CYBER CITADEL

THE THREAT TO LOGISTICS

Preparing for a new age of cybercrime

FTA
FREIGHT & TRADE ALLIANCE

CONTENTS

THE CURRENT SITUATION

The logistics sector does not need convincing of the risk of cybercrime to its operations. FedEx and Maersk in 2017 are two of the most notorious and devastating examples of network breaches, but already in 2020, TQL, MSC, and Toll Group have all been hit – the latter twice! These breaches have cost hundreds of millions of dollars in addition to reputational damage[1,2], but the true long-term danger of these attacks lies in how they have exposed the vulnerabilities of the logistics sector to cybercrime.

There are many reasons logistics firms are particularly at risk. They have large-scale and wide-ranging employment, involving permanent employees, contractors and third parties. Shipping requires on-shore and off-shore teams, which need constant lines of communication, and transport crews (over land, air or sea) are often transient, making device and traffic monitoring difficult and increasing the risk of cyber breaches due to phishing, human error or internal sabotage.

In addition, logistics company digital networks are complex and often highly heterogenous, with technology ranging from outdated legacy systems right up to state-of-the-art Internet of Things (IoT) devices.

These exposed vulnerabilities, and the associated risk, have been reflected in an increase in regulation. Aside from the responsibilities imposed by data regulations such as the GDPR imposed by the European Union, the International Maritime Organisation (IMO) is also increasing regulatory requirements, and Australia now operates a Notifiable Data Breaches (NDB) scheme with New Zealand following suit from 1st December 2020.

Whilst increased digitisation presents enormous opportunities to grow and optimise operations in a sector which has for a long time lagged behind other industries in the adoption of new technologies, recent years have seen a wave of aggressive modernisations in everything from aviation to warehouse management. Such an aggressive and rapid introduction of new technology has placed companies at risk as a result of rushed and poorly implemented integration and management.

Logistics firms would do well to remember: any digitisation that increases visibility, communication, and organisation of data and processes also has the potential to provide the same advantage to a potential cybercriminal. Modernisation must be done with care.

If the logistics industry is to maintain its long-term stability in the face of cyber threats, it needs to start integrating cybersecurity into the core of its operations. The coming year will bring increased pressures, both in the form of a continual rise in the number of attacks and the increased legal responsibilities brought on by legislation. Corporations will need to confront the reality that to maintain high cybersecurity standards, long-term commitment to continuous monitoring, incident response planning and personnel training will be needed, on top of a foundation of robust technology.

1 https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906
2 https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff

THE NEW CYBERCRIME LANDSCAPE

The world of cybercrime once belonged to computer geeks and lone ranger hackers, people without any tangible motivation or intent who saw breaching security as a challenging game to be won and where the penalty was more often than not just a case of revealing their methods (if sensitive data was not made public).

Then came criminal gangs, who quickly realised that the digital world was far less risky and far more anonymous than the real one, but had the potential for the same level of profit. Still, the computer geek played a crucial role and these gangs were operating in a professional but isolated fashion, with the motive being almost always financial.

Now we are in a new age: the age of the cybercrime marketplace.

Here, dedicated cybercriminal organisations such as the infamous Maze group operate as a business with development, deployment, marketing and sales teams. They generate attack software 'packages' – products to be bought and sold – which are designed and tailored to create maximum damage to or extract the maximum amount of data from companies they have carefully researched and mapped out.

Organised criminal groups are now reported to be behind 55% of breaches in the last year, up from 39% on the previous year[3].

There is also a network of 'affiliates', essentially freelancers who breach security systems, create these software packages and then publish them for a fee. Often these packages will be bought by a group such as Maze who then pay up in royalties if the package proves profitable, analogous to real-world freelancing.

Rogue, random, challenge-driven hacking is out. Organisation, professionalism, and efficiency is in.

Along with this new ethos has evolved an ecosystem fit to facilitate it: a 'dark' business world. Here, cryptocurrency is the new money, blockchain the new bank, and the Dark Web the new trading floor.

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.

Blockchain

All transactions made with cryptocurrencies are verified against a public ledger or blockchain, which is hosted simultaneously by many people running nodes of the network all over the world. Blockchains have many legitimate uses but also allow cyber criminals to easily and anonymously trade goods and services outside the regulated financial system.

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.

3 Verizon DBIR 2019 and 2020

Motivation: It's nothing personal

When we think about motivation behind cybercrime, we think about money, extortion, espionage, gaining competitive edge, reputation damage, even politics. Of course, these are still all the motives, but in a world of cybercrime organisations and professional freelance hackers these are the motivations behind the buyers. The people orchestrating the hacking often could not care less.

This is dangerous: the hackers have no personal justification, allowing them to be clinical, ruthless and indiscriminatory, much like a hired assassin. This also makes them more invisible and difficult to trace and affords the buyer the same virtues.

