Cyber attacks: Get your governance in order

By Alexandra Wedutenko, Managing Partner, Clayton Utz

- A report by the Australian Cyber Security Centre estimates the cost of cybercrime to Australia at $1.06 billion over a 12-month period.
- The use of cloud services means that substantial repositories of data are held in the cloud, and are therefore at risk of intrusion by cyber attackers.
- The audit or risk committee can play a key role in driving good corporate governance with respect to cyber security.

Having the latest technology is only one part of cyber security you need to train your people and have good governance around IT systems and related processes too.

The great disruption brought by the online revolution is not just disrupting business models it's created a new wave of business risks, not least cyber attacks.

The board and senior managers of your organisation are responsible for considering and addressing the risks of cyber attack. This responsibility is somewhat enshrined in legislation for many organisations, namely through directors duties in the *Corporations Act 2001*. While awareness and action at the senior level are vital, holistic strategies that shape and support the governance framework of an organisation are also necessary to effectively combat cyber risks.

In this article, we sketch out the nature of the risks (particularly from the growth in cloud computing), and the ways senior managers can address them, starting with the simple activities such as educating staff to help manage cyber risks, through to corporate governance and systems accreditation.

How big is the problem of cyber threats in Australia?

Australia's relative wealth, high levels of online traffic and use of technology make it an attractive target for cyber adversaries.

In July this year, the Australian Cyber Security Centre (ACSC) released its first ever unclassified cyber security threat report. The report, while perhaps not adding new concepts, demonstrates that 'the cyber threat to Australian organisations is undeniable, unrelenting and continues to grow.'

Cybercrime 'criminal acts involving the use of computers or other ICT, or targeted against computers or other ICT' is a much more prevalent issue, with an estimated cost to Australia of $1.06 billion over a 12-month period (an estimate the report acknowledges might be too low).

What are cyber attackers trying to do?

Cyber attacks can come from nation-states criminals seeking to make money, business rivals seeking an advantage, or hacktivists (or even bored teenagers) seeking to make a point. Their goals may include:

- disruption
- to get information which they can reuse (such as customers' credit card numbers or identity theft, or industrial espionage)
- to affect your ability to perform your business or functions by seizing control of your systems or stopping them from operating effectively; or
- to hijack your systems to use them for their own purposes (such as sending out millions of spam or scam emails).

A very common threat to organisations is the surreptitious addition of

malicious software ('malware'), which can suck up information and send it to the attacker. A variant is ransomware, which 'typically locks a computer's content and requires victims to pay a ransom or regain access.' It can also involve a message alleging that the computer has been used for some illegal activity and demanding payment of a fine. This can cause related difficulties if the victim has not performed a recent backup.

Cyber attacks

Cyber attacks will target your weakest links, which will often be human error. Critically, your people's failure to protect access to systems through poor passwords, password protection or betrayal will be the easiest way for cyber attackers to gain access to your systems.

The use of social engineering techniques, such as emails to entice a user to click on a link or open an attachment (known as spear phishing) are also popular. This tricks the unwary into introducing software which can wreak havoc. Organisations with poor cyber security are especially vulnerable to spear phishing.

Even if your own staff are well trained, avoid spear phishing attempts and have secure passwords, cyber attackers can exploit technical backdoors left open by you or third parties.

For example, the growth of 'bring your own device' practices and the blurring of the work/life distinction have meant more business is done on smart devices, which are relatively insecure and provide access to the firm's IT systems.

Another technique is the use of a watering-hole. This is a legitimate website, frequented by a cyber attacker's intended targets, which has been compromised by, for example, malicious software which has been covertly added to the site with the purpose of compromising viewers' computers. In 2014, the ACSC identified incidents involving watering-hole exploitation of websites frequently visited by Australian government employees. The ACSC notes that this technique is no longer opportunistic, but has become an activity targeting Australian government and business.

Finally, there are the risks unique to cloud computing.

Risks associated with cloud computing

Many organisations around the world, including in Australia, are using cloud services and this trend is likely to increase. You and the people around you also interact with cloud services, probably on a daily basis if you use online banking, social networks or email accounts such as Gmail or Hotmail, you are using cloud services.

