WHITEPAPER

Protecting data in a threat landscape

Frontier
software

www.frontiersoftware.com

Every modern organisation is collecting digital data at an astonishing pace. The storage of such data in connected networks has led to an explosion in the amount of nefarious activity designed to access, steal, or hold it to ransom. Assuming the umbrella description of 'cybersecurity', government and private sector organisations are waging war with an enemy that is unseen, highly competent and always looking for vulnerabilities. Without sound processes to defend against these attacks, organisations risk considerable loss, both of reputation and revenue.

This whitepaper seeks to define cybersecurity and its global scope. It then discusses the challenges inherent in combatting cyberattacks and what organisations can do to protect their data and mitigate their losses in the event of a data breach.

What is cybersecurity?

Kaspersky Lab, a provider of security services to more than 270,000 corporate clients, defines cybersecurity as, "the practice of defending computers and servers, mobile devices, electronic systems, networks and data from malicious attacks." Such definitions conjure up images of nation states and anonymous hackers. To an organisation trying to protect its data, cybersecurity is more about getting the right information to the right people at the right time, whilst stopping the wrong people from ever accessing it.

Sources and types of attacks

Devices (eg, laptops, desktops, servers) that can host software		
Methodology	**Definition**	**Examples**
Malware	Code designed to cause much expensive damage.	**Phishing:** Attempting to deceive a user into providing confidential information by impersonating another organisation or provider. **Spam:** unsolicited messages, often acting as advertising. Email, instant messaging and even unsolicited phone calls can actually be spam.
Keylogging	Software that can collect all keyboard input.	
Social Engineering	Having a user divulge confidential personal information under false pretences.	
Computer Networks are a favourite source of information and may be attacked actively or passively.		
Methodology	**Definition**	**Examples**
Active Attack	Where a hacker installs malicious code designed to sabotage network and computer performance.	**Spoofing:** a situation in which a person or program successfully masquerades as another by falsifying data, to gain an illegitimate advantage. **Modification:** where an intruder re-directs information to a different destination. **Fabrication:** Seeks to create illegitimate information, processes, communications or other data within a system. **DDoS:** A Denial of Service attack seeks to overwhelm network capacity by flooding the network with traffic.
Passive Attack	Where a hacker gets into a network and intercepts data exchanges within the network. It is dangerous as it is often very hard to detect.	**Sniffing:** An attacker detects and reads information between sender and receiver. There are no changes in the data. **Supervision:** Attack where hackers can read confidential data, but cannot edit it.

Cyber threats come in many guises but fall into three broad camps; those that seek financial gain (eg ransomware), those that seek to steal identities and those designed to effect a denial of service, often directed at public infrastructure, such as power producers or other heavy industrial operators.

The Australian Cyber Security Centre (ACSC) also agrees that ransomware is a major problem. According to the *ACSC 2017 report*, "increasingly sophisticated exploits are being developed and deployed against well-protected networks, particularly government networks."