Cybercriminals now work with their product as with every other in the world: on a basis of supply and demand. In the logistics sector the demand can broadly be categorised into theft and chaos. Theft seeks to obtain money or intellectual property (IP) from a company, both of which benefit from the company remaining functional. Chaos seeks to disrupt a company, perhaps to damage reputation or as leverage for some extortion.

In the last year, financially driven attacks were hugely predominant, with Verizon reporting that 86% of attacks had financial motivation[4]. Notably they also report that all the motives behind attacks of the traditional 'lone hacker' including grudges, fun or ideology combined now represent the smallest portion of attacks. This is further evidence of the change in cybercrime landscape.

Whilst it is important to think about motivation on an industry-specific level, it pays to watch the trends in other sectors too. In 2010, the United States is widely believed to have developed the worm Stuxnet to target systems used in Iranian nuclear reactors. Whilst this appears to have no relevance to logistics, the systems targeted were Supervisory Control and Data Acquisition (SCADA) systems, and these are employed by every logistics company in the world for process management. Military motivations may then also drive the development of malware which has translatable use to other sectors.

4 Verizon DBIR 2020

Cyber landscape: The take-home message

Cybercrime is now a service, bought and sold on a sophisticated and growing market driven by professionals and funded by multi-national corporations. It is both a lucrative and powerful enterprise.

Take out the word 'cybercrime' and replace it with 'logistics' and this statement sounds familiar and comforting. But this makes this statement far from comforting; rather it shows that cybercrime is ready and able to take on the old-world market giant that is logistics. The criminals have done their research and prepared their strategies. The question is, has the logistics sector done the same?

DATA PRIVACY: THE FUTURE IS HERE

The age of enforcement

Data protection is no longer an option. Any company that wishes to trade with members of the European Union must comply with the GDPR, in Australia companies are now required to meet the requirements of the NDB Privacy Amendment, and many organisational bodies such as the IMO are also implementing their own requirements to better regulate their industries.

Additionally, the risk of shareholder lawsuits following a cyber incident where the company share price drops has placed pressure on companies to better minimise risk and protect data. This is particularly prominent in the United States where board directors may be liable to accusations of inadequate disclosure and a failure to perform their duty to confirm the company continues to adequately protect consumer data.

GDPR

The General Data Protection Regulation (GDPR) is a regulation in EU law on data security and privacy. It is based on seven principles[5], highlighted in the box 'The 7 Principles of GDPR', and applies to any data within, from or passing through EU nations. In 2020, a series of guidance updates has been published which cover 'codes of conduct and certification', 'accountability', and 'criminal offence'[6]. Any company trading with the EU should keep themselves up to date and well-informed about this legislation, since violations can incur significant fines of up to 4% of a company's annual turnover.

The 7 Principles of GDPR

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

NDB Scheme

In Australia, a company is required to comply with the Privacy Act 1988 and must take reasonable steps to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. This extends to situations where an entity engages a third party to store, maintain or process personal information on its behalf.

The Notifiable Data Breaches Scheme makes it mandatory for companies and organisations to report data breaches that are likely to result in harm to an individual whose personal information is involved to the Office of the Australian Information Commissioner (OAIC) and any affected or at-risk individuals[7]. The notification must also include recommendations about the necessary steps that should be taken in response to the breach.

5 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
6 https://ico.org.uk/for-organisations/guide-to-data-protection/whats-new/
7 https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/

CCPA

The California Consumer Privacy Act (CCPA) is 2020's big data protection headline and is set to be the first of many state-level legislations in the US. This will pave the way for federal data protection legislation, so watch this space. This privacy act is based on four 'rights' of the consumer (see box 'The 4 Rights of CCPA')[8].

The 4 'Rights' of CCPA

1. The right to know
2. The right to delete
3. The right to opt-out
4. The right to non-discrimination

Around the world

Whether from an ethical perspective or a practical (economic) one, the GDPR seems to have carved a canyon into which other nations are gradually falling. 2020 has seen Brazil introduce LGPD, which is closely modelled on the GDPR[9], a joint parliamentary committee in India review the PDPB[10], and South Korea raise its national legislation in line with Europe's[11]. Other countries will follow suit to facilitate trade with these large blocs, and businesses need to keep up if they want to continue to tap into these fruitful economies.

Industry-specific requirements

In addition to government legislation, there has also been a significant increase in industry regulatory body directives. For example, as of January 2020, the IMO now require ship owners and managers to incorporate cyber risk into ship safety assessment. After this date, ships that do not comply with this requirement will be detained.

The International Air Transport Association (IATA) has also recently made significant efforts to standardise and regulate cyber security and data protection. It now maintains a compilation of regulations, standards and guidance applicable to aviation, last updated in August of this year[12]. In January they also forged a new cooperative agreement with the Airports Council International (ACI) in order to improve and integrate industry standards[13].

The battle for trust

Logistics, politics, science, technology – whatever sector you work in – 'the battle for trust' will be central to your 2020/21 campaign. The notion of trust has come to dominate daily headlines and looks set to be the defining philosophical question and humanitarian endeavour of this decade, however absurd this would have sounded in a pre-COVID, pre-Trump, pre-Brexit world.

