CYBERSECURITY AND THE THREAT TO LOGISTICS

Confronting the Demands of Security and Data Privacy in a Networked Supply Chain

Jonathan Sharrock / Jonathan.Sharrock@cybercitadel.com

Introduction

For many people working in transport and logistics, 2017 was a year of reckoning with a new era of cyberthreat. In a year that began with allegations that state-sponsored hacking was used to influence the US Presidential Election, followed hotly by two of history's most devastating ransomware attacks, WannaCry and NotPetya, scarcely a day went by without cybercrime dominating the headlines.

Logistics companies found themselves thrown unexpectedly into the centre of this new threat landscape following high-profile incidents such as the complete shutdown of A.P. Moller-Maersk's global shipping operations by the NotPetya ransomware. Maersk, which is responsible for 15% of global container shipping, was forced to shut down all of its communications systems to isolate the ransomware, causing ships to come to a standstill at sea and all operations to halt in 76 ports worldwide, at an estimated cost of up to $300 million.[1] Maersk was far from alone here: in 2017, targets as diverse Deutsche Bahn in Germany, Cadbury's chocolate factory in Australia and the UK's National Health Service fell victim to ransomware attacks.

Despite these risks, increased digitisation presents enormous opportunities for logistics companies to grow and optimise their operations. While logistics 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. Much of the digitisation in logistics relies on the Internet of Things (IoT), which refers to the growing network of internet-connected objects, encompassing everything from digital home assistants to pollution-monitoring streetlights.[2] Another area of focus is increasing integration of cloud computing at all levels of the supply chain. These changes enable radically increased visibility of internal and outsourced processes, which can allow companies to make major strides in their optimisation and cost-saving processes. What many companies currently lack is a full picture of how to manage the risks that come hand-in-hand with these digital rewards. A recent survey from PwC found that 38% of logistics companies have significant unresolved questions surrounding data privacy and security.[3]

[1] https://www.ft.com/content/785711bc-7c1b-11e7-9108-edda0bcbc928

[2] https://blogs.microsoft.com/iot/2016/04/27/iot-reshapes-transportation-whether-driving-down-the-street-or-flying-at-30000-feet/

[3] https://www.pwc.nl/nl/assets/documents/pwc-shifting-patterns-the-future-of-the-logistics-industry.pdf

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 only 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 such as the European Union's General Data Protection Regulation (GDPR) and Australia's Notifiable Data Breaches (NDB) scheme. Corporations will need to confront the reality that no technological solution can provide them with complete protection against cyber-attacks. To maintain high cybersecurity standards, long-term investments in continuous monitoring, incident response planning and personnel training will be needed, on top of a foundation of robust technology. The keys here are visibility and managed risk. Any corporation which is able to monitor its own systems well enough to detect vulnerabilities in advance, and respond quickly and efficiently to breaches when they do occur, will be able to effectively minimise the long-term costs of cyber risk. Soren Skou, the CEO of Maersk, remains optimistic about the future of digitisation in logistics. "It is pretty messy" he says, but with robust strategies to detect and respond to attacks, the benefits of increased connectivity are undeniable.

The State of Cybercrime

Cybercrime has developed a complex ecosystem, made of up of hackers, facilitators and funders, all with a range of motivations, from pure profit to political gain. The majority of cybercriminal activity does not conform to the stereotype of a hacker sitting at a desk, searching for cracks in a security system. To be able to properly mitigate the risk of cyberattacks, corporations need to understand the various types of threats they are up against.