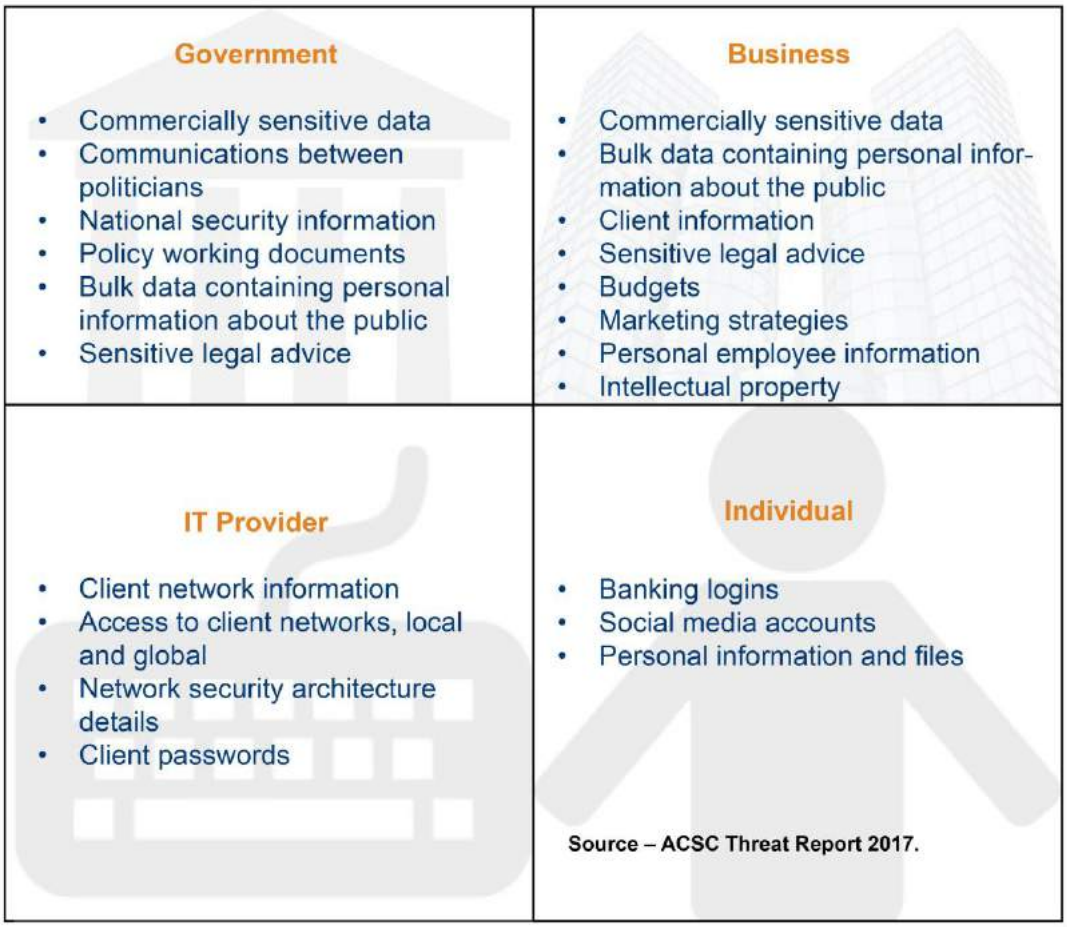
The scale of cybersecurity and data breaches

Organisations amass huge amounts of data. Government agencies and private corporations routinely gather personal data about the clients who use their services. Accumulating large volumes of data enables organisations to leverage knowledge and develop insights, but it also requires vigilance as unauthorised access to such data threatens privacy, reputation and even financial viability.

As Darren Hnatiw, CTO at Frontier Software says, *"modern organisations are in the business of data. Cyberattacks can put your data in the hands of unscrupulous people, who will keep it, change it or delete it. Sometimes, organisations don't find out for months and by then it's too late."*

For hackers, the data potentially available is immense and varies based on the source. The table below gives examples of the data types unscrupulous actors will target.

Potential data sources



According to the *Internet Organised Crime Threat Assessment (IOCTA) report* of 2017, data breaches alone led to the exposure of more than 2 billion data records of EU citizens. Remember, that figure only reflects official statistics. In Australia, in the quarter to March 2018, there were 63 data breaches reported to the *Office of the Australian Information Commissioner (OAIC)*. Of these, the health services industry made up 24% of breaches, followed by business services providers at 14%. Most data breaches reported to the OAIC involved contact information, such as an individual's name, email address, home address or phone number. This is distinguished from identity information, such as driver licence numbers and passport numbers.

The recent rollout of GDPR[1] legislation in Europe has placed further pressure on organisations worldwide to comply with the most stringent privacy controls ever imposed. Failure to do so could result in significant fines of up to 4% of global turnover. The flow-on effect on measures taken by organisations to protect access to identifiable personal data, only serves to illustrate the importance that governments and private organisations are placing on information security.

What is it costing?

The Gartner 2018 CIO Agenda Survey of more than 3000 CIOs ranked cybersecurity as the second highest priority item, behind Artificial Intelligence. Cyberattacks, such as WannaCry and NotPetya, impact corporate security spending because these types of attacks can persist for up to three years.

[1] For more information on the GDPR, see our eBook, "Is your payroll ready for GDPR", available on our *website*.

Gartner predicts spending on information security to top $US114 billion globally in 2018 and expects this figure to grow by 9% in 2019. Gartner estimates spending on security in Australia for 2018, will be $AU3.8 billion.

The way organisations think about cybersecurity has evolved. The typical stance taken by public and private entities on the question of breaches is not one of 'if', but 'when'.

Adopting the viewpoint that vulnerabilities exist and can be exploited, organisations are developing plans to minimise the likelihood and mitigate the impact of a breach they see as inevitable. They are investing in technologies designed to predict and identify breaches and the methods employed to enable them.

