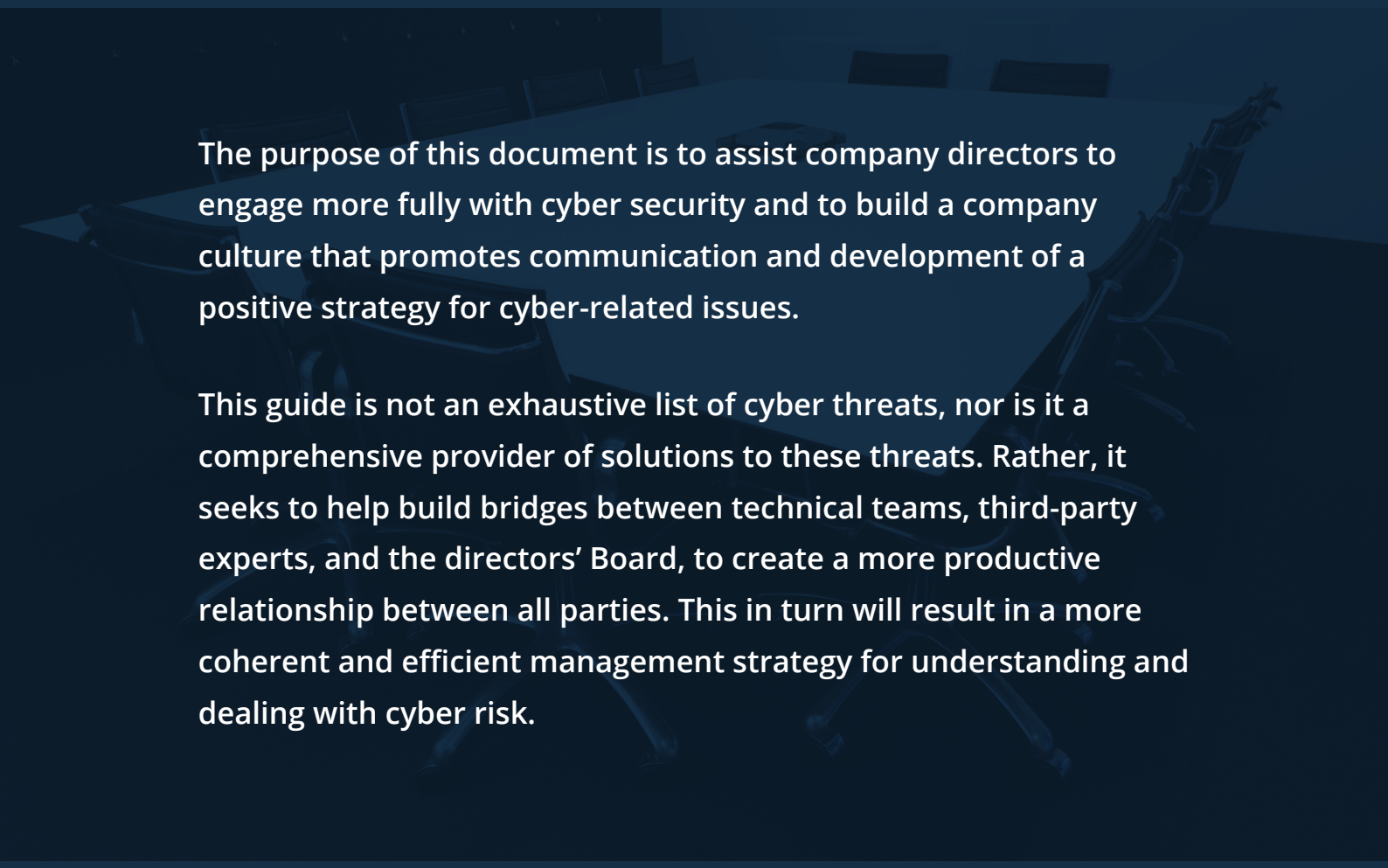
CHANGING THE CONVERSATION ABOUT CYBER SECURITY IN BUSINESS

A Guide for Board Directors



The purpose of this document is to assist company directors to engage more fully with cyber security and to build a company culture that promotes communication and development of a positive strategy for cyber-related issues.