To win at this game, businesses need to accept that creating trust is now significantly harder. For every piece of evidence a company provides, someone online will find or fabricate something in contradiction and someone, somewhere, will believe it. This has placed great emphasis on receiving certification, acknowledged compliance, and building an evidence-based reputation.

8 https://oag.ca.gov/privacy/ccpa
9 https://gdpr.eu/gdpr-vs-lgpd/
10 https://www.google.com/amp/s/m.economictimes.com/tech/internet/questions-for-2020-personal-data-gets-legal-protection/amp_articleshow/73024663.cms
11 https://www.endpointprotector.com/blog/data-protection-legislation-around-the-world-in-2020/
12 https://www.iata.org/en/programs/security/cyber-security/
13 https://www.logisticsmgmt.com/article/new_cooperative_agreement_forged_to_provide_cybersecurity_in_air_cargo_sect

Which means mistakes just became a lot more costly.

Nevertheless, this is not to say that working hard on cybersecurity cannot also bring you rewards. Businesses in Australia are being offered Australian Trusted Trader (ATT) status if they comply with a set of regulations outlined by the Australian Cyber Security Centre (ACSC). This status provides a range of privileges that any trading company would be advantaged to obtain.

Major benefits include increased administrative efficiency by reducing bureaucracy, especially with the handling of goods at the border, as well as improving cash flow as a result of the ability to defer duty to a specified date to be singularly processed. In addition, businesses receive recognition as a trusted trader, both at home and abroad, with the opportunity to apply for a business travel card (for Asia-Pacific participating nations) and fast-tracked temporary skills shortage (TSS) visas which would normally take 12 months to process.

The status also entitles you to personalised logistics support provided by border force, which can significantly improve the continuity and consistency of service at customs. The support even includes a data collection service which tracks your goods and can be used not only to improve logistics processes but also detect and reduce fraudulent transactions.

Centred around protecting data against theft, loss and misuse, the base-level requirements are defined by the ASD's 'Essential 8' and will help guide any business to better cybersecurity practice.

While no single mitigation strategy is guaranteed to prevent cybersecurity incidents, implementing the 'Essential 8' makes it much harder for adversaries to compromise systems. Furthermore, implementing pro-actively can be more cost-effective – in terms of time, money and effort – than having to respond to a large-scale cybersecurity incident.

Quick Reference: The Essential 8

The Australian Government (Australian Signal Directorate, or ASD) recommends an ***'Essential 8'*** list 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.

1. **Application control**
2. **Patch applications**
3. **Configure macro settings**
4. **User application hardening**
5. **Restrict privileges**
6. **Patch operating systems**
7. **Multi-factor authentication**
8. **Daily backups**

Organisations can meet different compliance tiers, called maturity levels, ranging from 1 to 4. The ACSC stipulates that most companies should aim for the third level unless they are particularly prone to cyberattack due to the sensitive nature of their data.

Achieving higher maturity levels will improve trust in your organisation.

Hiding mistakes will get you nowhere

Mistakes will be made; data breaches will inevitably happen. Covering them up will not help your reputation.

That is not to say any decision is straightforward.

As an example, take the ransomware attack on Travelex earlier this year[14] in which they tried to

14 https://www.wsj.com/articles/travelex-paid-hackers-multimillion-dollar-ransom-before-hitting-new-obstacles-11586440800?mod=business_major_pos7

cover up the breach. The cover-up and ransom pay-out left them extremely vulnerable to 'name and shame' blackmail and meant that customers could not respond by changing passwords and security details to protect accounts.

However, publicising the attack may have resulted in further extortion and ransom demands – making the right decision was almost impossible. But by lying to customers they ended up with the worst of both worlds: extorted, paying out a ransom, and with severe reputational damage.

Data privacy: The take-home message

Companies must do their research to find out what legislation they must comply with in order to legally trade, and keep in mind the rapidly evolving legislature. Do not forget industry standards and local rules in addition to the big-name regional regulations such as the GDPR.

Do not take a piecemeal approach: aim your policies and processes at the highest applicable standard and apply that across your organisation. Even if this means you exceed local standards, a consistent worldwide standard, based on the strictest requirements will give you the best outcome and create a good impression with your customers.

Finally, trust is everything: do what is possible to achieve it, and then maintain it for company reputation. Think of this as a legal way of obtaining a competitive edge in the cyberworld.

A NEW 'WAVE' OF RISK: SECURITY IN THE POST-COVID ERA

Whilst world businesses are grappling with a pandemic which has disrupted trade, isolated employees, and destabilised finances, cybercriminals are exploiting this global disaster for their own gain.

With companies already facing hardships, there is an even greater need to avoid data loss, reputational loss and customer loss. Additionally, any ransom fees or fines imposed by regulations such as GDPR would, in prosperous times, be an expensive mistake; in COVID-19 times this could be a fatal error for a business.

Tactics include impersonating executives, governments and key organisations; taking advantage of people's fear and financial instability; and capitalising on the increased vulnerability of company networks due to remote working.

