Locked Out: Tackling Australia's ransomware threat

Cyber Security Industry Advisory Committee

March 2021

Setting the scene

As our world becomes more interconnected, the threats related to cyber security continue to increase.

This was recognised by the Australian Government through the development and launch, in conjunction with its Industry Advisory Panel, of Australia's Cyber Security Strategy 2020 last year.

Significant initiatives since then have included the consultation and subsequent introduction into Parliament of legislation to boost the cyber defences of Australia's critical infrastructure and systems of national significance.

The Strategy's initiatives have preempted the malicious cyber activity that continued to grow pre COVID and has accelerated as COVID related restrictions forced many to work and study from home and more activities have become virtual.

Against this background ransomware has become one of the most immediate, highest impact cyber threats to Australia.

A highly disruptive form of cyber attack, ransomware is a form of malware designed to lock up, encrypt and extract data. These attacks are accompanied by extortion demands, requiring payment of a ransom (often in bitcoin) to decrypt or prevent publication of stolen data. The impact can be devastating, with organisations both large and small - often forced to spend many millions to respond, recover and manage the associated disruption.

This was evidenced in 2020, with various high-profile domestic attacks illustrating the very real threat domestically, and the ongoing impact across our society:

1 in 3 Australian adults were impacted by cybercrime in 2019[1]

$29 bn annual cost of cyberattacks on the Australian economy[2]

61% of executives consider ransomware attacks likely in the next 12 months[3]

62% of small to medium businesses have experienced a cyber security incident[4]

The Federal Government will make the nation's largest ever investment in cyber security, with $1.67 billion to build new cybersecurity and law enforcement capabilities, protect the essential services upon which we all depend, assist businesses to protect themselves and raise the community's understanding of how to be secure online.

This includes the significant investment in the Australian Signals Directorate, known as the Cyber Enhanced Situational Awareness and Response (CESAR) package, to identify more cyber threats, disrupt more foreign cybercriminals, build more partnerships with industry and government and protect more Australians.

This paper takes a focused look at the current ransomware threat landscape including real life case studies drawn from contributing Advisory Committee members. It also provides recommendations to businesses large and small to further strengthen Australian defences.

We will consider:

- the change in the threat actor business model
- the impact of weak controls or outdated software
- the role of strong foundational controls
- the impact attacks can have on small and medium businesses, and essential steps they can action themselves to protect their organisation
- whether cyber insurance is escalating attacks
- the legality of ransomware payment
- the role and obligations of directors
- the disclosure obligations on listed companies.

Given the stakes are so high, organisations need to understand the risks and prepare accordingly, know what action to take in the event of a ransomware attack and have a clear understanding of their legal and regulatory obligations. To put it simply, organisations cannot afford to be complacent.

This is not just good practice – it's good business.

[1] NortonLifeLock (2020), 2019 Cyber Safety Insights Report Global Results, available at now.symassets.com/content/dam/norton/campaign/ NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf?

[2] Microsoft and Frost & Sullivan (2018), Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World

[3] https://www.digitalpulse.pwc.com.au/digital-trust-insights-2021-the-need-for-cyber-resilience/

[4] https://www.cyber.gov.au/sites/default/files/2020-11/ACSC%20Small%20Business%20Survey%20Results.pdf

One of Australia's fastest escalating threats

Ransomware attacks today present a major threat to Australian organisations. In 2020, cyber criminals conducted successful attacks on major Australian organisations at a volume never before experienced. The Australian Cyber Security Centre explained the increased appetite for conducting ransomware attacks by cyber criminals: "...ransomware requires minimal technical expertise, is low cost and can result in significant impact to an organisation, potentially crippling core business functions".

The ability to monetise cybercrime has proved attractive to organised criminal groups, which have developed sophisticated and scalable ransomware software, launched in highly organised attacks and made available 'as a service'. It is cybercrime as an enterprise and poses an increased risk to organisations globally.

An increasingly sophisticated crime

Ransomware business models continue to evolve in scale and sophistication, honing in on bigger targets for larger ransoms. For these criminals, the proportion of victims that pay a ransom is key. Accordingly, anything they can do to increase or leverage payment leads to increased 'profits'.

It is difficult to investigate and prosecute the criminals responsible for ransomware. Many operate with impunity in countries that protect them, ignore them or do not have the legal systems in place to bring these criminals to justice.