This guide is not an exhaustive list of cyber threats, nor is it a comprehensive provider of solutions to these threats. Rather, it seeks to help build bridges between technical teams, third-party experts, and the directors' Board, to create a more productive relationship between all parties. This in turn will result in a more coherent and efficient management strategy for understanding and dealing with cyber risk.

Getting Motivated

Years of complicated, dry and technically driven digital security presentations, a general lack of communication and fear-driven expenditure have created a culture of uncertainty and distance between directors and security teams. This needs to change: directors' Boards need to engage, be concerned, and hold security officers to account. They need to retake the driver's seat in constructing proactive strategies to manage the risk of a cyber attack.

WHY SHOULD THE BOARD CARE?

Put simply: company self-preservation, financial cost, and legal obligation.

In the first instance, a successful cyber attack may lead to data loss (either company or client), system failure and logistics breakdown, or result in being held ransom to demands which can be variably motivated. Any of these will incur **not just a direct financial cost** resulting from ransom, loss of trading days, and clean-up processes, but also future financial loss as a consequence of **damaged reputation and the emergence of competition** resulting in the loss of custom.

Non-financial risks have financial implications.

If this still doesn't sell the importance of cyber security, then it must be understood that **there is an increasing legal obligation to protect personal data** held by businesses – both of company employees and clients. Failure to do so can lead to fines, market devaluation, and even lawsuits, as recent cases have demonstrated (see Box 1 below).

BOX 1 | THE UBER DATA BREACH, 2016

Timeline: **2 years** (2016-18)

Outcome: **Ransom**-like pay off, **settlement** pay out, new policy enforcement by regulators

Cost: **USD 248 million** (direct) + other clean-up costs and significant **reputational damage**

Taxi giant Uber was successfully infiltrated in a cyber attack which compromised the data of 57 million user accounts and included 600,000 driver's licenses: both employees and clients can be affected by a cyber attack.

The company failed to disclose this attack for almost a year by paying off the hackers with USD 100 million. They then settled an ensuing lawsuit in 2018 by paying out USD 148 million. Over the period, Uber endured significant embarrassing media coverage making this an incredibly damaging incident for the firm.

Importantly, as part of the settlement, **Uber was also required to reform its business culture** to better manage cyber risk. This **included appointing an executive** whose role it was to design a new cybersecurity framework and **to report to the Board of Directors**.

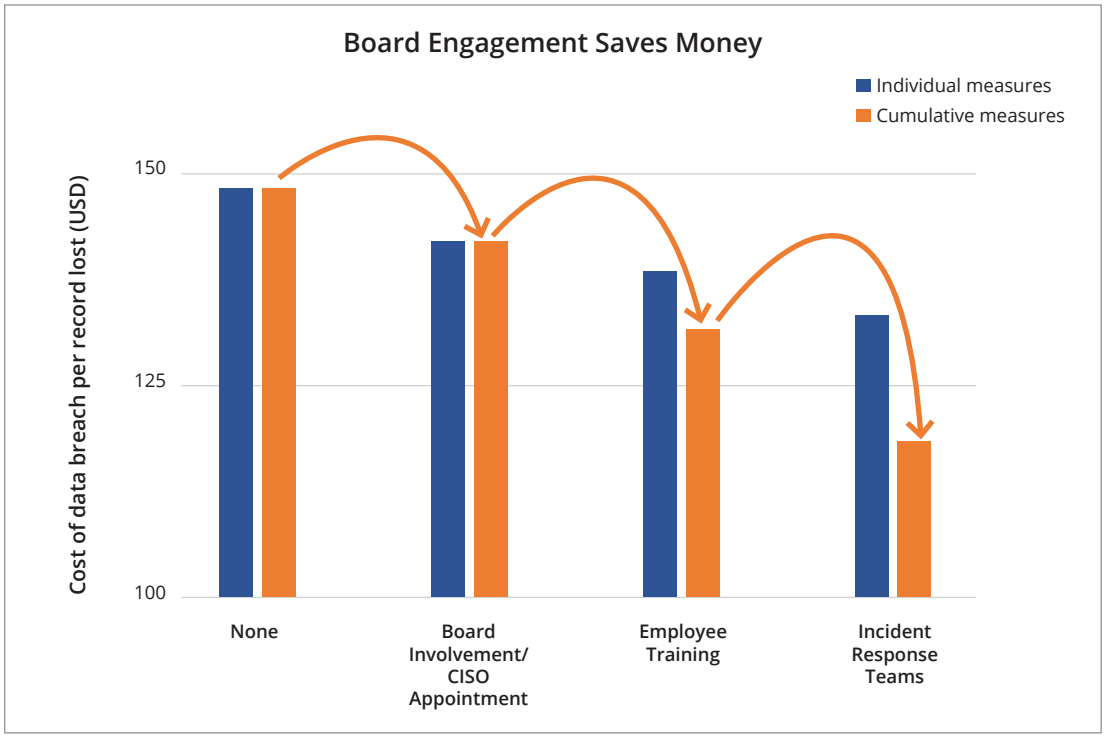
WHY IS THE ROLE OF THE BOARD IMPORTANT?