Motivations

While most cybercrime is conducted with the aim of making a profit, either through the sale of sensitive data or the extraction of a ransom from a victim, this often coexists with a more complex set of goals, which can include sabotage, political opportunism, espionage and even simply malicious desire to create chaos. In order to dissect these different motivations, we need turn no further than the dual ransomware attacks of WannaCry and NotPetya, which wrought havoc across the world in May and June 2017, respectively. Ransomware is, in general, a type of malware (malicious software), which seeks to extract money directly from its victims. When a system is infected with ransomware, often through a user clicking a malicious link, the program immediately goes about encrypting files to prevent users from accessing them. When the encryption is complete the program presents a screen demanding payment of a

ransom by a certain deadline, failing which the encrypted files will be permanently destroyed. WannaCry followed this fairly classic pattern, though it was able to rapidly propagate throughout the world by using an exploit called EternalBlue, developed by the US National Security Agency and illegally released online by The Shadow Brokers in early 2017, which allowed it to infect unpatched Windows machines without tricking any users into running malicious files. Infected machines would then present the user with a choice: pay a few hundred dollars' worth of Bitcoin to a given address or lose the encrypted data. By all accounts, the hackers remained true to their word, and many organisations did pay the Bitcoin ransom and recover their files, before a flaw in the ransomware was discovered which allowed it to be contained.

Compare this with NotPetya, the ransomware attack which hit Maersk in June 2017. NotPetya, which was a modified version of an earlier less successful attack called Petya, was also able to infect a large number of systems using NSA-developed exploits. On the surface, NotPetya too seemed to follow the ransomware pattern, encrypting data and demanding a Bitcoin ransom. However, the so-called encryption that NotPetya conducts on an infected machine's hard drive so badly mangles the data that it is permanently unrecoverable, even if the victim chooses to pay the ransom. NotPetya's system of identifying different infected systems was also not functional, meaning that the receiver of the Bitcoin ransom would have no way of knowing which machine to decrypt. All this removes any incentive for victims to pay the ransom and makes the attack entirely ineffective if its aim is to make money for the creator. Most security experts believe that NotPetya's goal was more destruction than profit.[4] The attack was centred on the Ukraine, spreading across the world through the M.E.Doc accounting package which most organisations with operations in Ukraine use for their local accounting. Russia, which is engaged in an ongoing territorial dispute with the Ukraine, is widely believed to have orchestrated the attack with the aim of further destabilising the Ukrainian government.

As militaries around the world increasingly engage one another in cyberspace, this form of destructive military attack is only going to become more prevalent. In 2010, the United States is widely believed to have developed the worm Stuxnet to target the Supervisory Control and Data Acquisition (SCADA) systems used in Iranian nuclear reactors.[5] Similar control systems are used in logistics, energy and chemical industries around the world. China is another frequently cited perpetrator of cyberattacks, on government and private sector targets in

[4]https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

[5]https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

the US, Canada and Australia.[6] There are increasingly fears that non-state militant groups such as IS could be able to adopt similar tactics to conduct acts of so-called "cyberterrorism."[7]

Attacks may also be orchestrated by corporations looking to illegally get an edge on their competitors through sabotage or industrial espionage. Approximately 19% of companies surveyed by PwC in 2017 said they had experienced some form of industrial espionage, which is increasingly being conducted by breaching a competitor's IT system, a form of attack which often remains undetected.[8] Destructive attacks may also have an underlying profit-motive if companies are able to use targeted cyber attacks to hinder the operations of their competitors.

Methods of attack

Cyberattacks vary wildly in their forms and levels of sophistication. While many attacks do involve hackers exploiting particular vulnerabilities in the code underlying a target's computing systems, an even larger number involve malicious actors simply **finding data which has been accidentally made public online**, or tricking people into giving them access to data, both of which require little to no technical expertise. There are an almost infinite number of variations on types of cyberattacks, and not all of them will be discussed here. I will briefly describe four of the most widely used types of attack: Malware, brute-force, phishing and misconfiguration.[9]

Malware: Malicious software, designed to run on a target machine, with the aim of harvesting data, causing destruction or extracting a ransom. WannaCry and NotPetya both fall into a particular subcategory of malware, called ransomware. Malware often needs to be downloaded and run by a user, but sophisticated programs can spread themselves undetected by exploiting flaws in operating systems and other software.