Cloud computing has been defined as 'a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'. Bypassing the technical language, cloud computing is essentially the delivery of computing services over the internet.

The widespread and constant use of cloud services means that substantial repositories of data are held in the cloud, and are therefore at risk of intrusion by cyber attackers.

Assessing the risks of cloud computing generally

The responsibility to mitigate risks associated with cloud computing is shared between the organisation (referred to as the 'tenant organisation') and the Cloud Service Provider. However, ultimate responsibility for protecting data and ensuring its integrity, confidentiality and availability lies with the tenant organisation and its senior management.

Before using cloud services, tenant organisations should perform a risk assessment and implement relevant mitigation strategies to manage any financial, jurisdictional, legal, governance, data ownership, data sovereignty, privacy, technical and security risks.

…the growth of 'bring your own device' practices and the blurring of the work/life distinction have meant more business is done on smart devices, which are relatively insecure and provide access to the firm's IT systems.

Risks will vary between tenant organisations, depending on various factors such as:

- the intended use of the cloud service
- how the cloud service will be implemented and managed
- the sensitivity of the data to be stored or processed
- the location of the cloud (in Australia or overseas)
- difficulties the tenant organisation will face in detecting and responding to incidents with its data.

Tenant organisations will also need to compare the risks associated with using a cloud service against those associated with using in-house or otherwise dedicated computer systems, such as inadequate security or capability.

Some points to consider include:

- whether your data will reside onshore or offshore (and if so where) and therefore be subject to lawful access by a foreign government and/or laws
- your information will be stored in various separate locations, and multiple people will have access to it, increasing opportunities for it and your networks to be compromised

> Building cyber management into the broader risk management umbrella as a discrete yet important part will help to establish cyber management as an engrained part of the governance of your organisation.

- cloud computing means multiple customers are hosted on the same infrastructure, also increasing the risks of unauthorised access or network compromise
- while you can include legal protections in your contract with your Cloud Service Provider, you cannot directly control all of the security measures — some will become the responsibility of the Cloud Service Provider, even if they were previously visible to and controlled by you.

Assessing the risks of cloud computing for government agencies: ASD certification

Every Australian government agency contracting cloud computing services needs a security assessment and certification to achieve accreditation of an outsourced service. To streamline the process and avoid agencies working in isolation, the Australian Signals Directorate (ASD) is conducting certification activities.

Some cloud computing services have been awarded ASD certification and Australian government agencies contracting these services are advised to request the ASD Certification Letter and Report from the Cloud Service Provider. ASD Certification will help agencies to understand the information security risks when contracting cloud computing services but agencies should also perform their own due diligence reviews.

Other organisations might choose to mirror these practices.

What are some key risks of cloud computing and what can you do to mitigate them?

Failure to maintain and protect the confidentiality, integrity and availability of its data

To mitigate this risk, even if you are a private sector organisation you could use a cloud service:

- that has been assessed and endorsed by the ASD Information Registered Assessors Program, and/or
- that has been certified and accredited against the ASD Information Security Manual at the appropriate classification level.

You would also include contractual protections in your contract with the Cloud Service Provider.

Data compromised in transit by a malicious third party

You could use cryptographic controls that have been approved by ASD to protect data moving between your tenant organisation and the Cloud Service Provider and data at rest on storage media in transit via post/courier, for example when transferring data as part of on-boarding or off-boarding employees.

Cloud service account credentials compromised by a malicious third party

To mitigate this risk, you could use a secured computer, multi-factor authentication security access control, a robust passphrase, limit access to the minimal level possible, and encrypt network traffic.

You could also obtain and analyse time-synchronised logs and real-time alerts for your tenant organisation's cloud service accounts which are used to access and administer the cloud service.

It is also important to protect authentication credentials so avoid using Application Programming Interface authentication keys on unsecured computers or in source code software that is accessible by unauthorised third parties.

Future trends in cyber attacks

Although the ability to detect cyber threats continues to improve and the development of robust cyber defences is progressing, cyber adversaries are constantly improving their tradecraft to tackle network defences.

