.

In addition, the bill seeks to establish **mandatory reporting of cyber security incidents for all industry participants** and will enable authorities at the Department of Home Affairs to declare some of these participants as 'critical'. It also intends to build on the SLACIP Act by introducing security risk assessments as part of security or risk management programs. Participants will also be obliged to periodically **confirm the validity of their assessments and programs**.

Further legal updates are highlighted in the Spotlight section 'New Legislation', and details of these can be found within the references. We want to bring to attention one final bill, which is the new UK Product Security and Telecoms Infrastructure (PSTI) Bill. The reason for singling this out is that it is one of the first pieces of legislation to specifically address the issue of IoT devices in the context of critical infrastructure. It is based on a 13-point code of practice for consumer IoT security, originally drawn up

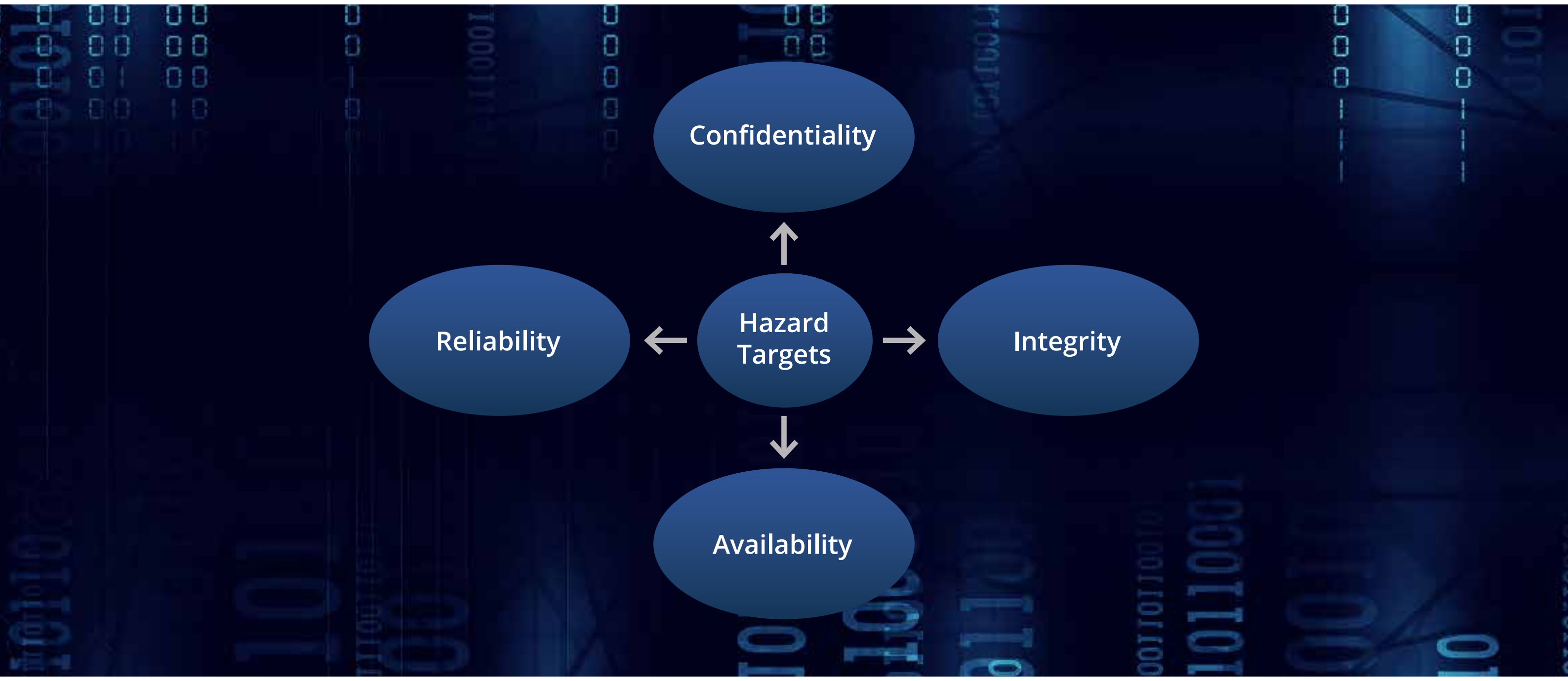
[11] www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022
[12] Australian Government Department of Home Affairs

in 2018, but this new bill goes beyond the consumer and also addresses issues within the telecoms industry too.

The motivation behind this bill is likely the rapid rise in the use of IoT in the UK; Deloitte released research claiming that a fifth of consumers bought a new digital device during Covid lockdowns[13]. And as we have discussed, as more business strive towards automation, the number of connected devices in industry is only set to rise. IoT devices are not only growing in number, but also growing in risk level to businesses. An introductory discussion to this issue can be found here[14].