Brute-force: Among the simplest forms of attack, brute-forcing essentially involves having a computer crack a password by trying a series of guesses until they get it right. In theory, this attack is extremely easy to defend against by just using basic password security. However, IBM recently demonstrated that using only a simple cracker they could guess the majority of Microsoft account passwords within a day, simply because the chosen passwords were too weak.[9]

Phishing: This refers to attacks which attempt to trick people into divulging sensitive data or security credentials using social engineering. Typically, this involves directing people to fake websites or getting them to download malware using links in spam emails.

---

[6]http://www.abc.net.au/news/2013-05-29/brandis-briefed-by-asio-on-china-hacking-claims/4719886

[7]http://www.internationalaffairs.org.au/australianoutlook/is-cyberterrorism-a-threat/

[8] https://www.pwc.com/gx/en/transportation-logistics/pdf/tl2030_vol.4_web.pdf

[9]https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN&

Misconfiguration: Refers to exposure of data online due to failure to properly restrict access to it. This accounts for 70% of data breaches of cloud security systems, where the system is simply not set up to prevent someone without access rights from viewing and downloading data.

How attacks spread

Both phishing and misconfiguration can be categorised as "inadvertent insider" attacks; breaches which are the direct result of an employee either failing to properly secure data for which they are responsible or being tricked into giving away access to it. Inadvertent insiders are thought to be responsible for two-thirds of all record disclosures. [9] In early 2018, a 19-year old from Nova Scotia, Canada, was handed a criminal charge for downloading a set of sensitive freedom-of-information documents from the provincial government's website, after discovering that they could be freely accessed simply by trying random document id numbers in the address bar of his browser.[10]

More deliberately planned attacks often rely on distributing malicious software or phishing with spam emails. These spam emails tend to originate from a botnet, a network of compromised computers which can send large volumes of spam emails to a target mailing list, without revealing the IP address of the real author of the emails. As of 2018, the world's largest botnet is Necurs, which at its peak activity may account for 90% of all spam emails.[11] Cyber criminals can pay Necurs to distribute all kinds of malicious content: they have been implicated in spreading malware, phishing and pump-and-dump stock scams, among others.

Some pieces of malware can replicate themselves and spread autonomously through a network. These are referred to as worms and are among the most technically advanced forms of attacks, making use of targeted flaws in operating systems and other programs. Both WannaCry and NotPetya spread themselves like worms, and as such they are sometimes called *ransomworms*. Certain types of worm specifically target cloud computing systems, which are being adopted at a rapid rate by logistics companies. These worms migrate between different virtual machines running on the same physical computer. This form of attack, sometimes sardonically referred to as Threat-as-a-Service, allows many unrelated entities to be breached in one fell swoop by compromising their shared cloud provider.[12]

Attackers often use these sorts of lateral migrations to breach their targets, first using a small "staging target" with poor security, and reaching their true target by exploiting the links between the entities. This was the strategy used in a major Russian-backed breach of sensitive

[10] http://www.cbc.ca/news/canada/nova-scotia/freedom-of-information-request-privacy-breach-teen-speaks-out-1.4621970

[11] https://blog.talosintelligence.com/2018/01/the-many-tentacles-of-necurs-botnet.html#more

[12] Hsin-Yi Tsai *et al.*, Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional,* **14**(1), 2012.