Challenges in cybersecurity

Organisations seeking to implement cybersecurity practices face several barriers to success.

Perpetrators are forever innovating

The sophistication and capabilities of those who want to manipulate or steal your data compromise your email or hold your systems to ransom, is developing all the time. These players operate using technology that innovates at a frightening speed. Prevention measures must always be assessed in light of the adaptability of the threat landscape. Victor Miloshis, National Technical Support Manager at Frontier Software says, *"The latest cybersecurity advice, centres on an approach of continuous monitoring and real-time assessments."*

Lack of cybersecurity skill sets

The enterprise IT consulting firm, Enterprise Strategy Group (ESG) completes an annual survey on the state of IT, quizzing CIOs in the US and Europe. In 2018, ESG found that 51% of its 600+ respondents claimed their organisation had a 'problematic shortage' of cybersecurity skills. Set against a landscape of continual threat and combined with a relentless push for digital transformation, organisations are right to be concerned. Scarcity has increased demand for cybersecurity skills and qualified candidates are often pricing themselves beyond the reach of all but the biggest employers.

Education providers have only recently offered formal courses in cybersecurity, which should attract the students capable of succeeding in the field, but this initiative will take time to alleviate demand shortfalls.

The threat and opportunity of Artificial Intelligence

Artificial intelligence is being singled out as a potential combatant against cyberattacks. Machine learning models that can predict and identify attacks could be a readily deployed defence against the growing threat landscape. At work 24 hours, 7 days and not needing breaks, AI could potentially fight a virus as it was downloading rather than after it had inflicted damage. Although AI could launch an attack, identifying potential vulnerabilities and targets, AI experts argue that it is not yet sophisticated enough to launch anything truly nefarious.