The key proposals and compliance conditions are outlined below. Critically, **all members and components of a supply chain will have a duty of care and diligence** and will be expected to report on security failures to the relevant authority and take steps to minimise the risk and remedy the failure. A regulatory body, which is yet to be decided upon, will be set up to enforce the new regulations and issue penalties for failure to comply[15].This new legislation will be ahead of the trend in addressing the growing threat of IoT devices. The USA has also recently passed an IoT Cybersecurity Improvement Act (2020)[16], which focusses on security by design. In their case, the National Institute of Standards and Technology (NIST) is the regulatory body which must set and monitors standards for smart devices. An overview of the NIST Cyber Security Framework (CSF 1.1) is covered in this video. The act however has received criticism for its interpretable wording, and we shall see how the new regulations play out[17].

We expect other regions, in particular the EU, to follow suit in either creating similar legislation or updating existing law to include specific clauses regarding IoT.



[13] www2.deloitte.com/uk/en/pages/press-releases/articles/uk-adults-purchased-up-to-21-million-new-digital-devices-during-lockdown-in-desire-to-stay-connected.html

[14] www.cybercitadel.com/what-the-internet-of-things-iot-means-for-cybersecurity-of-the-logistics-industry/

[15] New smart devices cyber security laws one step closer - GOV.UK (www.gov.uk)

[16] The Library of Congress, USA

[17] IoT Cybersecurity Improvement Act Signed Into Law: New Security Requirements for Federal Government Devices - CPO Magazine

Key Proposals

- A prohibition of marketing devices with easy-to-guess default passwords, and an inability to reset passwords to factory default
- A mandatory vulnerability disclosure for IoT products, with a procedure for the public to report on security issues
- Transparency and communication between manufacturers and consumers regarding the provision of security updates and support

Compliance

- Companies will have to ensure their supply chain (e.g. manufacturers) also meet the requirements of the bill
- Companies will also have to produce validity statements to prove their compliance with the requirements
- The regulator will have the power to issue fines up to £10 million or 4% of a company's annual turnover for non-compliance; they will also be able to demand product recall or halt sales

Changes to industry standards

In addition to rapidly changing legislation, industrial regulators are also ramping up their cyber security guidelines and standards. Most notable to the logistics industry are the new International Maritime Organisation (IMO) 2021 Cybersecurity Regulations, the key points of which are provided in the spotlight section 'Industry Enforcement'. Much of these regulations were postulated in 2017, but the guidelines are continuously appended to, and there was focus on on-board security in the latest resolution.

The International Air Transport Association (IATA) also released their latest incarnation of cybersecurity standards at the end of 2021. The focus of these is on standardisation across the sector, **making cybersecurity a regular part of security risk assessment** and review. Finally, we spotlight the new Australian Energy Sector Cyber Security Framework (AESCSF) developed by the Australian Energy Market Operator (AEMO).

The risk of cyberattacks on critical infrastructure is exemplified in Ukraine, where the power grid was hacked in 2015 causing power cuts to around 230,000 customers and then again, a year later resulting in about 20% power loss to the capital[18]. There was another attempt this year to target one of the largest energy providers, but fortunately it was prevented. Predictions suggested some 2 million people may have been left without power if the hack had succeeded.

This exhibits the **increasing need for governments to work with sector regulators and operators to develop cyber security frameworks and protect critical infrastructure.**

[18] Ukraine power cut 'was cyber-attack' - BBC News

SPOTLIGHT: INDUSTRY ENFORCEMENT

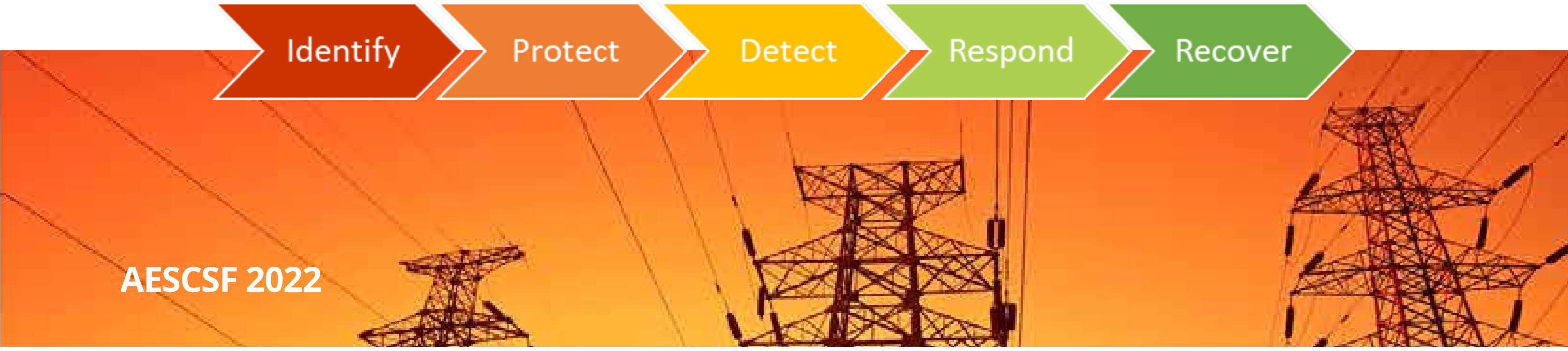
IMO 2021 Cybersecurity Regulations

Aim: support safe and secure shipping, which is operationally resilient to cyber risks.