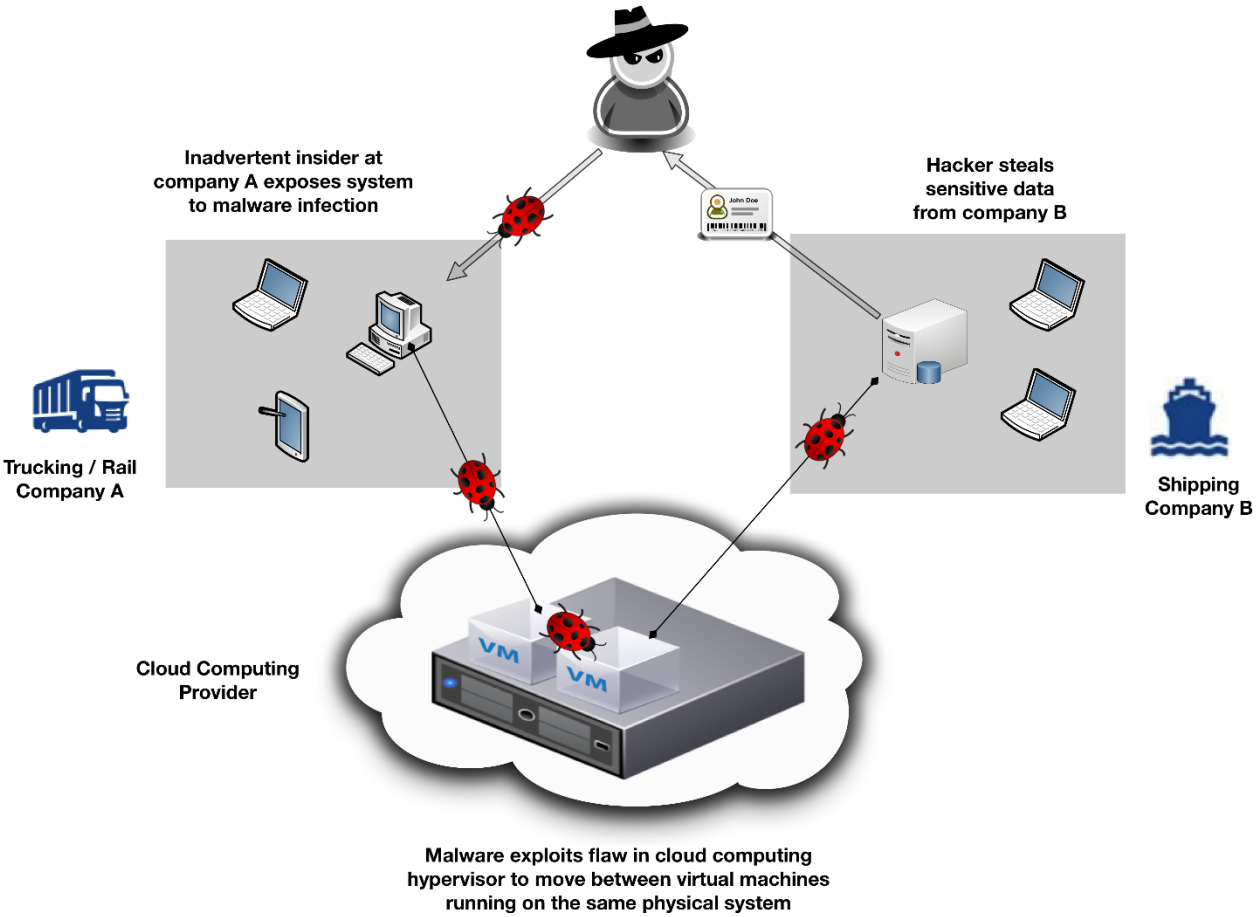

Figure 1: A piece of malware spreads between companies by exploiting flaws in the isolation of different virtual machines run by a cloud computing provider.

industries in the United States, including public and private entities working in the energy, nuclear, water and aviation sectors. This breach, identified by the US Department of Homeland Security and the FBI in March 2018, made extensive use of staging targets as entry points and malware repositories to hit their real intended targets.[13] This particular attack was able to proceed undetected for two years before it was identified by the law enforcement agencies.

The cybercrime market

A few recent technological developments have facilitated the formation of a burgeoning market for cybercrime, which allows funders to easily contract the services of hackers and botnets, and provides a means for criminals to sell stolen data to the highest bidder. The first of these developments is the advent of 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. All transactions verified against a public ledger, or *blockchain*, which is hosted simultaneously by many

[13] https://www.us-cert.gov/ncas/alerts/TA18-074A

people running nodes of the network all over the words. Blockchains have many legitimate uses, and are currently a great target of interest for companies seeking to secure a supply chain which involves many independent parties. However, one of the many uses of cryptocurrencies is to allow cyber criminals to easily and anonymously trade goods and services outside the regulated financial system.