Cryptocurrency

At the epicentre of the escalation of ransomware attacks, cryptocurrency is a digital currency secured by cryptography and based on blockchain technology. It is hard to trace, making it ideal for ransomware demands.

Current dynamics have led to ransomware groups developing new techniques, designed to increase the pressure on victims. These include:

Hack and leak: After gaining control of a company's IT systems, cyber criminals search for sensitive files, which are stolen before systems are locked. In the event the ransom is not paid, victims are extorted with threats to publish sensitive information on the dark web.

Targeting executives: Cyber criminals have started to directly target top executives. The techniques include emailing them directly with threats and ransom demands, as well as gaining access to their inboxes, files and computers and stealing their organisation's data which is then used for extortion or blackmail.

Tailored ransom demands: Cyber criminals trawl through stolen cyber insurance certificates, using this information to leverage ransomware attacks, often demanding a ransom payment that is the same as the insured amount. By insisting on payment in Bitcoin or other cryptocurrency, the attacker may remain anonymous and free to attack again.

Using ransomed data

Ransomware attacks increasingly involve the exfiltration of data by the attackers which is then used to extort a ransom. The data is often released by attackers on public or dark web sites.

Extracted data could include commercially sensitive corporate and customer data. Often, the victim organisation is unable to determine the data that has been exfiltrated, until it is released by the attacker. This also means that criminals release data to embarrass victims, particularly if they have publicly denied any data being stolen.

Victims of ransomware attacks need to be aware that data may be leaked over time onto the dark web and could be viewed by competitors, suppliers and customers. There are secondary and tertiary markets where this data can continue to surface, creating a need for continued management focus.

Case study
Netwalker's first strike

Victims of ransomware commonly experience theft of their data prior to the deployment of the malware on their networks. The extracted data is then used for extortion purposes.

In November 2020, the Australian Cyber Security Center (ACSC) received a report of a ransomware attack on a legal services company, which resulted in a partial, temporary outage to corporate systems.

The ransomware exploit was identified as Netwalker, known for exfiltration of data ahead of network encryption. The company's initial investigations were unable to determine whether data had been stolen but it was later discovered for sale on the dark web.

Extent of the impact

In the three months of April to June 2020 alone, there was a 65 per cent increase in cyber security incidents, at an estimated $7.6 billion cost to business for the financial year.

This cost is ultimately borne by consumers, often through higher prices, and is a drag on economic activity. If Australia could reduce cyber security incidents, resources could be used to build productivity, not pay for incident response and remediation.

If attacks continue at this rate, it is forecast gross domestic product (GDP) will be impacted by $86 billion in net present value (NPV) terms over the next decade. To put this in perspective, if this amount was not spent managing cyber security incidents, Australia's GDP would be one per cent higher.

The ACSC has highlighted that fraud is the most common category of cyber incident, but assesses ransomware as the highest threat. This assessment is based on the fact that ransomware requires minimal technical expertise, is low cost and can result in significant impact to an organisation, potentially crippling core business functions.

The ability for ransomware to be maliciously deployed is demonstrated by the effectiveness of April 2020's bulk extortion campaign where thousands of Australians were emailed the threat to release sensitive information to the recipient's friends and family unless they paid an amount in untraceable cryptocurrency. This single campaign in April caused an almost doubling of reports to the ACSC.

Ransomware is not just a cost for large business or individuals but is a threat for small business as well. A US study[1] found that ransomware attacks costs smaller companies an average of US$713,000 per incident, a combination of the expense of downtime and lost business due to reputational harm.

Australian small businesses are important to our economy and our community; they contributed almost $418 billion to GDP in 2018-19, and employ over 4.7 million people[2]. They are increasingly exposed to the threat of ransomware, especially given an increase in e-commerce activity, making access to cyber awareness and support vital.