Requirement: the new resolution makes cyber security part of the safety management system requirements set out by the International Safety Management (ISM) Code which almost every vessel is bound to.

Compliance: all internationally sailing vessels will be subject to the new regulations because of the SOLAS convention signed by 150 nation states. Port operators will not strictly be bound by the new resolutions, but ship operators are likely to show increasing reluctance to work with ports which do not comply.

Summary: the published guidelines are broadly based on the NIST CSF 1.1[19], and address the three areas of vulnerability – people, process, technology. The ISM code requires entities to **assess** their risks to ships and operations, **design** a risk management program and secure network architecture, and use safeguards to **protect** their infrastructure and ensure resilience. The NIST CSF helps to break this down further, providing real, implementable strategies to address each component that makes up a secure network.



AESCSF 2022

Aim: to protect the Australian energy sector (Gas, Electricity, and, as of 2022, Liquid Fuels) through the implementation of standards based on industry frameworks such as NIST, but with Australian-specific references such as the ASD Essential 8, the Australian Privacy Principles, and the Notifiable Data Breaches scheme. The framework enables organisations to assess, evaluate, prioritise, and improve cybersecurity with the aim of strengthening the resilience of Australian critical infrastructure as a whole.

Requirements and Compliance: the scheme is entirely voluntary but is designed to help entities responsible for critical infrastructure to test whether their current cyber security meets the standards required under the Critical Infrastructure and Systems of National Significance (CI SONS) regulatory reforms.

Summary: AESCSF divides security into domains: Enterprise, Operating Environment, and External Parties. **Enterprise is people and process** oriented and looks at risk and security program management as well as workforce management. Operating environment looks at issues such as **identity and access** management, **incident response, vulnerability and privacy** management, and **situational awareness**. Finally, External Parties focuses on supply chain vulnerabilities, and **the risks involved with informational sharing, communication, and the management of external dependencies**. Much more can be found in this informative Education Workshop Pack[20] released by AEMO.

[19] https://www.nist.gov/cyberframework

[20] https://aemo.com.au/-/media/files/initiatives/cyber-security/aescsf/aescsf-education-workshop-pack.pdf?la=en

INCREASING COMPLEXITY INCREASES RISK

Another major driver for updating legislation is the rapid evolution of supply chains. Compared to even 10 years ago, industrial supply chains are unrecognisable. It is obvious why businesses want to increase automation: consistency, increased efficiency, reduced overheads, and decreased quality control time. But concomitant with these benefits is an increase in supply chain complexity. **Increased complexity brings increased cyber risk.** In the last year, supply chain attacks have quadrupled[21].

As we've already discussed, automation is often achieved with the use of IoT, which introduce exploitable vulnerabilities into networks. Many IoT devices have been poorly regulated at the manufacturing level and suffer from a lack of security by design and undeclared loss of security support.

Until the necessary legislation comes into effect, businesses need to independently consider their IoT devices and manufacturers carefully. Changing default passwords, which is the first point of the UK's new legislation, is an obvious but crucial procedure and should be done immediately.

IT/OT convergence

Related to the issues of IoT security is **IT/OT convergence**. As previously described, this is the integration of Information Technology (IT) – everything we traditionally think of when it comes to digital networks – with Operational Technology (OT), which is everything we think of as real, physical devices. **IT is the realm of data storage and analysis. OT monitors real events, processes, and devices**.[22]

For some time, even before IoT, many real machines and manufacturing lines have been either partially or entirely automated, and remotely controlled operational machinery has always presented cybersecurity risk. You only need think of the SCADA systems used by companies worldwide to control industrial processes, monitor real-time data, directly interact with industrial devices, and keep logs of events to understand the scale of the dependency production lines on such systems and therefore the scale of the cyber risk.

The infamous worm Stuxnet was malware used to target SCADA systems in Iranian nuclear reactors in 2010, and the VPNFilter malware, which was designed to infiltrate routers and Network Attached Storage (NAS) devices and

[21] European Agency for Cybersecurity (ENISA)
[22] https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence

KEY DEFINITIONS

Denial of Service (DoS)

DoS attacks flood a target server with traffic, or information which causes it to crash. In either case, the server becomes inaccessible to its users. Distributed DoS (DDoS) attacks use multiple machines to flood a target making it harder to trace or block.