The Board makes the difference to the digital security of a company by driving policy and ensuring effective strategies are in place. Furthermore, the Board plays a critical role in ensuring an **efficient flow of information** between different parts of the company as well as external parties, either in terms of clients or services. Cultivating **effective communication to and within an organization is central to the effective management of security risk** and responding to an incident.

Board engagement translates into real-world benefit. A 2018 Data Breach study[1] reported that the average cost of a data breach per record lost was USD 148 but that this was reduced by USD 6.5 in companies with Board-level involvement, or the appointment of a CISO. Savings of USD 9.3 were seen when companies implemented employee training, and USD 14 when companies had dedicated Incident Response Teams. When you scale this up to the hundreds of thousands or even millions of records lost in a serious data breach, the financial saving becomes extremely significant. Importantly, appropriate and meaningful Board-level engagement really drives these other factors because directors have the ability to assimilate policies such as employment training into the framework of company strategy.

Time is always money and in today's world information travels fast. Customers will be providing the world with **real-time updates on company service failure or data breaches via social media** and news outlets. The critical factor in minimizing response time is streamlined, effective coordination: this has to come directly from the top.

Businesses need leadership which generates an organizational attitude of concern, preparedness, and critical self-evaluation. By being more proactive about cybersecurity issues, directors can play an essential role in safeguarding their organization's stability and future growth.



[1] 2018 Cost of a Data Breach Study, Ponemon Institute, Sponsored by IBM: https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf

WHAT ARE THE ROADBLOCKS TO BOARD ENGAGEMENT?

The key roadblock to Board engagement can be summarized by the mutually exclusive relationship between the Board and their technical teams.

Board members are business leaders not technical experts: they lack technical experience and often have little interest in learning. Technical staff are not leaders and have little management experience: they work in isolation and lack motivation to educate others. Thus, **there is often reluctance for these two parties to engage with each other** because either technical staff think that the Board will not understand them, or the Board thinks that the technical staff are unable to explain the issues within the context of the strategic aims of the organization.

This relationship combination conspires to build an environment where there is no communication and no overall strategy for dealing with cyber risk. **This must change, and directors must spearhead this change** because they are the experts in managing people, managing risk, communicating, and driving policy changes.

Why is it that confidence in cyber insurance policies was lowest among Board members and IT teams, but highest among finance teams, risk managers, and legal teams?[2] Yet IT and Board Members are the main drivers of cyber risk management. How can this discord exist? This highlights the **clear rift between business factions, and the lack of coherence in risk management**.

THE ROLE OF THE BOARD IN COMPANY CYBER SECURITY

The role of the Board in cybersecurity risk management and response is simple: **oversight**. Directors are there to provide direction by **policy change**, create the right company culture through **education strategy**, and **hold executives to account**. Some of the key roles of the Board are summarized in figure 1. Essentially, the role of the Board is to lead, which is what it is good at.

Effective cyber security is **not just about technology**, **it's about people and processes too**. Risk in all three of these areas must be managed, and the latter two are where the Board becomes really critical.

It is also important for Boards to realize that once an effective cybersecurity program is established, their work is not done. **The Board must continually review this program; it must be assessed and updated regularly**. Both Board and management should also routinely practice the cybersecurity response plan to ensure that complacency does not set in, and that all staff are aware of the individual role they must play in the case of an incident.

In being more proactive about cybersecurity issues, **directors can play an essential role in safeguarding their organization's stability and supporting future growth**.