The pandemic has placed great strain on all areas of business, but when it comes to cybersecurity it has not just exposed vulnerability, it has accentuated it. Business has changed, and companies need to adapt quickly and effectively.

A 'new normal' brings new risk

The COVID-19 crisis has resulted in a major shift in the way that the world is operating, from business to government, to education. All employees are working from home, where they are able, and this means that a significant amount of work is now conducted online. This is not just about virtual

meetings, but also about data sharing over online storage platforms, a greater volume of and reliance on email, connecting to business servers, and even accessing desktops remotely.

The modern global world is increasingly reliant on communication, data sharing and digital operations. In fact, the world is generally spending more time on the internet – increases during the pandemic of 20% or more have been reported in countries such as Italy and the UK[15].

Increased email traffic means increased opportunities for phishing and whilst this type of attack itself is not very sophisticated, it only relies on the mistake of a single individual opening an attachment, following a link, or in some cases (though rarer) just viewing the email in full to be successful.

In addition to a higher volume of emails, many employees are receiving update-type communications from senior members of their organisation who would not normally contact them. Unlikely to question information or instructions from senior executives, employees are at particular risk of being targeted by impersonators.

Files, online resources and virtual meetings are all being shared via email links. This is a dangerous game. Emails are easily replicated, and employees will often follow links sent to them without thinking or properly inspecting sender details. Especially if the sender is a senior member of staff (or masking as one).

Most of the malware currently in circulation is not new, just rebranded and repurposed for the COVID-19 era. In particular, Microsoft highlights malware known as Trickbot as the most commonly employed piece of malware in COVID-19-branded attacks. This software – originally used in attacks on banks to gain account information – is used to drop additional malware such as ransomware or remote access malware into a system. It is normally deployed through an attachment (or link to an attachment) on a convincing phishing email which instructs the recipient to open it.

For many businesses, the COVID-19 pandemic has meant a sudden need to manage remote workforces, which presents increased cyber vulnerability, and executives are now looking towards a range of future developments to combat this. Fortunately, this is something that the logistics sector is used to, however it now just needs to extend remote security protocols into employees' homes too.

In particular, many companies use applications only ever designed to be run internally. But, driven by remote working, these applications now face public networks and the open internet. Such applications must be rigorously tested to ensure they do not pose a risk to the company.

The attack on Toll Group, which has been hit twice since the pandemic outbreak, is notable for its use of ransomware distributed through exposed Remote Desktop Protocols (RDPs), which are naturally more prevalent with so many working from home.

Employees working from home are not protected by a corporate firewall and company data traffic often cannot be monitored. And if anything were to go wrong, the IT department is not necessarily at hand.

The remote working trend will not be short lived: before the pandemic, more and more people were conducting work on commutes, in cafes, and in shared 'coworking' office spaces.

These unsecured sites place company data and function at risk.

Unsecure sites mean more vulnerabilities and more opportunity for cybercriminals. Document access and sharing, connecting virtual meetings and generating file backups are cause for serious concern.

File access must be protected with strong, unique passwords, and multi-factor authentication (MFA) which confirms authorisation by a second method, such as a code sent to a mobile. Using public networks without a company VPN (such as those in cafes and on trains) when accessing company files should be banned, because cybercriminals can easily intercept this traffic and steal valuable data.

15 https://blog.cloudflare.com/on-the-shoulders-of-giants-recent-changes-in-internet-traffic/

If an employee's device is linked to a company server or contains credentials (such as saved passwords) allowing access to servers, it puts the entire network of an organisation at risk. This is why high-privilege credentials should only be given to those who absolutely need it, why it is important to train employees to be vigilant, and why server access and data traffic need to be monitored.

More so than ever, businesses must think about cybersecurity holistically: people, policy and process, as well as technology. People need to be educated about the new risks of working remotely, employers need to adapt their policies to facilitate this new work environment whilst keeping data safe, and security teams need to implement processes to enable this.

A lesson in virology

The growing sophistication of computer viruses brings them ever closer to the complexity of the real thing. Ransomworms, for example, can now land on a system, understand its architecture, encrypt and steal its data, and then hijack its machinery in order to replicate itself and spread laterally to other machines on the network. This basically resembles a biological virus, perhaps minus the encryption part.

There is one upside then to this pandemic: science has been refocussed into virology, epidemiology, and social psychology, and all of this can be repurposed for cybersecurity.

For example, much work has gone into modelling the spread of the COVID-19 virus using statistical network analysis[16], and this of course applies to a cyberattack, where instead of people we have machines, each a node in a local network which makes up a company. That company acts as a larger node – or a higher-order structure – which could then spread the virus to any other connected structure such as a contractor or service provider.

However, it is not just about these technical underpinnings: the response to the pandemic can also offer board directors and information officers real, practical lessons in dealing with a viral 'outbreak'. Namely the concept of testing, tracing and isolating.

Get tested, track and trace, isolate!