Artificial Intelligence (AI)

Intelligence demonstrated by machines, most commonly in the form of Machine Learning. Machine Learning refers to the process of fitting predictive models to data or identifying informative groups within data. It attempts to imitate the human ability to recognise patterns in an objective manner using computation.

SCADA Systems

ISupervisory control and data acquisition (SCADA) is a category of software applications for the supervision of machines and processes, monitoring feedback data in real-time, and recording events in log files.

then seek out SCADA systems[23], was used in a number of attacks including the Ukraine power grid incidents. Modules of VPNFilter are capable of intercepting traffic through ports, executing commands on devices, and rendering devices unusable. For further discussion on the issues surrounding SCADA, read our 2020 white paper on The Threat to Logistics[24].

The advancement of OT is accelerating. Not only does industry rely on OT like SCADA for process control, but also on digital devices for communication and geolocation, and on technology such as driverless vehicles, drones, and other IoT devices throughout supply chains.

Whilst these are all targetable systems in their own right, the real danger comes with merging OT devices with IT. More devices are interconnecting every day, and not just through local connections but on the open internet to facilitate remote access. **Remote access works both ways.** Human users can access physical systems to initiate processes, assess and verify operations, and manage supply chains; at the same time, **OT can access databases, make decisions, and relay information elsewhere**.

This can be incredibly useful, but also creates huge vulnerabilities. We as people naturally understand the risk of data access on an IT network in the context of a cyber-attack: malware entering an inbox for example can make its way into a network and exfiltrate data. This is bad. But now, with IT/OT convergence, malware entering an inbox can migrate onto a network, and then piggyback on the IT /OT connections, normally used for data flow or execution of control protocols, to access physical devices. So **it is able to exfiltrate the data used by the OT but also hijack the real-world system.** This is very bad.

Ransomware in this case can become even more dangerous than we already realise. Such an attack spreading to OT devices could result in complete operations, vehicles such as trucks or ships, and cargo being held to ransom. This type of ransom may have financial or espionage motivations; stolen cargo could be sold on for money or to those interested in extracting intellectual property for example.

Artificial Intelligence

IoT is not the only way to improve supply chains. Artificial intelligence (AI) is increasingly being employed to improve automation, as well as monitor production and transportation within supply chains.

AI is not very common in cyber-attacks themselves, but this is likely to change in the near future. Machine learning (a type of AI) is an obvious tool for cybercriminals to utilise when dwelling within a breached network, where the goal is to learn as much as possible about the network architecture, data types, and exploitable vulnerabilities. It could also be used to hide suspicious activity by masking itself with apparent randomness or developing employer-like traits.

This, however, is not the point we are trying to drive home. Using AI to monitor and optimise supply chains is indeed an effective way to boost productivity, but it removes the human element from tracking and quality control. This is ok as long as your AI architectures were trained with extensive, robust data sets, and the algorithms can adequately cope with variability whilst flagging true outlying incidents. **Bad data and by extension bad training will compound the chaos of a cyber-attack.**

Bad data may not come from you. This is a vulnerability many do not appreciate. A cybercriminal which knows about a supply chain's reliance on machine learning can feed bad data into the system, teaching your algorithm something you did not intend. And this could be long lasting. An AI system retaining this information could have its learning affected for some time, and the result of this could be catastrophic and unpredictable.

Companies implementing good AI-supported processes will have utilised very large, comprehensive data sets, often comprising years of historical information about

[23] VPN Filter Malware shows how cyber resilience is becoming a critical part of democratic resilience | Global Resilience Institute (northeastern.edu)
[24] The Threat to the Logistics Industry - Cyber Citadel

their supply chain. This data set will be continually added to so that the learning algorithm can continue to improve too. So your company owns an enormous, wide-ranging dataset, with intimate details of its entire working operation. **This is a dataset with a very high storage-risk attached.** The price of setting up AI would be very high indeed if a cybercriminal was able to access this data and so a huge emphasis must be placed on its security and access rights. The tricky part is implementing this security whilst still allowing your AI system to access it in order to learn.

AI-driven cybersecurity is going a long way in protecting global supply chains too. Not only can artificial intelligence be robust against social engineering, and far less susceptible to human intelligence errors such as engaging with spear phishing, but it can also help cope with attacks when they do occur. Partly this is due to the lower response time of AI to incidents, and also because it can react in a much more pro-active way, for example isolating parts of a network or objectively protecting core structures or processes.

Take essential action to cope with complexity

After all this description of threats, vulnerabilities, and the prospect of ever-increasing risk, most readers are probably wondering if there is anything they actually *can* do to cope with the tidal wave of changes to business that are now effectively upon us – ready or not!