FIGURE 1 | The role of the Board in cybersecurity risk management

[2] 2019 Global Cyber Risk Perception Survey, Marsh & McLennon Companies, Sponsored by Microsoft: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

The Legal Perspective

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

The Privacy Amendment (Notifiable Data Breaches) Bill 2016, makes it mandatory for companies and organisations to report "eligible data breaches" to the Office of the Australian Information Commissioner (OAIC) and any affected or at-risk individuals.

In the United States, the risk of shareholder lawsuits following a cyber incident where the company share price drops has been highlighted. Directors should be aware that they may be **liable to accusations of inadequate disclosure** and a **failure to perform their duty** to confirm the company continues to adequately protect consumer data.

These legal obligations and risks are most holistically understood by the Board of Directors; they are realized in a personal liability context, a context of future business success, and within the wider field that the business operates in.

IMPROVING CYBER RISK MANAGEMENT

Time

Directors must make the time to discuss and agree their approach to cyber security, and **cyber debriefings should be a regular item on the agenda of Board meetings**. There must be regular communication between the cybersecurity experts – whether in-house, third-party, or both – and all the members of the Board.

Debriefings should include **reports from management directly involved in managing and responding to cyber risk** and must provide information on the ongoing and current security status, key metrics on critical controls, as well as details of incidents if they have occurred. Importantly, these communications **should be clearly designed and accessible to all members of the Board**, regardless of background or expertise.

It is important that Boards set **specific, measurable, and time-bound targets**. Part of the role of holding executives to account is in setting up categorical timelines to deal with threats. Any critical findings discovered by technical staff or a third-party consultant running a Penetration test for example, should be labeled based on the risk it presents to the company and **a timeline for resolution established – usually 30, 60, or 90 days**. Resolution time will depend on the severity of the risk, the complexity of the solution, and the roll-out time; analysing this and making the decision clear is an essential part of the risk management.

With cyber security regularly discussed, Boards will be able to make informed decisions on cybersecurity policy, and thus invest resources in a time- and cost-effective fashion.

Communication

Improving the communication between directors and technical staff requires effort from both sides.

Boards need a reasonable understanding of cyber security so that they can understand how it supports their overall organizational objectives and the **technical staff need to appreciate that communication of cyber risk is a core component of their job**. They also need to understand how their role fits into the organization's overall goals and objectives and how they contribute to these.

It is important to have **open and direct dialogue** between the Board, any third-party experts, and management to evaluate the risk management programme and develop an effective strategy for cyber threat mitigation that is implemented company wide.

Education

If Boards are educated on the risk, they will ask the right questions to determine whether appropriate processes are in place. **This will drive company engagement at all levels, as well as hold management accountable** for evaluating current cybersecurity risks and maintaining response plans.

Any question is worth asking, but some which may be pertinent to assessing a company's current cyber security status are provided below.

1. Have we been told about cyber attacks that have occurred in the past and their severity?
2. What are the organization's internal and external cybersecurity risks and how are we managing them?
3. What is **management's** response plan regarding cyber attacks?
   - What disclosure obligations exist for our organization?
   - Are these plans and obligations regularly tested and checked for effectiveness?
4. Have we conducted a **penetration test, external assessment, or cyber security audit**?
   - What were the results and what have we changed or improved since then?
   - What are our priorities for improvement?
5. Do we have a **systemic framework** in place (US National Institute of Standards and Technology or equivalent) to address and ensure adequate cyber security?
6. Do we have access to cyber expertise?

7 Is management **reporting regularly**?

8 Is the information provided by reports sufficiently engaging and of high enough quality to provoke robust discussions about cyber security?

9 Is management aware of the threats and identified potential attackers, as well as their methods and motivations?

It isn't just about Board education, however. The new cyber ethos acquired by the Board should then be propagated down the management chain eventually to every member of the company.

Most cybersecurity attacks and data losses are the result of a mistake made by an individual, not a complex infiltration and take-down of defence systems. This was made extremely apparent in the compromise of personal data at the Australian National University (ANU), in which **the breach was initiated via a spear phishing email** targeted at a single staff member (see Box 2: The ANU Data Breach)[3], which was then further distributed to more staff members afterwards. Better education leading to more diligence and awareness may have prevented the spread of this system entry mechanism.

In this case, it is truer than ever that technology cannot be relied upon: the people and processes of the company matter just as much.