The ACSC report has predicted that both spear phishing and ransomware will continue to be popular, and there will be an increase in:

- cyber criminals
- cybercrime-as-a-service
- the use of watering-hole techniques
- the number of cyber adversaries with destructive capability
- electronic graffiti (for example, web defacements and social media hijacking).

How can you defend your organisation against cyber threats?

Training and good governance

Any action has to start with your people. This means, as a bare minimum, training them to understand the risks of spear phishing and poor password security.

This must be backed up by good corporate governance across your organisation. Many people will have a crucial role to play in managing information security: the legal team, IT infrastructure and procurement team, the CEO and COO and whoever else is responsible for risk management, those with information security oversight and management (such as information security managers and the CIO), those with system/security design, development and implementation responsibilities and those who test, monitor and audit information systems. You should also consider getting external advice, both on technical and legal issues.

Of course, getting everyone educated and aligned is only the first step. Responsibility should be assigned, and processes mapped and maintained. For example, you should look at using cyber drills or authorised attacks by third parties to test your systems periodically, create and update cyber risk protection documentation, maintain asset registers, know what hardware is accessing your systems, and ensure all relevant systems are accredited.

Leadership from the top

The senior leadership team should play an active role in order to implement an effective framework to combat cyber attacks. Not only will this help to protect your organisation, but it is within the scope of responsibility of directors and senior officers. Directors owe various duties, including the duty to exercise powers and discharge duties with reasonable care and diligence, in good faith in the best interests of the company and for a proper purpose. These duties encompass a range of matters, including in the area of risk management.

Considering the growing threat of malicious cyber activities pose, there should be a focus on cyber as part of risk management. As cyber adversaries develop more sophisticated strategies of attack, organisations will need to develop more sophisticated strategies of protection. Building cyber management into the broader risk management umbrella as a discrete yet important part will help to establish cyber management as an engrained part of the governance of your organisation.

This will not only be beneficial from a cyber point of view, but will also be important from a financial perspective as cyber attacks can cause significant financial loss. Organisations suffer direct financial loss through the clean-up process after a cyber attack and the associated bolstering of cyber protections, but also indirect financial loss through reputational damage.

Audit or risk committee as a microcosm of good governance

The audit or risk committee can play a key role in driving good corporate governance with respect to cyber security. This can shine through in the responsibility of the audit or risk committee to assist the board in fulfilling corporate governance and oversight activities including in relation to risk management (and even financial management) systems.

Bringing cyber security within the ambit of the audit or risk committee and equipping that committee with appropriate knowledge and resources can help to address cyber security at a high level which would then in theory flow through the organisation.

Structured response to incidents

A structured response to incidents is also a useful tool. This can be achieved by developing, implementing and then testing (annually) an incident response plan. This would ideally encompass responses to data spills, e-discovery of data and ways to obtain and analyse evidence (for example, time-synchronised logs, hard disk images, memory snapshots and metadata).

Technical aspects and proactive approach

Finally, there is a lot of very useful guidance on the technical aspects of information security and protection from cyber attacks coming from the public sector. The US Government's National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cyber Security, released in February 2014, sets out a risk-based approach which is evolving to meet new threats. Closer to home, there's the Australian Signals Directorate's four strategies:

1. Application whitelisting.
2. Patching applications (such as PDF readers, Microsoft Office, Java, Flash Player and web browsers).
3. Patching operating system vulnerabilities and using the latest versions.
4. Minimising administrative privileges.

As the ACSC report notes, organisations must be proactive, invest resources in cyber security and implement measures to make them a harder target. This needs to be supported by Australia's ICT community, academia and decision-makers in the public and private sector, by keeping up to date with developments, identifying new vulnerabilities and advising Australian organisations on strategies to mitigate emerging threats. This will be critical to provide a high degree of confidence in network and information security and to enable your organisation to enjoy the benefits of the internet. ◪

Alexandra Wedutenko can be contacted on (02) 6279 4008 or by email on awedutenko@claytonutz.com.