[1] https://www.acronis.com/en-au/articles/costs-of-ransomware-attacks/
[2] https://www.acsc.gov.au/publications/ACSC-Threat-Report-2020.pdf

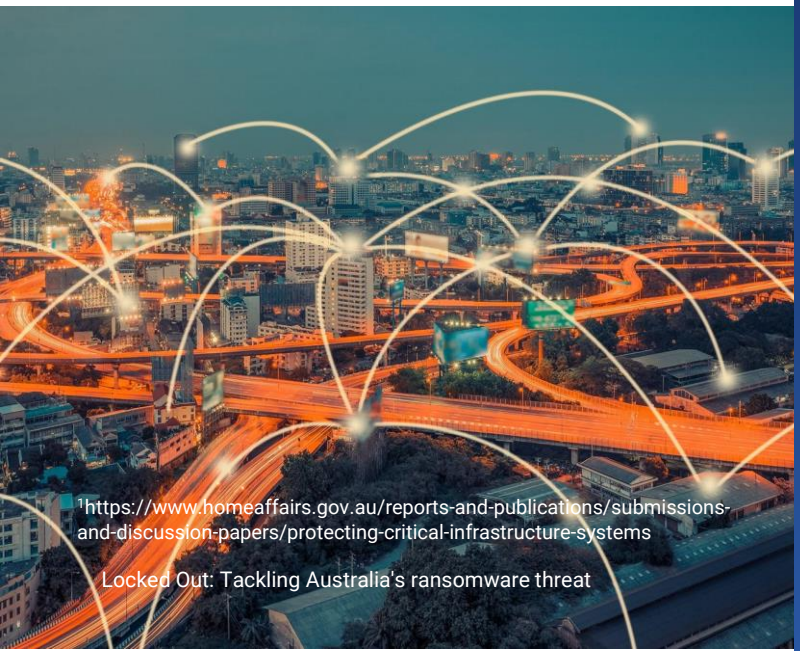
Targeting weakness

As digital complexity within organisations has increased, so too has the challenge of maintaining legacy technology and managing the accompanying ransomware risk. Security updates may no longer be available for legacy technology, creating an entry point for cyber criminals.

Remote access solutions provide a mechanism for an organisation's employees, service providers and partners to remotely access a corporate network, but cyber criminals can take advantage of weak controls or outdated software. Weaknesses in an organisation's website and web-based applications can also be a path to network access, particularly if web applications are misconfigured or the systems that support them are not kept up to date.

The ability to integrate the monitoring of legacy technology with wider systems is central to threat detection. Early detection of a ransomware attack is paramount to minimising impact, but continuous incident detection and response capabilities may not extend to legacy systems. In those instances organisations won't discover an attack until a ransom is requested. Compensating or alternative controls may be required to achieve the same baseline of security monitoring as that achieved in more modern systems.

The targeting of critical infrastructure has seen the Government progress the Protecting Critical Infrastructure and Systems of National Significance[1] reforms, a key initiative of Australia's Cyber Security Strategy 2020.



[1]https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

The value of good cyber hygiene

The reality is that many of the most impactful ransomware attacks could have been avoided with foundational cyber security controls and good cyber security hygiene.

For small businesses, which make up 93% of employing businesses in Australia and provide employment for nearly 45% of Australia's workforce, the challenge is different. They don't have Chief Security Officers, an IT team or possibly even an IT qualified team member, which is understandable when over half employ less than 4 people.

Some argue that market forces will ultimately drive the change required to mitigate the threat of ransomware across the Australian economy. **However, this will not drive change quickly enough to match the evolving threat - organisations need to act now, evolving their cyber strategy to encompass solid controls and hygiene standards.**

This has never been more important. As the potential for critical infrastructure to be impacted increases, so does the threat of more severe economic disruption and very real health and safety risks.

Recommendations for all businesses

All businesses have valuable data and systems they need to protect. It is vital that they establish strong foundational controls and practice good cyber security hygiene practices, including the ACSC's Essential Eight: https://www.cyber.gov.au/acsc/view-all- content/essential-eight

ACSC also provides advice and guidance for:

- Individuals and families
- Small & medium businesses
- Large organisations & infrastructure
- Government

To access, please visit: https://www.cyber.gov.au/acsc/view-all-content/publications/ransomware-australia

Recommendations for small businesses

For small businesses, who often don't employ an IT team, let alone a cyber security qualified individual, the key to reducing the risk of a ransomware attack is having appropriate security controls. The controls detailed below and the guides referenced can allow this to be easily actioned:

Email security
National Australia Bank (NAB) provides a guide to increasing security for email: Multi-factor authentication (MFA) to protect your business.

Multi-factor authentication for email
This reduces reliance on passwords being the only control used to access email systems. It explains what multi-factor authentication is and how to implement it.

Keeping software up to date
An update is a new, improved or safer version of a software (program, app or operating system like Microsoft Windows or Apple iOS) that is installed to provide up to date protection to computers or mobile devices.