Most of these transactions take place within what is called the Dark Web, the other key technology which has enabled to growth of a cybercrime market. The Dark Web is a relatively small network of websites which cannot be accessed using a traditional web browser. These websites are not indexed by any search engine and can only be found if the user learns the web address from an existing user. The websites can then only be accessed using the Tor browser. When using a traditional browser, a web host will be able to see the IP address of all its visitors. With Tor, the host has no information about the location or identity of users, and different users have no information about one another. This anonymity has been used to create numerous illegal marketplaces, including the notorious Silk Road, a major online market for illegal drugs. On online dark web marketplaces, buyers can contract hackers, purchase stolen information and orchestrate the spread of malware. Even when law enforcement agencies become aware of these marketplaces, they are very difficult to shut down, 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.

New frontiers of cyberthreat

Over the next several years, various nascent technologies are likely to open up new vulnerabilities in cybersecurity systems worldwide. One area of particular concern for logistics companies is GPS spoofing, the mid-range disruption of GPS systems which can lead them to report their location incorrectly. In June 2017, the first suspected real-world GPS spoofing attack occurred, when 20 ships in a small area of the Black Sea all reported that their GPS systems were giving their locations to be 32 km inland, at the nearby Gelendzhik airport.[14] This form of attack, which is much less easily identifiable than GPS jamming, could soon become a favoured tool of criminals seeking to disrupt or steal from logistics companies.

Another area to be closely watched is the increasing use of artificial intelligence in hacking. Using modern AI technology, software can be trained to quickly seek out and exploit vulnerabilities in code. An automated hacker has already been awarded the DEFCON Black Badge, one of the highest awards in hacking, and in 2018 AI is expected to become more efficient than skilled human hackers at detecting vulnerabilities.[15] As it stands, there are close to **1.8 billion cyberattacks occurring every day**, and as hackers begin to

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

[15] http://www.wired.co.uk/article/hackers-ai-cyberattack-offensive

automate more processes, companies can only expect this number to go up.

The Threat to Logistics

While cybercrime is a problem for all sectors of the economy, there are a few key areas of concern for logistics companies, which may leave them increasingly vulnerable in the coming years. In particular, the dangerous cocktail of new, poorly secured IoT devices and old, poorly updated systems which exist in many logistics companies presents a golden opportunity for hackers.

In order to mitigate these risks, logistics companies need to root out their blind spots as they move into the digital age, adopting a philosophy of transparency and visibility across their entire networks.

The Internet of Things (IoT)

Many logistics companies are racing to incorporate internet-connected devices and sensors to improve their monitoring and analysis capabilities in a vast array of different areas. IoT devices are used for everything from monitoring fuel usage in jet engines, to tracking fleets of trucks[16] to monitoring damage to railways.[17] These devices can 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 update infrastructures and cannot generally be manually updated or secured by users. This makes them a favoured target of hackers. In a recent case described by the CEO of cybersecurity company Darktrace, hackers were able to steal a casino's entire high-roller database by first gaining access to the system via an internet-connected thermometer in a fish tank.[18] Despite these vulnerabilities, the market for these devices continues to expand rapidly. Already, it is estimated that 11% of homes in the US have some form of internet-connected smart speaker, such as Alexa or Google Home.[19] These devices are increasingly being brought into offices as well, providing another potential back-door into an otherwise secure system.