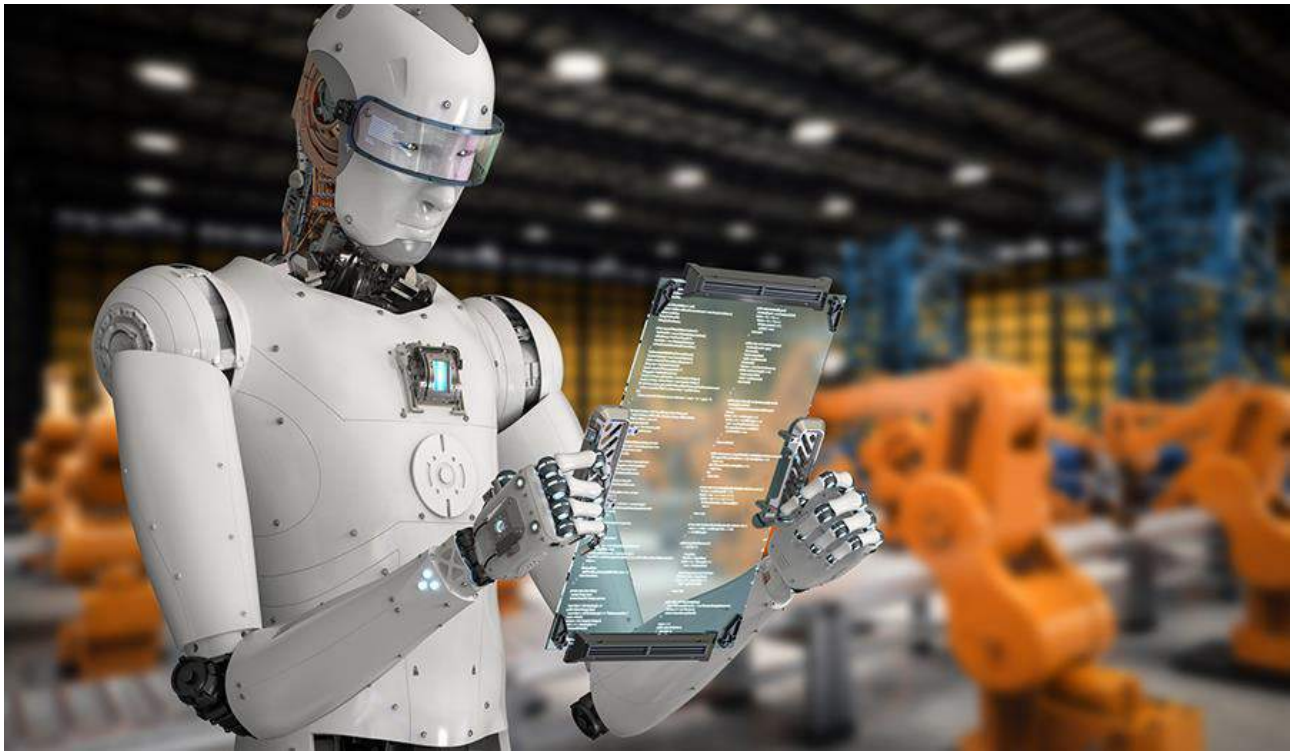
The onslaught of ransomware

Most of the current ransomware attacks encrypted files on the infected system and some will even erase files or block access to the system. Once access is blocked, the ransomware demands a ransom in order to unlock the files. More recently, ransomware variants have included unauthorised copying or transmission of data and participation in distributed denial of service (DDoS) attacks. Others delete files regardless of whether or not a payment was made. Businesses not employing the measures discussed below, or whose employees are not vigilant about clicking on email links or attachments, will always be at risk from ransomware. The WannaCry and NotPetya attacks alone infected over 300,000 computers in May and July of 2017.

The internet of things

Technology is creating ever more sensor-laden, internet connected devices. The so-called, 'internet of things', presents challenges to cybersecurity as it is a potential weak point in cyber defences. Such devices often lack basic security features or are not configured to use custom passwords. Basic AI and sophisticated hackers are identifying these sorts of vulnerabilities to target using default passwords. When attacks do occur, they come as botnets mounting large-scale attacks that capture and export data or find further vulnerabilities. The emerging trends of Bring Your Own Device (BYOD) and the employment of contingent workers, further increases the risk of data breaches.

Hnatiw reminds us, *"Developing a comprehensive cybersecurity position is not a quick process, but it is possible. One of the biggest challenges faced by CIOs is gaining a company-wide commitment to the changes and governance required to bed it down."*



What can you do

There is a well-known saying in IT circles, "good security is built in, not tacked on." Inadequate IT security for internet-facing entities will continue to result in sensitive data being unlawfully accessed, exfiltrated and disclosed every year. Defending a network from compromise is far less costly than dealing with the aftermath of a compromise.

Organisations must view cybersecurity as a fundamental business practice or risk it becoming a reactive response when critical vulnerabilities cause actual harm. Miloshis adds, *"In addressing matters of risk, guardianship and trust, our mission is to get cybersecurity right for ourselves. In doing so, we get it right for our clients."*

The Australian Signals Directorate's (ASD) Essential Eight provides a prioritised list of actions that organisations can take to enhance IT and network security. These actions offer defences to the threat landscape and are considered to be the baseline for Australian organisations.

Whitelist applications

Application whitelisting refers to the maintenance of a register of authorised applications and code that may run on a network. This prevents users from running unauthorised or unlicensed software in an IT environment. Whitelisting can also prevent malicious code, not yet detectable by gateway scanning technology, from being introduced to an environment.

Patch applications

This process ensures that software deployed throughout an organisation has all the relevant vendor-supplied patches applied. Malware uses known software vulnerabilities to access and proliferate within a network. Once access is gained, the malware is used to grant the same access as the authorised user and to execute ransomware, impacting data to which the user should have access. Keeping applications up to date minimises the potential vulnerabilities that can be exploited.

Configure MS Office macros

MS Office macros should be disabled as they may be obtained from external sources. This presents considerable risk as macros have been commonly used to download and execute malicious code. Even if a user opens a document with embedded macros, they remain dormant when macros are disabled system-wide.

Harden applications

Application hardening refers to the process of protecting applications by making them less susceptible to attack. A common means of attack is via untrusted code in web browsers that can be executed on a user's machine. Software such as Adobe Flash and website banners have been exploited to deliver malicious code and it is suggested that organisations disable Flash and other common content delivery mechanisms on internet connected devices.

Restrict administration privileges

Restricting administration privileges refers to the practice of restricting access to administration accounts to authorised staff only. That access is then further restricted to only those tasks deemed imperative. When administrators use privileged accounts to perform general duties, the risk of malware infection and dispersal is significantly higher as privileged accounts operate with greater access levels than normal user accounts. In addition, those accounts may have the ability to change the configuration of the wider infrastructure or provide an attacker with the ability to move elsewhere within the network.

Patch operating systems

This practice ensures that operating system software has all the relevant vendor-supplied patches applied. Malware uses known software vulnerabilities to access and proliferate within a network. Operating system attacks will often seek to change access privileges or capture user information by mimicking other, legitimate software.