Directors should aim to empower their staff, so that they feel able to raise concerns regarding cyber security. This means not only that there should be a well-established mechanism to do so, but that staff should feel comfortable in doing this, whether it be raising general concerns or reporting a specific incident. **Not only will this approach engage employees in a positive cybersecurity culture, but also will provide a valuable source of information** for directors to detect vulnerabilities and assess the progress of their cybersecurity strategy.

BOX 2 | THE ANU DATA BREACH, 2018

Timeline: November 2018 – March 2019 (6-week primary attack period)

Outcome: Significant **negative media coverage**. Firewall change and attacker blocked, but an ***unknown amount* of *unidentified* personal data stolen**

Cost: Unknown. **Millions spent on university system upgrade; cost of stolen data** for the university and Australian government is unmeasurable

The ANU data breach was a sophisticated operation which erased almost every trace of itself; even the data stolen was unknown. It was **initiated by a single spear phishing email** which only required previewing to allow access to user credentials. These were then used to further distribute emails to other, more privileged users. These **emails contained files which were then opened by the users** and allowed the hacker to infiltrate the network.

Identified issues included a legacy **email server which did not require authentication**, mail servers associated with the ANU network being allowed to accept and relay traffic, and the **use of unencrypted connection protocols**.

Where this stolen data might end up is unknown and will depend on whether the attack was orchestrated by a nation state or organized criminals.

[3] The full incident report released by the Australian National University can be found at: http://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf

REASONABLE STEPS IN MANAGING CYBER RISK

Taking reasonable steps to achieve security targets that are relevant to an organization are a good, **realistic approach to building a revived, positive security strategy**. Reasonable steps to ensure the security of personal information will depend on the circumstances but will include the following:

- The nature of the company or entity holding the personal information
- The amount and sensitivity of the personal information held
- The possible adverse consequences for an individual
- The information-handling practices of the entity holding the information
- The practicability of implementing the security measure, including time and cost
- Whether a security measure is itself privacy invasive

So, what are reasonable steps?

Here we focus on policy, and on the management of risk from a holistic and leadership perspective. These reasonable steps have been highlighted by The Office of the Australian Information Commissioner (OAIC). Technical steps are also mentioned by the OAIC, and some of these have been placed in Appendix 1 of this document for reference.

Perform Privacy Impact Assessments (PIAs)

A privacy impact assessment (PIA) is a tool used by companies to help them identify and **assess the privacy risks** arising from their collection, use or handling of personal information.

Implement a Privacy by Design Principle

Privacy by design calls for **privacy to be taken into account throughout** the whole engineering process.

Perform an Information Security Risk Assessment

Risk assessments **identify, estimate and prioritize risks** to organizational operations and assets resulting from the operation and use of information systems.

Create and Maintain a Privacy Policy

A privacy policy is a statement or a legal document that **discloses the ways a party gathers, uses, discloses, and manages a customer or client's data**. It fulfils a legal requirement to protect a customer or client's privacy.

Have a Comprehensive and Up-to-date Set of Information Security Policies

An information security policy is a set of policies for your organization to ensure that within the company network all **information technology users comply with rules and guidelines** related to the security of all digitally stored information.

Restrict Access to Personal Information on a "Need-to-know" Basis

Individuals should be given **access only to the information that they absolutely require** in order to perform their job or carry out their duties.

Keep All Software Up-to-Date and Current

Make sure all software is up-to-date and patches are done regularly and diligently. Keep in mind legacy-based systems and ensure that they are compatible with and meet the requirements of any new security implementations.

Perform a Vulnerability Assessment

A vulnerability assessment is an automated, comprehensive scan of an entire network which identifies, quantifies, and prioritizes the vulnerabilities in a system. **This will help determine what needs to be tested in a penetration test**.

Perform Penetration Testing Exercises

A penetration test (pentest) is an **authorized, simulated, cyber attack on a computer system performed to evaluate the security of the system**. This is a time-intensive, human-led test carried out by highly trained cyber security personnel. It is vital that this process be carried out by an independent third party so problems can't be covered up or ignored. This is **not to be confused with vulnerability testing**; they do not perform the same function but work in complement.

A good pentest will provide a comprehensive report with detailed vulnerability findings. Nearly all reports will have some critical findings, as it is not practical for companies to be entirely critical free. Nevertheless, such findings need to be identified, documented and discussed in order to inform improvements on security strategy and systems.