To switch on auto-updates, especially for operating systems.

- Regularly check for and install updates ASAP if auto-updates are unavailable, especially for software
- Set a convenient time for auto-updates to avoid disruptions to business as usual
- If Anti-Virus software is in use, ensure automatic updates are turned on

If aged hardware or software is in use, it may not auto-update and therefore leaves your business susceptible to technical, software and security issues. The ACSC recommends upgrading devices and software. It is important to note that Windows 7 and Microsoft Office 10 are not supported after 14 January 2020 and 13 October 2020 respectively.

Small businesses should track software end dates and budget to upgrade the software before the expiry.

Employee Training
Training employees to be better prepared to identify suspicious emails and what to do about them is an important step to increase protection of your business. Employees are a key part of protecting a business because all it takes is one click on a link to become a victim of ransomware.

A number of security awareness training resources are available for small businesses:

- NAB's Cyber safety for small and medium business owners
- ACSC's Know how to spot phishing messages

Telstra's Active Scam CrowdSupport page provides an update on current scams to be aware of and can be worthwhile checking if you do spot anything suspicious.

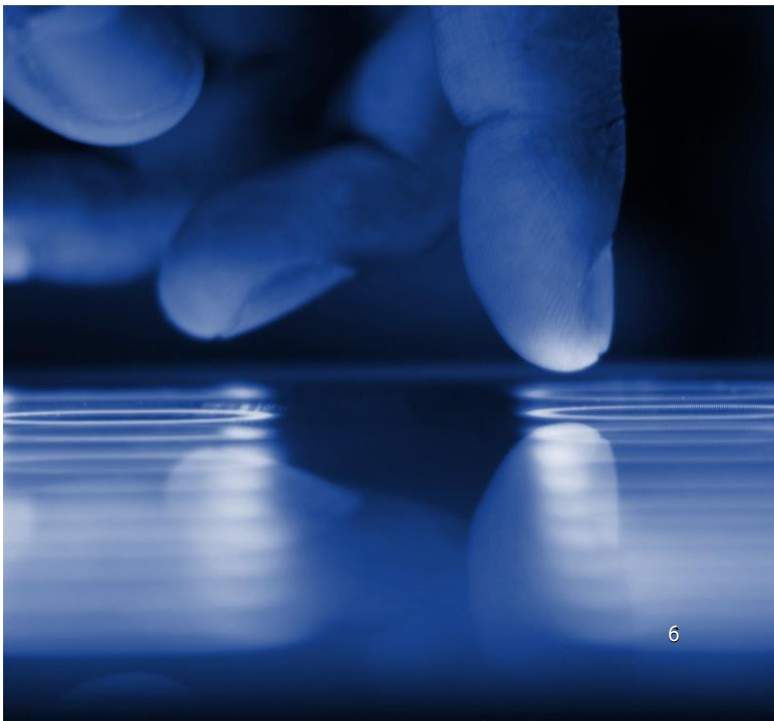
Back-ups
ACSC's Step-by-Step Guides provide advice on how to back-up your data, so you can recover it if you are victim of a ransomware threat.

Data lifecycle management
Reduce the data which can be impacted by an attack by archiving data over 15 months old.

Built in security features
There is also a guide to taking advantage of built in security features for software you may use.

For these tips, we have used the following practical guides to implementing security:

- ACSC's Small Business Cyber Security Guide
- NAB's Safety tips for business



Learning from one another

Case study
Bringing a wholesaler to a halt

In 2019 the operation of Australian business, wholesaler Heat Group, came to an instant halt. A malicious attacker had infiltrated its systems in a ransomware attack. The business was incapacitated, unable to process, ship or pack orders.