Our first directive is always the ASD Essential 8. This is a checklist of eight vital improvements to cybersecurity which can be implemented to different levels of 'maturity' depending on the risk status of the business and the sensitivity of their data. These recommendations are from the ASD, and **enterprises operating SONS should implement the Essential 8 to the highest maturity level.**

This list of recommendations can be grouped to highlight important themes. The first is patching. Patching should be a given for any company who wants to stay on top of evolving malware and known vulnerabilities; failure to install security patches led to the devastating Maersk attacks and countless others. **Patch your systems, it is that simple.**

ASD Essential 8	Application Control
	Patch Applications
	Configure Macro Settings
	User Application Hardening
	Restrict Privileges
	Patch Operating Systems
	Multi-Factor Authentication
	Daily Backups

Privileges: We would go one step further than the Essential 8 and suggest businesses **work on the Principle of Least Privilege** (PoLP). This is the idea that at any user, program, or process should have only the minimum privileges necessary to access the information and resources needed in order to perform its legitimate function. MFA then steps in to make sure that those using credentials with privileges to log onto systems are real, legitimate users. **PoLP and MFA are a double act of process and technology that produce an enhanced procedure for access to IT or OT.**

Backing up really is essential for IT security. Ultimately, if you have backups of your data, or better yet backups of whole systems, then a lot of the risk of ransomware is mitigated, since it removes a considerable amount of the leverage that the attacker has. For more information on the importance of backups and strategies for dealing with ransomware, refer to our 2020 white paper[25].

The final group deals with issues surrounding **browsers and macros: full of functionality and good intentions, but too easy for hackers to co-opt for their own ends**. Businesses need to be more aware of them and configure them such that they can't compromise systems.

For more information on the ASD Essential 8, refer to the Australian Cyber Security Centre (ACSC) website[26].

[25] Your Money or Your Data. The Issue of Ransomware - White Paper (cybercitadel.com)
[26] Essential Eight | Cyber.gov.au

Other good guidelines can be found from NIST and the ISO, and for other approaches such as the Zero Trust model we refer you to our previous logistics white paper[27].

Continuous monitoring – knowledge is power

With the increases in data traffic resulting from remote working and IT/OT interconnectivity, and increasing complexity through AI and operational automation, cyber security comes down to how well you can monitor your network.

The more you monitor, the more likely you are to identify suspicious activity. Like using CCTV in the real world. And when it comes to IT/OT convergence, that monitoring can detect suspicious activity in your supply chain, as well as in the more traditional IT environment.

Ideally, businesses would **continuously monitor** their network in real-time, day and night, all year round. To do this you need a **Security Operations Centre (SOC)**.

With continuous monitoring, digital behaviour and cyber threats can be tracked and attacks prevented. Additionally, knowledge can be gathered about network vulnerabilities and weak spots reinforced before they are exploited. And in the event of a breach, having existing threat intelligence means the incident response plan can be invoked immediately, without delays which often allow malicious software to spread through a network.

We understand that the reality for most businesses is that this level of security monitoring is simply impossible. Whether it is too expensive to set up or to run, or whether companies lack the cyber security expertise to make best use of such a SOC. But companies should do their best, especially if they involve critical infrastructure or SONS. One option is to **use a Managed Security Service Provider** (MSSP) which provides a completely outsourced security solution, giving companies access to specialist expertise and 24/7 protection, and offering the opportunity to increase security maturity levels. Useful if you need to comply with regulations.

KEY DEFINITIONS

Security Operations Centre (SOC)

A facility that houses a team responsible for monitoring and analysing the cyber security posture of an organisation. Comprised of both automated systems and human experts who oversee the security operations, the aim of an SOC is to detect and respond to cyber security incidents, investigate their causes and effects, and o generate reports that can be used to inform investment and improvement in cyber security.

Security Patch

A method of updating systems, applications, or software by adding new code to 'patch up' a vulnerability. Many companies such as Microsoft, Adobe, and Oracle regularly release patches to their software in order to stay on top of newly discovered vulnerabilities.

[27] The Threat to the Logistics Industry - Cyber Citadel

ARE WE ALL DOING ENOUGH?

Whose responsibility is it to ensure the safety of data, of operations, of national digital security? The reality is that governments cannot provide all the solutions because they cannot monitor all data traffic, nor would we want them to in a democracy. But companies cannot be expected to fund and resource huge, comprehensive cyber security without support, motivation, and expertise. The 'all' then, is the important part in this section header.

Different entities – governments, companies, regulatory bodies – share common cyber security interests. An attack on critical infrastructure such as the power grid is distressing from a national security perspective but will also incur loss of revenue and large reparations expenses on the energy provider. Both government and industry would benefit from attack prevention or, in the case of a successful breach, a swift and coordinated response. This should **encourage greater collaboration and cooperation between entities who are striving for the same goal**. This could include sharing expertise, resources, information, or even cyber security services.

This notion of collaboration should also run *within* industrial sectors. Sharing cyber security information between companies, or different sectors such as energy and transport, could vastly **increase the knowledge pool and reduce the chance of the same attack strategy being employed** on two different entities. Attack strategies could be a type of malware, leveraging a particular network vulnerability, or a social engineering tactic.