It was clear from the start of the pandemic – or at least to those knowledgeable in the field – that the key to getting to grips with the virus was mass testing. The quicker that cases were found, the quicker they could be isolated and prevented from spreading. But more importantly, testing also revealed vulnerabilities in the population, both in terms of which demographics were most at risk of infection and which were most vulnerable to the disease.

The same is true of cyber viruses. Thorough testing is crucial to revealing systems that are at risk of infection (e.g. client facing, remote access machines or personal devices) and vulnerable to the result with serious consequence (e.g. process control systems such as SCADA, communication and geolocation devices or data backups). Preventing lateral spreading through the network is paramount and this can be achieved by completing regular testing, tracing the path of any infection, and isolating all compromised machines.

Finally, we can think about some of the forward-planning techniques that were implemented to try and reduce the rates of infection.

For example, China placed strict provincial segmentation rules on its country, so that if one city suffered an outbreak, a neighbouring city did not. This idea of segmentation is a powerful tool in preventing lateral infection in a digital network. An infection of a SCADA or Internet of Things (IOT) device managing some transport process should never be allowed to cut itself a path all the way to company backup servers or financial databases for instance.

One of the simplest measures all governments tried to take was the idea of reporting and self-isolating. Equivalently, staff should feel empowered within a company to report suspicious activity on a digital device and quarantine it from the network until it is thoroughly tested and cleaned. Staff should also be adequately trained so as to be vigilant and able to maintain their own personal and work devices.

16 Loyal & Chen, Statistical Network Analysis: A Review with Applications to the Coronavirus Disease 2019 Pandemic, Int. Statistical Review, 2020, https://onlinelibrary.wiley.com/doi/10.1111/insr.12398

THE THREAT TO LOGISTICS

The logistics sector is vulnerable

Logistics firms have always been susceptible to cyberattack. Toll Group have been attacked since the start of the pandemic, and their current CEO is no stranger to this susceptibility, since he was an executive at Maersk during the infamous ransomware attack of 2017.

The vulnerability is partly due to the nature of logistics and its reliance on digital communication, but also due to the way their networks are built up over time – often comprising a full range of technology, from outdated legacy systems right up to state-of-the-art IoT devices.

The drive for automation

Logistics firms are searching for new ways to streamline process, make supply chains more efficient, and automate tasks to cut costs and reduce the impact of human error. Whilst the logistics industry has lagged behind others in the adoption of cutting-edge technology, companies are now introducing technologically driven solutions including IoT, cloud computing, and artificial intelligence at an alarming rate. Why alarming? Because they are often invoking these without giving due consideration into the risks and new vulnerabilities that such technologies carry.

New tech in an old environment

One of the biggest problems, and one that is particularly prominent in logistics, is the integration of new technology into a network environment that itself is old and which evolved over many different eras of technology.

Both ends of the spectrum make logistics firms vulnerable, and exacerbating the problem even further is the often poorly designed 'spaghetti code' holding all these systems together. A lot of this code was built in an era predating serious cybersecurity, and by people who have left the company. This makes issues hard to fix and leaves holes for attackers to exploit.

Old machines running outdated operating systems might be stable, but are often no longer supported from a security perspective, and no longer receive patches. Updating these systems may seem like a huge and painful task, but leaving them in place provides weak points in the network which can be exploited by hackers to gain access to other systems.

The devastating NotPetya attack which affected Maersk is the perfect example of this. It was not in fact possible for this malware to spread through the newest operating system from Microsoft, Windows 10. However, because many companies were still using older versions, the malware was able to spread. Even new operating systems will need to be patched and keeping these systems updated should be a priority for any security team.

In addition to the problems of old operating systems, some technology, including the ubiquitous SCADA systems, were never designed to be connected to the internet at all, being built before the advent of the worldwide web. SCADA systems allow organisations to control industrial processes, monitor real-time data, directly interact with industrial devices, and keep logs of events. Often these systems have been incorporated into networks in a makeshift way, and their IP addresses available by simply searching online, giving hackers access to essential physical systems crucial to running processes at ports or warehouses.

At the other end of the tech spectrum sit brand new IoT devices. Estimates vary, but statistics suggest that around 30 billion IoT devices are currently connected to the internet, with this predicted to

rise to 75 billion by the year 2025[17]. Many logistics companies are racing to incorporate internet-connected devices and sensors to improve their monitoring and analysis capabilities in a vast array of areas, from monitoring fuel consumption, to tracking fleets of trucks, to monitoring damage to railways. These devices radically enhance the visibility of a supply chain, allowing companies to better understand their processes and those of their third-party providers.

This visibility is a double-edged sword, however, as connecting more devices to the internet necessarily increases a company's exposure to online attacks. This exposure is exacerbated by the fact that many IoT devices have poor security features and update infrastructures, often not having been built with a 'secure by design and by default' philosophy and are now difficult to retroactively secure.

These devices can be a back door for hackers to gain access to a wider network. Malware such as VPNFilter even appears to have been tailored to play on the worst fears of logistics companies because after initial infection, it targeted SCADA systems. Modules of the malware were found to be capable of intercepting all traffic through selected ports, executing commands on connected devices, and even rendering devices unusable.