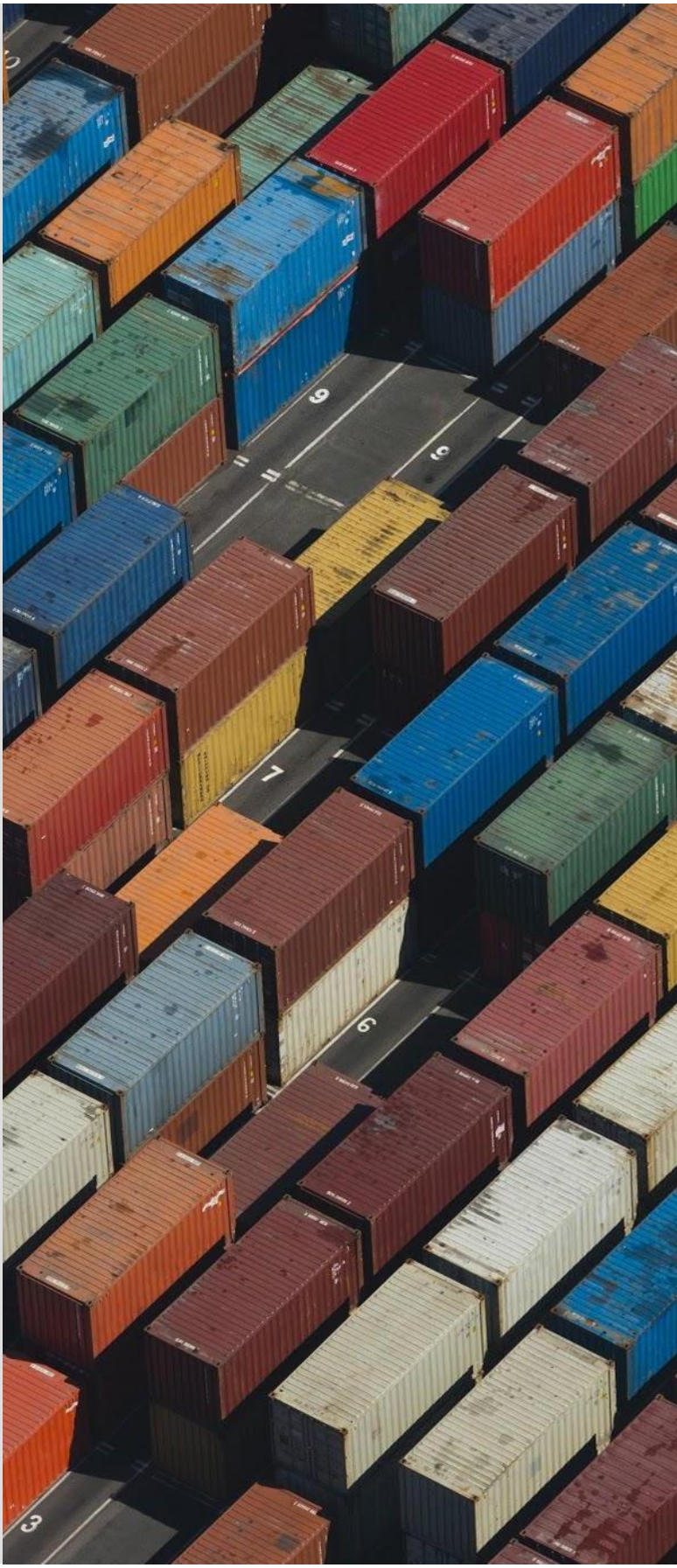
Heat Group is responsible for distributing a portfolio of more than 40 brands across beauty, healthy living and confectionery to more than 7000 retailers - it's a business which many other businesses rely on. The long-term danger was worse. Twenty years of sales history, employment details and customer trading terms were captured.

Heat Group had two options. Attempt to pay a Bitcoin ransom on the promise all its business files would be decrypted and handed back, or bring in a team of IT specialists and attempt to recover the data.

What followed were four days of around-the-clock work to get the business into a position where it could trade again, which remarkably only took 5 days.

In total, the company estimates it lost around $2m in cash and it was a month before the whole business was back online and all files were restored. It later learned those files had been sold on the dark web for US$3,500 (AU$4,750) with the malicious attacker linked to a range of other attacks, directly impacting at least another 15 Australian businesses.

Business owner Gillian Franklin has a simple message for other Australian businesses: "Assume you may be hacked one day and prepare for this, have all your records accurate and up to date and backed up remotely. Use double authentication security levels and test and train your staff very regularly."



Learning from one another

Case study

Attacking a community through its carers

Like many small businesses, pharmacies rely heavily on their IT systems and even more so on their data. Health data is critical for the safe and effective dispensing of medications, and the cornerstone of their financial model, with payment from the Public Benefits Scheme (PBS) dependant on that data. Without it, pharmacies can lose significant revenue.

Despite that critical dependency, investment in cyber security has been adhoc across the industry. While anti-virus software is common, for most it is the extent of their cyber security defences and adding to their exposure, anti-virus can easily be circumvented.