Legacy devices

While struggling to control the proliferation of new, poorly-secured IoT devices, many companies are simultaneously dealing with the opposite problem: how to secure older hardware and software upon which their systems

[16] https://blogs.microsoft.com/iot/2016/04/27/iot-reshapes-transportation-whether-driving-down-the-street-or-flying-at-30000-feet/

[17] http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf

[18] https://www.businessinsider.com.au/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=US&IR=T

[19] http://www.parksassociates.com/blog/article/cus-2017-pr12

depend. A vast number of cyberattacks are successful primarily because targets are using outdated or improperly updated software. The devastating WannaCry and NotPetya attacks can, in fact, not spread through the newest operating system from Microsoft, Windows 10. However, because many companies still use older operating systems, which to their credit may be more stable, the worms were able to spread all across the world. To make matters worse, Microsoft had released a patch for their old operating systems in March, months before the first attack, which fixed the NSA exploits used to spread the worms. If companies had properly updated their systems, these two ransomworms would never have gotten off the ground.

Many logistics companies also rely on systems which were **never designed to be connected to the internet** in the first place, and have only been progressively connected into modern digital systems as technology has developed. The supervisory control and data acquisition (SCADA) systems still widely used to manage automated mechanical processes are a particular weak spot. This control architecture, which predates the internet, has often been incorporated in a makeshift way into internet-connected software control systems. This leaves many SCADA devices exposed but completely unsecured. The IP addresses of SCADA devices can often be found using a simple online search, which gives hackers a way to target and take over essential physical systems in ports, warehouses and factories across the world.[20] However, many experts in SCADA, who are responsible for setting up and maintaining these systems, have no security backgrounds themselves. As a result, they are often not fully aware of the vulnerabilities in the systems, which can lull companies into a false sense of security.

Vulnerabilities via third-parties

Logistics companies tend to have relationships with many third-party logistics providers (3PLs) who manage parts of a supply chain, particularly warehousing and "last mile" delivery. These 3PLs, which may be smaller and less technologically sophisticated than the company contracting them, can make ideal staging targets for would-be hackers. A multinational conglomerate may have an airtight security system preventing their systems from direct attack, but that will all come to nothing if a hacker can get access via the system one 3PL uses to organise deliveries. We need only look to the recent Maersk attack to see an example of this: Maersk's global IT systems were shut down by NotPetya, which originated from a single accounting package they used only in their Ukrainian operations. The aviation industry may be particularly vulnerable in this regard, due to their heavy reliance on small 3PLs for maintenance, repair and overhaul. Forbes reports that of a range of aviation 3PLs they surveyed, only 67%

[20] https://www.thalesgroup.com/sites/default/files/asset/document/thales-cyber-security-for-scada-systems.pdf

described themselves as prepared for a cyberattack.[21]

There has been a push to increase visibility across the supply chain using new technologies, including IoT monitoring devices, ubiquitous RFID tagging and distributed ledgers (blockchains). Investments in cybersecurity across the supply chain can have direct benefits beyond simply improving security, allowing companies to gain a better understanding of their dependencies on their 3PLs and identify areas for improvement.

The Future of Data Privacy

Many companies may have to make a major short-term investment in overhauling their cybersecurity practices in order to become compliant with new data privacy regulations such as the GDPR, which greatly expands corporations' responsibilities to protect and manage their customer data.

The European Union's General Data Protection Regulation (GDPR), coming into effect on the 25th of May 2018, is already having a major impact on corporations not just in Europe but around the world. Any corporation which does business in Europe or holds personal data from a significant number of European customers will have to comply with the new regulations set out in the GDPR. Many of these regulations are already included in national privacy laws. The Australian privacy act of 1988, for instance, already requires corporations to adopt a number of measures in the GDPR, such as implementing a **"privacy by design and by default"** philosophy in all their operations, and being able to clearly demonstrate compliance with regulations. Some elements of the GDPR, however, afford some radical new protections to consumers. Among these new provisions is the "right to be forgotten", which means that companies must give consumers the option to have all their personal data held by the company permanently deleted. Laws surrounding consent to data processing have also been significantly overhauled, requiring companies to be entirely transparent with users about all collection and processing of their data, and banning the use of "opt-out" approaches to data processing. The GDPR goes beyond many existing privacy regulations by introducing large fines for violations of the regulation, which can be as high as 4% of a company's annual turnover.