AI and associated data analytics are now central tools for companies to sort and organise data traffic and improve process efficiency. This also comes with risk – it is harder to monitor data of these volumes and difficult to flag anomalies. Unauthorised access to this data also provides invaluable insight into company operations and enables hackers to quickly learn and exploit supply chain vulnerabilities.

The growing use of AI looks to soon be at the heart of logistics, with potential applications in autonomous vehicles or vessels, drones and process optimisation (everything from collision-avoidance systems to vessel cleaning). Companies will need to keep pace with these developments and keep pace with the security that must accompany them. Otherwise digital hijacking and piracy will become commonplace, and ransomware could be merged between the digital and real worlds with drones or trucks of cargo held to ransom in addition to data.

Third parties: More is not merrier

One of the more nuanced difficulties faced by logistics is the huge number of third-party systems and networks that they need to interact with and, in some cases, even operate within. These might be customers, partners or third-party logistics (3PL) providers, and the reality is that a company is only as secure as its weakest link.

Any third parties should meet the same network security requirements as your own organisation, and any points of interaction need stringent monitoring. Data handling should meet a standard and any network traffic entering a company or external devices connecting to the company network need to be screened.

Such a complex ecosystem and array of interactions often leaves logistics companies at a loss with where to start in securing their supply chains, and thus the issue is pushed back in favour of pushing company growth forward. This needs to be addressed, because when it comes to cybersecurity the risk of pushing ahead insecurely does not outweigh the benefit.

Growing a business, the smart way

As a manager or company director, it is easy to be overwhelmed by this seemingly colossal task of addressing problems with such a complex network. The solution is to tackle the problem with a comprehensive and holistic risk management programme: always think people, process, technology.

17 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Integrate with care

The vulnerabilities created by introducing new technology or integrating old legacy systems is clear. The solution is to properly incorporate them into the company network so that they do not provide a weak entry point for a potential cybercriminal. Update old software and use the latest operating systems where possible. Ensure that legacy systems are still supported and have the latest patches and if not, then segregate them from the network as much as possible whilst decommissioning and replacing them.

Simple steps, like making cybersecurity features a priority in the acquisition of IoT devices and banning employees from connecting their home devices to a corporate network, can help prevent the spread of unnecessary new vulnerabilities. Of course, companies want to remain functional and, as with every risk, they must employ the 'as low as reasonably achievable' principle. If a company does not want to prevent employees from connecting their personal devices to the network, then employ rigorous background checks on these devices and require them to be heavily vetted in terms of their security status and anti-virus features. A similar approach should be taken with new IoT devices.

The zero-trust approach

As has been highlighted, the traditional network perimeter is being brought down; whether this is because of third parties, remote workers or cloud computing. Thus, the traditional approach to security must evolve to cope. In zero-trust architecture, every aspect of the network is treated as hostile and something connected to that network should not assume to be able to connect with everything else.

Trust is then obtained in users, devices and services through authentication, device health and authorised access to services. Access to the network is then awarded based on a set of policies which rigorously test the connection credentials and health.

Recent research from the UK's National Cyber Security Centre[18] has produced a set of 8 principles which comprise the foundation of zero-trust architecture. These provide an excellent platform from which to reassess the design of a company network.

Again, there is a danger of being overwhelmed at the thought of overhauling your entire network to meet more stringent requirements. It is important to realise that this will take time and cannot all happen at once. Deploying a zero-trust approach should be done in phases, and all traditional security methods already in place should stay there

The 8 Principles of Zero-trust Architecture

1. Understand your network structure: users, devices, and services
2. Create and require strong user, device, and service identities – these are the new perimeters
3. Know the health of your network users, devices, and services
4. Use well-defined policies to authorise requests
5. Authenticate everywhere, preferably with multi-factor
6. Focus monitoring on devices and services
7. Don't trust any network, including your own; trust can only be obtained by network users, devices, and services – not by a network itself
8. Use services with built-in support for zero-trust architecture

18 https://github.com/ukncsc/zero-trust-architecture/

during any transition period. Furthermore, even if a company decides that the zero-trust architecture model is not suitable or possible to deploy, there is much that can be taken away from its concepts, so it is still worth investigating.

A good example of this is in interacting with clients, third parties and remote workers. If none of these networks are trusted by the logistics company network, then each potential user and device must gain the confidence of the logistics network by meeting the access policy requirements. This is excellent practice regardless of whether your entire network architecture is built on zero-trust.

Low-cost/high-return solutions

There is a common misconception among business directors that developing comprehensive cyber security involves serious financial investment, including the purchase of advanced security software and the hiring of expensive cybersecurity contractors.