Business continuity and disaster recovery planning is seen as a significant issue to be addressed within all organisations - including small business. Two recent examples highlight the differences in impact based on levels of preparedness:

Pharmacy A. A staff member clicked on an email believing it was from a supplier. Unfortunately it was not and within minutes all PCs were locked, with a ransomware demand across the screens. The attack had bypassed the small businesses anti-virus software and disabled access to the critical files and point-of-sale system. The pharmacy could not dispense or trade.

Fortunately the businesses IT provider had an encrypted backup in place (both locally and in the cloud) that had not been infected. The pharmacy's PCs were cleaned and within 24 hours they were up and trading again - but not without significant damage done. However, the loss of trade, reputational damage (including not having vital health data available) and restoration costs could have been avoided, or the risk significantly reduced, if security awareness training of staff had occurred, and the business had more advanced technology in place.

Pharmacy B. Upon opening the pharmacy one Saturday morning the staff immediately realised something was wrong. The primary dispensing PC, which housed their dispense database, was locked with an on-screen ransomware demand stating the businesses files had been encrypted and a ransom in bitcoin must be paid for their recovery.

The staff immediately contacted their dispense provider for assistance. Unfortunately they did not have a working backup and had nothing to restore from. They had a deep mistrust of paying the ransom and instead made the difficult and only choice to start again with a blank database, losing all their history.

These events played out over a number of days, with the ongoing issues of dealing with unhappy customers lasting weeks. On top of the reputational damage and direct costs, the stress resulted in the resignation of a key employee.

Cyber insurance: panacea or problem?

Australia's cyber insurance market has evolved materially over the last few years. Though it's relatively immature compared to international markets (particularly the US and the UK) uptake continues to increase. Many organisations now hold some form of cyber insurance and require their vendors to do the same, and the trend is expected to continue.

The scope of cyber insurance is broad, covering costs associated with incident response, business interruption, system damage and regulatory obligations (including fines) and policies often provide for "extortion" costs, including reimbursement of ransom payments. This feature is causing some concern.

Enabling payment through this mechanism plays into the hands of the threat actors. It "legitimises" the payment of ransom, and can create complacency within an organisation, shifting risk management focus away from cyber resilience, preparedness and readiness.

It may even go one step further and encourage ransomware attacks. Threat actors don't care about the source of the ransom payment and insurance policies make payment an easy "solution". Recently threat actors have stolen data including cyber insurance certificates then demanded ransom for the insured sum.

The critical takeaway is that organisations should see cyber insurance as one component of a holistic cyber security program, not as a replacement for one.

Case study
Lessons from leaders. Thomas Knudsen, Toll Group Managing Director

The cyber incident that impacted Toll was described, at the time, as one of the most significant in Australian corporate history. As you would imagine there were immense learnings from the cyber-attacks that impacted Toll last year both in the actions needed to prevent an attack and and in the response and remediation to the attack.

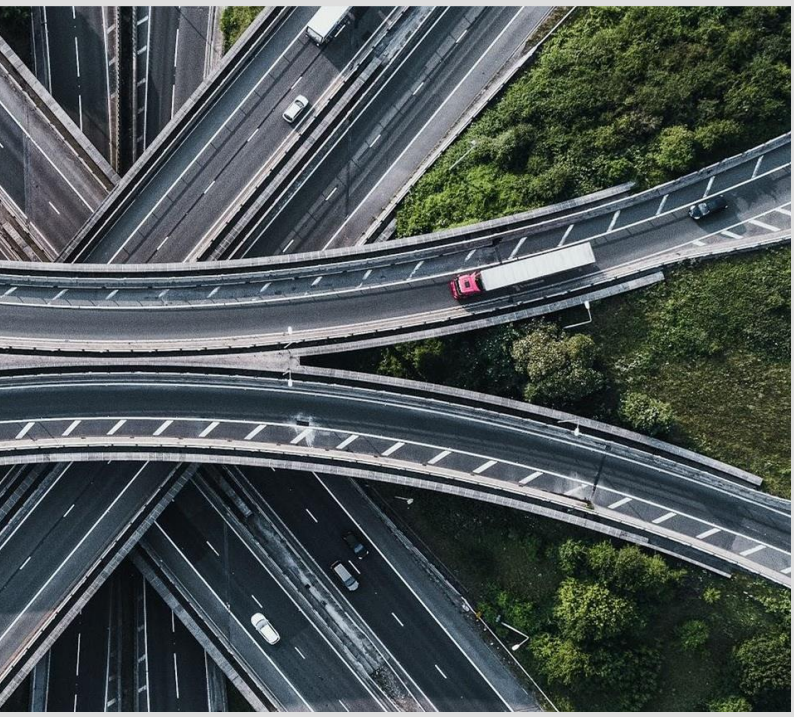
From a positive perspective, the events certainly provided us with the opportunity to contribute to a growing knowledge bank to help inform an all-of-community effort to understand and combat the threat and impact of large-scale cybercrime.