For more information on the differences between vulnerability assessments and penetration tests, and what makes a thorough and comprehensive Cyber Security Audit, see our article *Bug Hunting: A Penetration Test Finds Security Flaws Before the Bad Guys Do*[4].

Ready a Data Breach Response Process

The plan must list the contact details for all designated staff in the event of a data breach. It must **clearly state all roles and responsibilities and all the processes and procedures** that must be followed. Plans should **aim to be holistic**, covering everything from attack mitigation to client communication. Non-technical responses should not be sidelined: during the ANU attack, a burst in negative media coverage resulted in a surge in attack attempts. A plan including press releases and containing a media response would thus have been very useful.

[4] Sharrock, J. Bug Hunting: A Penetration Test Finds Security Flaws Before the Bad Guys Do. Cyber Citadel (2018): https://www.cybercitadel.com/penetration-test-finds-security-flaws-before-the-bad-guys-do/

SUMMARY

- Boards of Directors have a responsibility to take a lead on implementing improved cybersecurity frameworks to keep their company and client data safe
- Boards can achieve this by dedicating more time to a regular review of the security status of their organization, and by considering cyber risk management in the same tone as any other business risk
- A cyber risk team will lead the development of a cyber risk management plan that includes all necessary departments; this should be conveyed to the Board for scrutiny, and to allow the Board to hold management accountable
- Any plan should be regularly reviewed, including a quantification of the impact of cyber risk management efforts, producing metrics to explain the outputs and report these to the Board
- Internal audits should be conducted on the effectiveness of cyber risk management on a quarterly basis; continual assessment and critical evaluation of the company's performance in dealing with cyber risk is central to ongoing success
- Using independent third-party security services to achieve regulatory compliance not only gives companies greater protection through reduced bias and complacency, but can save money due to security services' already well-established expertise

DIRECTORS' TO-DO LIST

APPENDIX 1
Further technical steps

The emphasis in this report is on generating good business culture surrounding cyber security. Although **there are technical steps a business can take to improve their security**, and some of these are listed below, it should be restated that the role of the Board is in driving policy change; **it is the role of *technical* staff to implement *technical* advances which meet the demands of new, more rigorous policy**.

Employ Multi-factor Authentication (MFA)

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

Employ Endpoint Security Software

Endpoint Security refers to the approach of **protecting a business network when accessed by remote devices** like smartphones, laptops, or other wireless devices. This is becoming increasingly important in an exponentially more connected world, where remote devices are often the communication mode of choice.

Employ Security Monitoring Tools to Detect Breaches

Implement host intrusion detection tools. Not only is this useful in its own right but companies in Australia are regulated and required to report breaches, and thus it also fulfils a legal obligation.

Companies can use SIEM (Security Information and Event Management) – **a log management software** – to protect their most sensitive data and to **establish proof** that they are doing so, which allows them to meet compliance requirements. A single SIEM server receives log data from many sources and can generate one report that addresses all of the relevant logged security events among these sources.

APPENDIX 2
Glossary of terms

Cyber security audit	A complete assessment of the internal and external risks of a company, which will involve procedures such as pentests and vulnerability assessments (collectively called VAPT: Vulnerability Assessment and Penetration Testing)
External cyber risk	Any threat to an organization's security originating from outside of the network; items such as perimeter devices, servers, applications, and encryption are important players in reducing external risk
Internal cyber risk	Any threat to an organization's security originating from inside the network, for example by an attacker gaining user credentials through a phishing email which are then used to access the network
Log management	The process for generating, transmitting, storing, analyzing, and disposing of computer security log data; proper management is about deciding what you need to log, the best way to store this information, and how long it needs to be kept
Penetration test (pentest)	A human-led investigation involving an authorized, simulated, cyber attack on a computer system, performed to evaluate the security of the system and provide both technical and business solutions
Systemic framework	A voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The guidance is specific to an organization's requirements and objectives, risk, and resources[5]
Vulnerability assessment	An automated comprehensive scan of a cyber network which detects technical vulnerabilities and can be used to inform a penetration test to increase its effectiveness

[5] A complete and detailed description of the Systemic Framework concept can be found via NIST at: https://www.nist.gov/cyberframework/framework