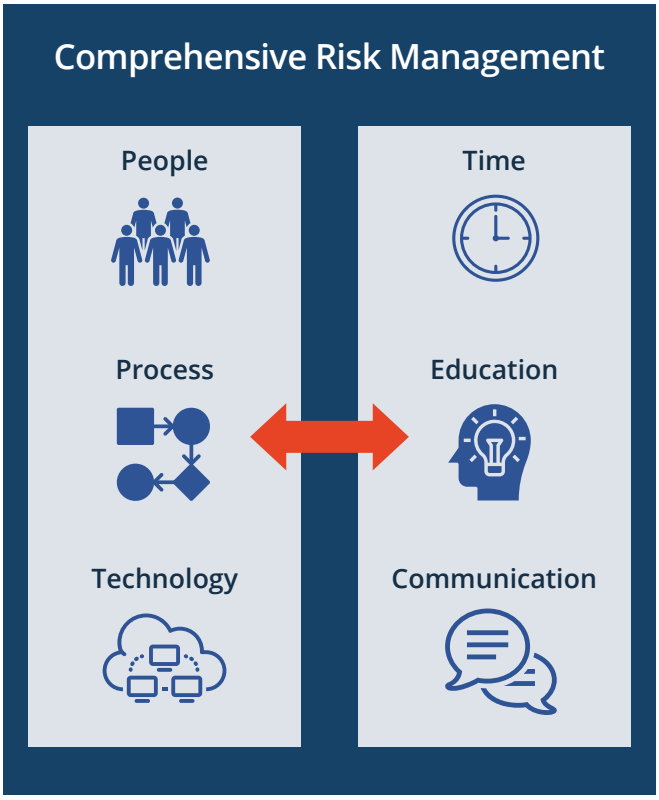
This is just that: a misconception. There is in fact plenty that a company can do without significant expense.

Be aware

Awareness takes many forms. First, company directors need to consider themselves; they need to be aware of the problems and aware of what they can do to help mitigate them. They also need to make their staff aware of the potential risks their devices carry and they themselves as users carry when they access the company network.

Education and communication are key. The board should seek proper training in cybersecurity and appoint a dedicated Chief Information Security Officer (CISO) to show they are serious about security. This should then be cascaded down the company so that every member of staff receives adequate training and to cultivate good cyber practice.

If staff know the risks, know how to recognise vulnerabilities, and know how to spot irregularities, then this can be passed back to the relevant team and the CISO, thus setting up a powerful positive



feedback loop for maintaining and improving network security. Irregularities may be something as simple as a suspicious email, but staff need to feel empowered and should have a direct and easy means to report these incidents, however minor, and even if this means challenging an email that appears to have come from a senior figure. In any case, irregular emails should not be brushed aside, since the Australian Cyber Security Centre recently reported malicious email as being the number-one type of incident last year[19].

19 https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020

A recent study in the UK suggests that 90% of reported data breaches there were due to human error[20], which could include falling prey to phishing scams, mis-delivery of email or providing unintentional privilege. Educating and building a cyber-conscious workforce will lead to better reporting, logging, and following of good security practices. Additionally, it yields a much larger and free-of-charge 'monitoring' team, even if not specialist, which in the event of a breach could help severely reduce the undetected dwell time of the hacker. Essentially, training is definitely worth a time investment.

Awareness also means critical evaluation of the company network as it currently stands. At the heart of this is testing. This is the one area in which an external contractor can provide an unparalleled service because it is far harder to recognise the problems from the inside. Cybersecurity testing experts are specialists in finding network vulnerabilities and scrutinising existing protection for faults. A cybersecurity audit is the most comprehensive of assessments and involves vulnerability and penetration tests (VAPT) to evaluate the digital ecosystem as a whole.

It cannot be stated enough: assessing a network means assessing people and processes too. Identify high-risk staff, such as those who are client facing, communicate constantly with external devices or have high security privileges and so are likely to be targets for hackers. Understanding who in your company is high risk can also help to direct more targeted and appropriate training to those who need it most.

Identifying high-risk processes can be difficult, but consider the flow of information involved, the level of device interconnectivity that processes require, and how varied those devices are. A process which involves communication between internal and external networks, and communication between SCADA systems and IoT devices, for example, is going to be harder to monitor and will be more accessible to cybercriminals.

Be secure

This may sound like very general advice, but specifically it refers to good security practice. The Essential 8, which are a requirement for ATT (trusted trader) status offers some good starting points in this regard, including implementing Multi-Factor Authentication (MFA), patching applications and operating systems, and restricting privileges.

The latter is of particular importance. Applying the principle of least privilege is one of the simplest and cheapest ways to improve cybersecurity, and if done right, one of the least disruptive. This, combined

Vulnerability and Penetration Tests (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

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.

20 https://www.infosecurity-magazine.com/news/90-data-breaches-human-error

with MFA, greatly reduces the number of high-risk staff, attack due to human error, and reduces the potential number of unhappy employees (or ex-employees) able to sabotage the company.