What was your first reaction when your team confirmed that a major ransomware attack had struck Toll?

Of course, it was shock. Once we understood the magnitude of the attack it was clear this would regrettably impact every area of our business – customers, suppliers, and employees.

We immediately activated our Crisis Response Team. As with any cybercrime of this nature it took some time to assess the severity of the attack. Toll has strong crisis management protocols and we swiftly put in place our Business Continuity Plans (BCPs) so we could continue to service our customers.

Let's be clear. This was an unscrupulous attack. At the time, and still today, I strongly condemn the actions of the perpetrators.



What factors did you consider when deciding if Toll would pay the ransom?

In line with our values, at no point did Toll consider paying the ransom. We were of the firm belief that this would only encourage future criminal enterprise.

What impact did the incidents have on Toll and your customers and how did you manage this?

The cyber-attacks cause a very serious and regrettable situation and it resulted in significant impact on our ourselves and many of our customers, particular in the early stages. We were very focussed on methodically and quickly bringing systems back online, but with a Risk and Security focus being a priority over expediency.

We focussed on core services first to ensure we were minimising customer impact. We worked closely with customers to align with their priorities, both in terms of service (what was most important to bring online first) but also security and risk (ensuring that they were comfortable with controls that were in place). This is where our BCP was critical.

Following the events of 2020, the Toll Board endorsed a comprehensive cyber resilience program with 30 streams of work covering all aspects of Information Security. The cyber resilience program includes the global rollout of a new cyber awareness program - 32,000+ hours of cyber training across our workforce has been undertaken to date, we have strengthened detection and response capabilities across 16000+ endpoints and improved IT stability by 42 per cent.

We've continued to communicate extensively with customers and partners about the actions we are taking to improve our resilience. This has been critical in re-establishing trust and confidence.

With your experience, what would you advise a CEO at another company to consider about cyber security risks, and specifically, ransomware attacks?

Do not underestimate the importance of a strong security program and culture. It's important to think about scale and impact, and whether your organisation is equipped to respond effectively and to mitigate the fall-out.

Take personal interest. I (Thomas) am personally involved in Toll's cyber resilience program and I sit on the steering committee for that program.

It's also crucial to really understand your IT team's concerns. Get into the detail with your IT department and security teams about how you and other executives can help to drive appropriate risk decisions.

Ransomware and the law

While it is crucial that organisations understand how to prevent a ransomware attack, following an actual attack the focus often moves quickly from the technical to the legal implications.

In certain circumstances, ransomware payments may be unlawful under Australian law. The “instrument of crime” provisions contained within the Criminal Code Act are broad and the available defences (for example, duress) are narrow. There are also various sanction laws that may apply.

If an organisation pays a ransom to a threat actor, whether directly or indirectly, there is a real risk the payment may be used in the commission of further offences. Given the profile of the threat actors, there is also a risk that funds may be used by terrorist organisations or paid to sanctioned entities or countries.

ACSC’s advice regarding ransomware payment is clear - do not pay. Payment may be illegal under certain circumstances.

But for an organisation which is under attack the decision to pay or facilitate payment of a ransom can be further complicated - and pressured - as the legal position is unclear. At worst, payment of these amounts may be unlawful and involve committing a criminal offence.

Ransomware – Current legislative regime

Instrument of crime offences: Under the Criminal Code Act, it is an offence to “deal with” money or other property if: (a) there is a risk that the money or property will become an instrument of crime, and you (b) are “reckless” or “negligent” as to the fact that the money or property will become an instrument of crime.

Terrorism funding offences: Under the Criminal Code Act, it is an offence to “make funds available to a [terrorist] organisation” if you either (a) know that the organisation is a terrorist organisation, or (b) are reckless as to whether the organisation is a terrorist organisation.