This is the aim of the **new ACSC Partnership Program**[28] which enables organisations and individuals to engage with the ACSC to lift cyber resilience across the Australian economy. This engagement welcomes cyber security experts, businesses, government agencies, and even individuals who just want to be kept updated with the latest information. As an ACSC partner, you can be provided access to threat intelligence, news, and advice, as well as educational material for improving cyber resilience and the opportunity to join the Joint Cyber Security Centres (JCSCs) network.

More organisations should be onboard with programs such as these where everyone stands to benefit.

Are deterrents an effective motivator?

It is the role of governments and industrial regulators to set standards for the entities they are responsible for. The question is, how are standards enforced? We've talked a lot about enforcement through legislation and industry operator standards but whether they are effective in ensuring organisations follow these guidelines is another question. **In most cases legislation uses fines as a punishment and deterrent.** In the case of GDPR these are quite substantial: up to 20 million Euros or 4% of the annual business turnover of the preceding year in the worst-case scenario[29].

In the US and many other parts of the world the fines are not this steep. Violating the Australian Notifiable Data Breaches (NDB) scheme can cost you a penalty of A$2.1 million (£1.2 million for comparison) in a serious or repeat-offence case[30].

Even where fines are significant, as is the case within the EU, it seems large companies are often able to negotiate their way out. British Airways for example was able to reduce a nearly £183 million fine down to around 20 million. This is still a huge amount of money, but far less than might have been expected from 16,000 claims filed as a group action, and this settlement was delayed until years after the initial breach[31]. Results such as these undermine the credibility and efficacy of regulation enforcement – at least in the case of a very large business.

For industrial regulators, the threat is often **revoking accreditation or licensing**. And as we mentioned before in the case of ports used in the shipping industry, entities

[28] https://www.cyber.gov.au/partner-hub/acsc-partnership-program
[29] https://gdpr-info.eu/issues/fines-penalties/
[30] www.oaic.gov.au/updates/news-and-media/mandatory-data-breach-notification-comes-into-force-this-thursday
[31] British Airways, data breach fines and credibility | Simmons & Simmons (simmons-simmons.com)

who choose not to comply with industrial standards will lose work to those who do. Often this leads to self-regulation: the pressure from clients drives the service provider to comply. Indeed, this may be a far more effective pressure than the notion of accreditation.

Deterrents are not always the best motivation. The **Australian Trusted Trader** (ATT) scheme works by positive reinforcement: offering an enhanced trader status to those who meet certain cyber security standards. We first talked about this in an article[32] in the logistics magazine Across Borders back in 2019, where we discussed the various benefits the scheme offered, including fast-tracked visas, personalised border force support, and goods tracking services to reduce fraud. To achieve the status, companies need only meet a maturity level of the ASD Essential 8 corresponding to their cyber risk. Recently, **the Australian Border Force has suggested they will undertake a re-accreditation audit of those with the ATT status** to reflect an increasing rigor of the assessment of cyber security. This will also ensure that those with the ATT status continue to keep up with the latest recommendations.

A complementary scheme also underway in Australia is the **Trusted Digital Identity Framework** (TDIF). Members of this scheme demonstrate that their digital identity services are trusted, safe and secure and built to the standards set by the Australian Government[33]. By establishing rules around how end users prove their identities, and providing assurance about the privacy, security, usability, and interoperability of an identity provider's processes, the TDIF provides the ability for organisations to have greater confidence that the person they are dealing with is who they claim to be.

The AESCSF Scheme previously discussed have provided some proof in the idea that negative pressures aren't always the most effective. **The voluntary nature of the scheme seems to have been an advantage**, with the AEMO noting that **CEO engagement with cybersecurity has increased substantially since the framework was introduced.** With no legal enforcement possible, this is clearly not out of fear of some violation.

In part, **organisations should be self-motivated by the desire to safeguard their data and processes**. Or at least by the fear of the result of not doing so. For the transport and logistics sector there are many hidden costs to cyber-attacks. Data loss is one thing, but an OT breach could completely halt operations and expenses can run very high. When Toll Group was attacked, operations were halted for weeks, and Paul Zalai from the Freight and Trade Alliance (FTA) noted how one of their current members was still dealing with storage bills and container detention fees that they incurred as a result of the delays caused by an attack, but long after the attack was over. They said **they wished they had invested in cyber security sooner.**

The financial effects are long-lasting. From bills resulting from delays, fines and individual claims sometimes taking years to conclude, the loss of revenue during down-time, and of course the potential for serious damage to reputation.

Ultimately, **the need to protect your business should be first and foremost in motivating cyber security improvement.** Negative pressure such as legislation and industry standards should be there to help guide your cyber security program and inform you of minimum requirements, but not as a bare minimum list of necessities that you should only do if you can't get away with avoiding them.