In logistics, it is highly recommended to ban personal devices from being connected to network-connected systems on board a ship, plane or freight train. Even charging a phone could allow malware to infiltrate the network. Removable media devices should also be avoided, except those that have been scanned and only connected to approved devices. This may become increasingly important with attacks such as GPS-spoofing now coming onto the scene, in which ships or other means of transport incorrectly report their current locations. The first known example of this was in 2017, when 20 ships in the Black Sea all reported their locations as 32km inland[21].

The Principle of Least Privilege (PoLP)

The principle of least privilege is the idea that at any user, program or process should have only the minimum privileges necessary to access the information and resources in order to perform its legitimate function.

It is important to realise that once an effective cybersecurity programme is established, it must then be continually reviewed, assessed and updated. This is crucial to ensuring that after all the hard work of making your company cybersecure, it stays that way.

Be prepared

Backing-up company data – the final checkpoint of the Essential 8 – is perhaps the most important way in which a company can be prepared for a data breach. Properly backed up and encrypted data is the most powerful defence against ransomware attacks: it leaves the criminal with little leverage to make demands if they cannot leak your data, and further encryption does not matter because you have other copies. Backups should be made regularly and comprehensively, with effectively managed encryption keys, and should exist on at least two different media, such as external hard drives and cloud-based storage.

One of these media should be stored disconnected to the network so that it is inaccessible to any adversary. An off-network backup device is becoming increasingly important because cybercriminals are spending time within a company network – undetected – seeking information to build a more crippling ransom case or other malware attack. If they find the one and only copy of backed-up data, then they will have the ultimate advantage.

Having a strong incident response process is the other most important preparation a company can make to efficiently cope with a cyberattack. This involves implementing initial response measures quickly and effectively, engaging with response strategists (especially in the case of ransomware), and enlisting all necessary internal and third-party personnel required to deal with the incident.

The basic outline of any response plan should be containment, eradication and recovery. Whilst this is happening, do not underestimate the need for damage control; any public relations team should be prepared to deal with customers and the press.

The board and management should also routinely practise any response plan to ensure that complacency does not set in and that all staff are aware of the individual role they must play in the case of an incident. Communication will be at the centre of any response and practising rapid and clear dissemination of information will be invaluable when it comes to the real thing.

Preparing in advance will also reduce stress throughout the response process and help keep everyone involved calm and level-headed.

21 https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

What *can* tech provide?

Technology, of course, still has its own place in cybersecurity. The more thought that goes into network design, the easier almost everything else is. Whilst a complete zero-trust architecture is not always feasible, ensuring that certain categories of process, departments of users, and backed-up data occur in separate, segregated regions of the company network is becoming essential. With hackers increasing their 'dwell time' within a network, spreading malware and thoroughly investigating the companies they attack, it has become imperative to prevent lateral spreading. Network 'segmentation' is the way to achieve this.

The other major role of new technology will be in continual monitoring. This cannot be carried out manually and solely by an internal IT team, and many companies cannot afford the continual monitoring of expert third-party security providers. One way to resolve this is to employ the same type of technology logistics is using to monitor, automate, and optimise its supply chains to automate the logging and reporting of data traffic. Machine learning algorithms could also be employed to recognise and flag anomalous activity and even automatically quarantine suspicious material. If developing this technology is beyond the remit of in-house teams, then companies can use SIEM (Security Information and Event Management) – a log management software – to protect their most sensitive data and to establish proof that they are doing so.

Other technological solutions could include endpoint security which helps protect a business network when accessed by remote devices like smartphones, laptops or other wireless (including IoT) devices by securing these end-user devices or servers. As discussed previously, this is becoming increasingly important, both due to the increasing number of internet-connected devices and the number of employees requiring remote access.

OUTLOOK

Cyberattacks are more sophisticated, better orchestrated and on the rise. The booming new 'dark' market offering lucrative business to knowledgeable hackers is only fuelling the fire and as the demand and rewards rise for malware and stolen data, so too will the supply. The logistics sector must be proactive in addressing this before attacks like those seen on Maersk, Toll Group and others will become commonplace.

With the logistics sector looking to catch up with the latest technological innovations in improving transport operations, optimising processes and reducing costs long term, it must also consider investing in parallel in the cybersecurity of this new technology. In addition, it must not forget about the legacy technology still in place and still crucial to operations: leaving it behind will create vulnerability.

Technology is rapidly evolving and with every development comes a new risk. This will change year on year, so it will be important for logistics companies to dedicate time and effort to researching and keeping abreast of these new developments so that they might stay ahead of the game. 5G will no doubt be the next big leap, and as AI continues to progress, its capabilities are becoming ever more impressive with autonomously controlled IoT devices and smart spaces (essentially IoT rooms) to follow[22]. These technologies will no doubt present as both a blessing and a curse to logistics and whilst technology rapidly evolves, the intrinsic vulnerability of the logistics sector is not set to change.

22 https://www.forbes.com/sites/bernardmarr/2020/04/20/these-25-technology-trends-will-define-the-next-decade/?sh=3d6aa43a29e3

CYBER CITADEL

Cyber Citadel

Jonathan Sharrock

jonathan.sharrock@cybercitadel.com

www.cybercitadel.com