UN sanctions laws: Under the Charter of the United Nations Act (which implements UN Security Council sanctions), it is an offence to (a) transfer assets to sanctioned people and entities or (b) contravene UN sanctions enforcement laws.

‘Due care and diligence’: Ransomware and directors’ duties

The risk of a ransomware attack, the company’s preparedness for an attack, as well as its response to any actual attack, are all matters of such significance to an organisation that its board of directors would, pursuant to their duties to the company and their obligations under the Corporations Act, be expected to have appropriate oversight. For small and medium business, the directors’ responsibilities are equivalent to a larger enterprise, a fact which directors of small and medium business need to be aware of.

Obligations

- While directors are not expected to be experts in cyber risk and ransomware attacks, they need to have a level of understanding to oversee and challenge, where necessary, what management is doing to address the risk and manage any issues. They also need to be equipped to make independent assessments on the capability of the experts advising the company and whether they can rely on their advice.
- Following a ransomware attack directors will need to consider whether it is legal for the company to pay the ransom. If it is not, then the directors risk personal liability under ASIC’s stepping stone liability approach.

Getting prepared

- One important action for directors and executives is to ensure the organisation's crisis preparation includes recovery and response planning specifically for ransomware attacks.
- Ransomware attacks require additional considerations which require a targeted strategy for the whole organisation. This includes ensuring all business units have a plan to manage a ransomware attack.
- A lack of preparation can lead to knee-jerk responses and an increased impact on the victim, often extending the time it takes to restore operations. BCPs are typically designed to run critical business processes for 48 to 72 hours. Yet, an impactful ransomware attack can last weeks.
- Directors should encourage management to secure sufficient cyber coverage.

Making it personal

- Importantly, there has also been a trend towards threat actors directly targeting directors and executives personally, in the hope of blackmailing them into paying the ransom.

Corporate disclosure

Ransomware attacks can have significant and enduring effects on the market value of a company.

In Australia, there are strict obligations to notify various regulators of data breaches and cyber security incidents, including obligations under the Privacy Act, the Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234 and the EU’s General Data Protection Regulation (GDPR). Proposed reforms to Australia’s critical infrastructure legislation are also likely to increase this reporting requirement.

Under the Corporations Act and the ASX Listing Rules, listed companies must notify the ASX of ‘market sensitive’ information immediately – that is, information that would, or would be likely to, influence investors in deciding whether to acquire or dispose of securities.

A significant ransomware attack has the potential to affect the market value of a listed company. Disclosure may be required and failure to disclose could result in both civil and criminal action.

Case study

In October 2020, an ASX-listed media monitoring company fell victim to a REvil ransomware. The incident impacted hundreds of servers, compromising the majority of internal systems and resulting in extensive disruption to core business functions. As a result, the company was incapable of providing its services to consumers.

Most of the company’s backups were also impacted by the ransomware and available offline backups did not cover all necessary servers. The spread of the infection was only interrupted by the company identifying and changing the password of the administrative account cyber criminals were using to install the ransomware.

The company had to work around the clock to rebuild its networks and regain the trust and confidence of their customers. The total cost of recovery was in excess of $7 million.

Stop the spread: Key questions all organisations should be prepared to answer

- What data is valuable to your organisation? Who would your organisational data be valuable to? What data would cause your organisation damage if you lost access to it?
- Where is your data stored? Onshore, offshore or in the cloud? What arrangements are in place to ensure storage is secure?
- How secure are your service providers (and the arrangements in place to ensure security) and have they shared your data with other third parties?
- Who is protecting your data and how is it being protected? What security systems currently exist?
- How prepared are you to respond to any breach? Do you have a breach response plan in place? One that aligns all parts of our business (technology, PR, comms, legal, regulatory, etc)?
- What is your position on ransom demands? Are you clear on your legal position and your fiduciary obligations?

If your business is the victim of a ransomware attack the first port of call should always be your Chief Security Officer (or similar).

For a small business, the first point of contact should be the ACSC's Australian Cyber Security Hotline – 1300 292 371

You should also, where possible, seek professional advice around responding to the incident and getting your organisation back in business.

The ACSC recommends you do not pay any ransom, as there is no guarantee paying will reduce the threat to your network and can make you vulnerable to future attacks.