Employ multi-factor authentication

Access to a system is made more difficult when additional elements, other than just user-name and password, are required to authenticate a user. Name and password combinations can be guessed or cracked via brute-force techniques[2]. Users who employ the same password for multiple systems are doubly at risk. Access via multi-factor authorisation uses one level of authorisation to trigger a second level, thus increasing the security. A good example would be Apple or Google requiring additional codes that are sent to a personal device, such as a phone, to be entered before permitting access.

[2] The most common example of the brute-force attack is the use of a dictionary attack to crack the password. In this example, the attacker uses a password dictionary that contains millions of words that can be used as a password. The attacker then tries these passwords, one by one, for authentication. If the dictionary contains the correct password, the attack will succeed.

Perform regular backups

When efforts to protect data have failed, organisations will rely on backups for restoration. Completing regular backups ensures organisations have 'latest state' data, accurate to within a number of hours. Storing backups separately to the main infrastructure protects them from cyberattacks and physical threats. Testing of backed up data to ensure it is retrievable, is a critical step in this process.

Although the Essential Eight provides organisations with the basics, there is much more that can be done to embed testable, systematic and repeatable processes around information security. Importantly, all levels of the organisation can be involved.

Management

Organisations must educate C-suite managers to understand cybersecurity and the associated risks. As users with access to sensitive corporate information, hackers often target C-suite managers for ransom attacks. Managers must therefore understand how their online behaviour can impact information security. Importantly, organisations need to understand that regulators will chase the board and/or CEO when things go seriously wrong.

All managers must show support for, and commitment to, cybersecurity initiatives. CIOs should engage managers with regular updates on security initiatives, news of reported breaches and spear phishing attempts, directed at managers. In addition, CIOs could use updates to present industry benchmarks, such as the Essential Eight, and a comparison of their own organisation to recommended minimums.

Employees

Every employee has to take responsibility for securing their organisation's data. It only takes one open infected email, or a stolen unprotected device to cause serious harm and employees must be cognisant of this. As a rule, employees are not actively thinking about data security, so building conscious awareness is of paramount importance.

Miloshis says, *"Our actions and responses need to be driven by the real threat of exploit. Organisations must provide constant reminders of proactive awareness and defence behaviours that employees should be exhibiting."*

Organisations must adopt communication and education campaigns to increase awareness of the means by which breaches can occur and the behaviours that will minimise their occurrence. Through quizzes, videos or regular bulletins, employees must understand the dangers and the mitigating behaviours required to create a culture of active cybersecurity awareness.

Developers

Organisations that employ developers must be even more vigilant. Hackers target the code written by developers to find vulnerabilities they can exploit. As Gartner warns, the application layer holds 75% of vulnerabilities and developers must be careful to vet and test every line of code. A skill set that developers must possess is training and experience in secure coding.

CIO's should also embed cultures where:

- developers review code as though they were a hacker
- developers keep on top of web application security by following organisations such as OWASP and their Top Ten Project
- sessions are regularly held with developers and security specialists to discuss found vulnerabilities and how to prevent them by secure coding
- security testing processes form part of the software development life-cycle.

Information security management system

Organisations seeking to implement stringent information security controls must develop an Information Security Management System (ISMS).

An ISO 27001-compliant ISMS is a set of policies, procedures, processes and systems that manage information risks, such as cyberattacks, hacks, data leaks or theft. Unlike the Essential Eight, an ISMS covers not only preventative activities, but also details processes to follow in the event of a breach. It offers a systematic approach to managing sensitive company information that includes people, processes and IT systems. Importantly, the standard adopts the "Plan–Do–Check-Act" (PDCA) model which is applied to all ISMS processes:

Darren Hnatiw agrees, *"The ISMS identifies, assesses and manages both internal and external security risks. The ISMS equips organisations to manage the risk of a cyber event occurring and then minimises the impact if an attack is successful."*

For any organisation, cybersecurity must be considered in light of the impact that a breach would have on its client base.

Conclusion

Cybersecurity is a challenge faced by every user of an internet-connected device. Despite organisations spending billions of dollars on prevention, prediction and mitigation, the threat is mutable and dynamic. Organisations need to develop and support multi-layered strategies that can respond to new and evolving threats. Success delivers the benefits of data-driven insights and decision making, but a breach may cause damage that is significant enough to ruin brands or even an organisation's future viability. Every business need not consider whether they must take steps to ensure data security, but to what degree.