If large companies want to avoid fines, they will find a way, but this is really not the point of legislation. Hopefully positive pressure from schemes such as AESCSF and ATT will lead the way in promoting a positive attitude to cyber awareness.

[32] https://www.cybercitadel.com/australian-trusted-trader-cybersecurity-compliance/
[33] https://www.digitalidentity.gov.au/tdif#tdifaccreditation

TAKE THE PLUNGE WITH CYBERSECURITY

There is great temptation within logistics to push assets further and further, to squeeze every last capability to maximise output and minimise cost. We understand this, it's just business. But there is great danger in doing this without investing in safeguards. This strategy of **'sweating assets' is not sustainable**, and **far greater long-term growth can be obtained by making investments in cyber security**, such that your assets and capabilities are protected against threats now and in the future.

Ignorance is *not* bliss

The FTA advertised a **no-win-no-fee cyber security assessment** to its members. The offer was simply that if Vulnerability and Penetration Tests (VAPTs) were not successful in identifying *critical* cyber security issues, the company would not pay a penny for the service.

The FTA were "surprised we haven't had a bigger uptake on that". But why?

Why would you not take the offer of a service that will cost you nothing if you don't have any critical problems or will save you an enormous amount of money if you do? This no-win-no-fee is a win-win for any company. End of discussion.

There can only be one answer: human nature. Paul Zalai noticed this giant flaw: **"they don't want to know the bad news"!** People don't want to know if work needs to be done, they don't want to know if they have problems, they would rather live in blissful ignorance.

But ignorance is *not* bliss.

As Paul said, companies have been through this: ignoring their problems (or not even finding out if they have any), becoming the victim of an attack, seeing how much it costs them in operations, finance, and clients, and then wishing they had invested sooner. Hindsight can be cruel, but no one can say they were not warned.

The fact is, **work will always need to be done**, especially in logistics where vulnerabilities can always be found in the many legacy systems still in place, but now connected to the internet without having been properly tested for resilience to cyber attack in the modern age. But companies shouldn't look upon the discovery of a vulnerability as a bad thing. **Finding a vulnerability in a VAPT is a *good* thing** – it is one less vulnerability exploitable by a hacker. It is one more win for the company against the scourge of cybercrime.

KEY DEFINITIONS

Vulnerability and Penetration Test (VAPT)

A **vulnerability assessment** is an automated comprehensive scan of a cyber network which detects technical vulnerabilities and can be used to inform a penetration test to increase its effectiveness

A **penetration test** is a human-led investigation involving an authorised, simulated, cyberattack on a computer system, performed to evaluate the security of the system, and provide both technical and business solutions.

Red Teaming

Red Teams play an adversarial role and attempt to break into a target network. These operations simulate a real attack and aim to reveal network vulnerabilities, particularly to new and sophisticated techniques. Red teamers are experienced specialists with a deep understanding of the structure and behaviour of complex networks, as well as in security testing and system compromise.

Insurance is *not* the answer

Cyber risk is managed through strong and proactive cybersecurity, by having a tight and well-practice incident response procedure, and by having comprehensive cyber-insurance. **Whilst cyber insurance is important, strong cybersecurity should come first.** To get the most out of insurance, businesses must have mitigations in place. You need to demonstrate that you have understood and taken measures to reduce risk and respond effectively to an attack.

Cyber insurance can help you cope with the fallout of a successful breach into your network, but no one can argue with the fact that it would be much simpler and less costly in time and money if you sought to reduce your risk of cyber threats in the first place.

Insurance providers will try to shift responsibility and reduce their pay out rate. Already **premiums are increasing** – in some cases by 40-50%[34] – to meet the rising frequency of ransomware. But more significantly, insurance providers are reassessing outdated policies not designed for the vast modern cyber threat landscape.

Claiming on insurance will get harder. Unless of course you can demonstrate that your company has taken all the necessary steps to mitigate as much risk as possible. Hopefully you can see that the discussion is becoming circular. If you take all the steps to reduce risk, you are more likely *not* to need your insurance. If you don't manage your risk, you will likely need your insurance, but will be unlikely to win a pay-out.

The conclusion: invest in risk management. Then, not only will you reduce your chances of a serious security breach, but you will increase your chances of a successful insurance claim.

A VAPT is an excellent way to demonstrate your commitment to risk management. Not only might it protect your company from attack, but it will also help with any insurance claim. Even more reason (if you needed any) to accept the no-win-no-fee offer. We discussed the issues of insurance in more detail in a recent (2022) article for Across Borders[35], where we look at further ways you can demonstrate your commitment to reducing cyber risk.

Do be prepared

Insurance is a financial backup plan. But other plans are equally, if not more, important, and we have stressed time and time again that Incident Response Plans are absolutely critical for managing a security breach. These should prepare for all eventualities: containing the infiltration, dealing with ransomware negotiation, even the publicity fallout. Everything should be accounted for.