Crucially, once the GDPR comes into effect, companies will be required to actively investigate, review and report on their data processing and security. This means not only adopting the best available cybersecurity measures, but also securing against inadvertent data disclosures at all levels of an organisation. To understand the difference between these requirements, we can take the example of the recent Cambridge Analytica scandal. Cambridge Analytica, a British

[21]https://www.forbes.com/sites/oliverwyman/2018/04/11/how-aviations-global-supply-chain-may-open-up-the-industry-to-cyberattack

psychometric firm, harvested large amounts of consumer data from Facebook users, via a personality quiz app released by a professor at Cambridge University. When users completed this quiz, they consented to their data being used by the creator, who then provided it to Cambridge Analytica. Crucially, however, the app also harvested data from all a user's Facebook friends, who had not themselves used the app or in any way consented to their personal data being processed outside Facebook. No actual breach occurred here; Cambridge Analytica simply extracted the largest volume of information they possibly could using the tools that Facebook provided. This rather vague approach to data privacy is among the practices that are likely to change once the GDPR comes into effect. Cambridge Analytica was later contracted by Donald Trump's presidential campaign in the United States, and the data they harvested is largely credited with driving the campaign's sophisticated voter microtargeting campaign. In April 2018, one month before GDPR comes into force, Reuters revealed that Facebook was moving the data of approximately 1.5 billion non-European users away from its European headquarters, meaning that these users' data will not be governed by the GDPR.[22]

Responsibilities of companies to notify authorities when they are breached will also be increased, under both the GDPR and Australia's new Notifiable Data Breaches (NDB) scheme, introduced in February 2018. Companies bound by the GDPR will now have to notify the European regulatory authority within 72 hours of a breach occurring. Under the NDB, which systematises many obligations introduced in the Australian Privacy Act of 1988, companies must notify the regulatory authority of any breach which could feasibly result in serious harm to any of the consumers whose data is disclosed. This means that companies will need to become proactive in identifying and containing breaches to fulfil their reporting obligations.

Despite the multi-year build-up to the introduction of the GDPR, many companies are still not fully ready to meet their new privacy obligations. In a survey conducted by Deloitte, only 15% of companies reported that they expected to be fully compliant by the May start-date of the regulation. In fact, only 45% of companies had even conducted a readiness assessment to determine their compliance. The news is not all bad, however. A full 61% of surveyed companies expected that improving their data management would yield significant benefits on top of GDPR compliance.[23] This attitude is becoming increasingly prevalent, as executives come to the realisation that the core changes they need to make to improve data privacy will enable far-reaching improvements in

[22] https://www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P

[23] https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-readiness.html

reporting and analytics across entire businesses.

Improving Security and Managing Risk

Despite the complex and sometimes confusing landscape of cyberthreat, companies can significantly reduce their risk by taking a few simple measures centred on increased visibility, improved incident response practices, regular evaluation of existing systems and staff training. While promises of technological panaceas offering complete security can be alluring, technology is no substitute for effective planning and management of risk.

The steps which need to be taken to reduce cyber risk cannot be left entirely to a few technology experts – to make effective changes, security strategies need to be driven by company executives and integrated into the core of a company's business plan. By integrating technological solutions and business infrastructure in a few key areas, discussed below, executives can make major strides in ensuring the digital security of their companies.

Visibility

Perhaps the most important area on which companies can focus in efforts to reduce their exposure to cyberattacks is increasing visibility. Networked systems produce enormous volumes of outputs and logs beyond what is seen by end-users, which can be vital in identifying and containing breaches. However, if cybersecurity staff or consultants cannot access and compile these records, they serve no purpose whatsoever. To enable thorough monitoring of a network, it needs to be possible to observe its operation at all levels. This requires ensuring inter-operability of different software and hardware devices, and designing data management and automatic reporting systems with the express purpose of rationally gathering and sorting data.