But these plans shouldn't be relied upon. Such a passive approach to cyber security will end in disaster because you cannot manage everything and everyone, for example the effect on third-party providers or business partners. Or if you are a provider yourself, you might not be able to rely on your client's security. There are too many unknowns.

In addition, when it comes to logistics and transport, you may need to liaise with other entities such as border force, ports, storage units, freight forwarders, the list goes on. Some entities such as the Australian Border Force have worked hard on building continuity plans which in theory do enable industry to continue even in the event of a significant cyber-attack. The FTA however makes it quite clear that it is "a lot easier just not to have to go down that path… because the plans are there but they are very complex and difficult to implement" and it is somewhat unclear how many personnel have the training, expertise, and experience to implement these plans with confidence.

It is far easier to have protections in place, protections you can manage and take control of without external dependency.

[34] https://www.egress.com/resources/cybersecurity-information/phishing/cyber-insurance-payout

[35] https://www.cybercitadel.com/what-lies-beneath-security-operations-centre-as-a-service/

When is enough really enough?

An issue that many grapple with is quantifying successful cyber security. If you have not been attacked, how do you know if this is because you have good security or because you are not being targeted?

Let us end this debate here and now. In the Verizon report they analysed 23,000 attack attempts and 5,000 successful breaches. This tells you one **there are orders of magnitude more attempted breaches than successful ones. If you are not aware of the attempts this means your cyber security posture needs improving.**

It also means you have been incredibly lucky not to have suffered a successful breach. Or does it? With the new business approach to cyber-crime, and the growing marketplace on the Dark Web **it is possible someone has already stolen your data, posted it on the Dark Web, but no one has yet bought it or used it against you.** At least not in a publicly determinable way, this doesn't exclude more subtle uses such as identity theft or sale of intellectual property currently being used to replicate a product or business strategy without your knowledge.

To convince directors to approve investment into cyber security, we understand you need a metric – something that is meaningful in describing whether investment is worthwhile, something that measures the success of implementing security strategies.

VAPT is a good place to start. Performing this test reveals issues within your network security – solve these issues and repeat the VAPT. Your overall security posture score should go up because your vulnerabilities should go down. **Regular assessment using VAPT should make it harder for Red Teams to successfully infiltrate your system**, and metrics such as 'time required for successful penetration' or 'probability of penetration within 48 hours of attempt' could be used to demonstrate to directors that meaningful improvements have been made.

VAPT is not just about picking holes, it can be used to show progress!

If you have a good continuous monitoring program, such as one provided by an MSSP, then you will no doubt be aware of suspicious activity and the number of attempts to breach your systems. This really is **an ultimate metric for assessing security: the number of successful breaches as a fraction of the number of attempted breaches.** The smaller the successful breach fraction, the better your security.

An additional metric to consider, especially for larger companies, is **the number of breaches (or attempted breaches) per connected devices.** This is a great metric to **show that your cyber security is coping with company expansion**, as well as with the drive for increasing automation and supply chain complexity. This is also a powerful argument for increasing cyber security investment, as it shows the **investment is supporting the overall growth of the company** and not a waste of resources.

OUTLOOK AND FUTURE PERSPECTIVES

We are certain that the next time we write about logistics, transport, and critical infrastructure the world will have changed again. No doubt the sector will always be playing cyber security catch up. But we hope that by highlighting all the resources available, whether drawn from legislation, industrial standards, or from voluntary schemes hoping to improve community response to cyber threats we can help businesses catch up as quickly as possible and even get ahead of the game.

It isn't all catch up: **some strategies are timeless**. Critical self-assessments with VAPTs, implementing good incident response plans, and employing cyber aware risk management will always be at the heart of good cyber security posture.

If you take nothing else away from this white paper, let it be that **ignoring the issues in the hope that they won't affect you or that they will go away is not a viable approach to dealing with the risks of cybercrime.** It will cost you far less money, far less inconvenience, and possibly save your business from unrecoverable reputational damage if you take your company's head out of the sand and **face up to the threat of cyber-attack.**

Work together with industrial partners, industrial regulators, and government agencies. Engage with resources and educational support from organisations such as the Joint Cyber Security Centres Network, the Freight and Trade Alliance, and their educational provider WiseTech Academy. These organisations, alongside government agencies are there to inform and support your business because everyone serves to benefit from improved cyber security.

Remember, it's all for one, and one for all.

Cyber Citadel

Jonathan Sharrock

jonathan.sharrock@cybercitadel.com

www.cybercitadel.com

Cyber Security specialists

With highly-satisfied clients in over 26 countries across 5 continents, we provide Penetration Testing, Vulnerability Assessments, Red Teaming, Incident Response, Malware Analysis, Asset Discovery, Source Code Review and Forensic Analysis. We have particularly deep expertise in multi-lingual Web Application and Network Infrastructure Penetration Testing.