A further requirement for visibility is conducting regular thorough assessments of a network, a key practice for the detection of potential vulnerabilities and existing breaches. Currently, breaches often go months or even years before being detected. Globally, the average time taken to detect a data breach is 146 days.[24] Over half of all breaches are eventually discovered by someone outside the company, often a third-party such as a bank. Breaches which are detected by a company itself are almost always found and resolved more quickly, which correlates strongly with a reduction in their financial cost.[25] The simple process of setting up a regular search for breaches could end up saving a company millions of dollars in the long-term.

[24] https://www.infocyte.com/blog/2016/7/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you

[25] https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/

One key way of assessing a network is to conduct **pen tests** (penetration tests). Pen tests are, essentially, friendly attacks on a company's IT system. A contracted cybersecurity professional will attempt to break into the system using the same methods that a malicious hacker would employ. A thorough pen test will include not just hacking but also social engineering, trying to deceive employees or third parties into opening up vulnerabilities in the network. While there are an increasing number of automated pen test applications, these are generally unable to come close to the abilities of a real hacker, or a hacker using artificial intelligence as a directed tool. A rigorous pen test will be able to assess not only the technological security of a network, but also the effectiveness of staff training and good individual security practices.

Awareness and planning

You can have the most comprehensive cybersecurity suite in the world, but if your staff are constantly falling for phishing scams or inadvertently making data public, your company will inevitably suffer a data breach. Training all staff in good security and data protection practice should thus be an essential aspect of any company's cybersecurity strategy. This can include everything from how to identify scam emails, to keeping personal and work IT systems separate, to more sophisticated skills such as how to properly configure a cloud storage system to restrict access to sensitive data. Using this sort of training, the incidence of inadvertent insider breaches, which account for a majority of security events, can be significantly reduced.[9]

It is also essential that companies have a plan in place which guides their staff on how to respond in the event of a cyberattack. It is a reality that most companies, no matter how good their cybersecurity, will eventually face some form of breach. Companies which do have a plan will be able to contain a breach more quickly, and in the end reduce its impact. Experts surveyed by PwC recommend that companies "plan for the possible, not just the probable."[8] This is the attitude of Maersk CEO Soren Skou, who states that following the NotPetya attack, Maersk's main priority is to learn to "isolate an attack quicker and restore systems quicker."[1]

Technological solutions

Though new technologies cannot offer all the answers to cyber threats, keeping pace with developments in the field should certainly be a target for all companies. At the most basic level, this means using systems which are current enough to still receive regular security updates, and making sure that those updates are installed shortly after they become available. Careful integration of new technologies and processes can also reduce a company's vulnerability to cyberattacks. Network design strategies such as micro-segmentation, which involves isolating parallel processes from one another, can compromise the ability of malware to propagate laterally through a

network.[26] Companies may also be able to make increased use of artificial intelligence to rapidly sort and analyse data coming in from a large network, allowing security professionals to spend more time detecting and containing threats.[27]

Outlook

As logistics companies embrace the benefits of increased digitisation and connectivity, they face a challenge in adapting their cybersecurity practices to address their new hyper-connected reality.

The daily volume of malware attacks and other security breaches continues to rise, and as cybercriminals begin to make increasing use of new technologies such as Artificial Intelligence, the severity of these attacks is only likely to increase. Logistics companies confront some particular vulnerabilities, largely due to their links with multiple third-party providers, and their use of both new, poorly-secured IoT devices and old, poorly-maintained control systems.

By conducting thorough assessments of their practices and working towards a model of visibility and active monitoring across all their systems, companies can manage the risk of cyberattacks. No solution can offer complete protection against a potential attacker. However, by contracting security professionals to regularly monitor and test security procedures, companies can stay abreast of the competition and ensure their long-term resilience to cyberthreat.

[26] https://blogs.cisco.com/datacenter/microsegmentation

[27] https://www.ibm.com/blogs/watson/2017/08/how-watson-ai-is-helping-companies-stay-ahead-of-cybersecurity-attacks/

Jonathan Sharrock

www.cybercitadel.com