In response to heightened public interest and concern, this briefing highlights some of the key technical, commercial and legal issues that businesses currently need to understand about cyber security. This rapidly evolving field is increasingly attracting public and regulatory attention, resulting in the Government signalling its intent to replace New Zealand’s current privacy laws.

Historically there has been an attitude in New Zealand amongst SMEs and some large corporates, that they aren’t vulnerable because they are either too small for cyber criminals to worry about or, that because they outsource their cyber security, they aren’t at risk. In reality, any business that has access to the internet is at risk.

- It is data rather than size that makes a business attractive to cyber criminals, especially if it is attractive data such as employee or customer information, credit card data or valuable intellectual property.
- SMEs are more attractive targets because they tend to be less secure and because automated attacks can be instigated for little effort or cost. Statistics show that 60% of all cyber-attacks are aimed at SMEs.
Understanding the risks faced by the business

What assets do you need to protect?
Every business should identify the key assets that need to be protected from a potential cyber attack. For example:

- Customer databases.
- Financial information.
- Sensitive personal data.
- Intellectual property (such as product designs or manufacturing processes).
- IT equipment.
- IT services (such as the ability to take payments via the company website).

What impact could a cyber attack have on your business?

- Financial losses stemming from:
  - Theft of information, bank details or money.
  - Disruption to trading (especially if the business undertakes a lot of online transactions or is reliant on networked systems to operate).
  - Costs associated with cleaning up affected systems and getting them functioning again.

- **Reputational damage** - A business that has been the victim of a cyber attack will be keen to convince its customers, owners, employees and the general public that the incident was a one-off event and the situation is now under control. Reputational damage can often lead to a reduction in profits and the erosion of a business’s customer base.

- **Contractual liability** – The business could be liable under its contracts with customers and suppliers where disruption causes defaults in delivery of goods or services or where their data has been compromised. Internationally companies are beginning to request the other party to disclose all details of cyber attacks that compromise that business and to have ability to cancel contracts where security is compromised.

- **Regulatory sanctions** - The business could be fined if personal data is lost or compromised due to a cyber attack. Current data protection/privacy laws require businesses to implement appropriate technological and organisational security measures against unauthorised or unlawful processing, accidental loss and destruction or damage of personal data. Damages of up to $168,000.00 have been awarded for breaches of privacy in New Zealand.

What is a cyber attack?
A cyber attack is an assault against a computer or computer system, which is intended to compromise its integrity, availability or confidentiality. For example:

- A remote attack on a business’s IT systems or website e.g. the Ashley Madison hack, Target and Sony hacks and the Apple “selfie” hack.
- Malware and ransomware - this is a type of malicious software, or malware, that locks a computer and demands payment to unlock the computer or system and has been particularly prevalent in New Zealand recently with a number of professional services and other businesses compromised.
- Attacks on information held in third-party systems (for example, the company bank account).
- Denial of Service (DoS or DDoS) – this is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

Disclaimer: the content of this update is not intended as a substitute for specific professional advice on any matter and should not be relied upon for that purpose.
Under the Privacy Act there is currently no requirement for organisations to notify affected individuals when their information has been made available to unauthorised persons. The Law Commission is currently reviewing the Privacy Act, which may result in the introduction of obligations for businesses to self-report data breaches.

Planning for a potential cyber attack

How can you prepare your business?

As with natural disasters, your chance of responding effectively following a cyber attack is greatly improved by having good systems in place to prevent and attack and by planning and practicing for your response when an attack happens.

You should be alert to the possibility that your suppliers, major customers and competitors can also fall victim to cyber attack. Aim to stay informed in these situations, as the information can help you avoid similar attacks.

Business continuity planning

As part of your risk management planning, you should undertake the following:

- Produce an incident management plan detailing what actions should be taken following a cyber attack and who to contact for support if the business is attacked or its online services are disrupted. The plan should set out the business’s recovery procedures and explain how it would continue operating, particularly if the business trades online.
- Ensure that all important business records (for example, sales information) are backed up regularly and archived in a secure, off-site location that can be easily accessed after a cyber attack.
- Compile hard copies of staff, supplier and customer contact lists. The business should ensure that copies are retained off site and kept secure, for use in the event of an attack.

Businesses can take a number of steps to improve their security controls

<table>
<thead>
<tr>
<th>Network security</th>
<th>Increase protection of the business’s networks (including wireless networks) against external attacks through the use of firewalls, proxies and other measures.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware protection</td>
<td>Install anti-virus solutions on all systems and keep software and browsers up to date. Consider restricting access to inappropriate websites to reduce the risk of being exposed to malware.</td>
</tr>
<tr>
<td>Secure configuration</td>
<td>Maintain an inventory of all IT equipment and software. Identify a secure standard configuration for all existing and future equipment used by the business.</td>
</tr>
<tr>
<td>User privileges</td>
<td>Restrict employee and third-party access to IT equipment, systems and information to the minimum required. Excessive user privileges, with too many employees having access to confidential information or systems that do not help them perform their job, should be avoided.</td>
</tr>
<tr>
<td>Remote access</td>
<td>Access from external and mobile devices increase a business’s cyber risk profile. Implement a home and mobile working policy and train employees to adhere to it, especially if the business allows employees to use personal mobile devices (for example, laptops or tablets) for business use.</td>
</tr>
<tr>
<td>Removable media</td>
<td>Restrict the use of removable devices such as USB drives. Make sure any data stored on removable media is protected to avoid the data being lost and to help prevent malware from being installed on the business’s IT networks.</td>
</tr>
</tbody>
</table>
Security controls
Consider instructing a third-party IT security consultant to carry out an audit to determine whether the business’s existing security processes provide sufficiently robust protection. A specialist consultant will have experience of how other similar businesses are responding and can provide you with a detailed plan of how to respond to an attack.

Review your contractual commitments
Under New Zealand law, contractual obligations cannot easily be avoided. Businesses should conduct a legal health check to analyse the business’s existing contractual commitments and requirements. Businesses should seek advice on:

- Liability for failure to deliver goods or services on time as a result of a cyber attack. Are there appropriate limitation clauses in the business’ contracts?
- What disruption means for them legally. Most contracts do not include cyber attacks, and the resulting disruption, as a force majeure event, which means that the business will likely be liable for failure to perform the contract as a result of such an attack. Businesses should consider whether adding cyber attacks as a force majeure event in their contracts is appropriate.
- The implications of customer and supplier personal and financial information and intellectual property being accessed by cyber criminals.
- What legal recourse they will have against their third party cyber security provider. Most such contracts limit liability to a proportion or multiple of the fees paid by the business and this can often be insignificant compared to the loss suffered by the business as a result of an attack.

Review your cyber insurance cover
You should ensure that you have adequate cyber insurance in place, suited to the nature and scale of your business. Standard business insurance does not provide adequate cover where cyber attacks and cyber breaches affect electronic data but do not cause physical damage.

Cyber and data coverage gaps in current policies could include the following:

- Professional liability policies are tied to professional services and also may have a requirement that there be an act of negligence. This might also be restricted to claims from customers only, so claims related to the disclosure of employees’ data won’t be covered.
- Commercial general liability may be limited to bodily injury and property damage. These policies often also have exclusions relating to the unauthorised disclosure of personal information.
- Business interruption insurance won’t cover cyber-attacks that don’t cause physical damage.
- Crime policies require intentional acts to trigger them and only will cover money, securities and tangible property.
- Kidnap and ransom policies will not cover cyber risk unless a specific ‘cyber-extortion’ amendment is made.

Your lawyer and insurance broker can help you better understand how to manage your liability around cyber attacks.

Educating employees

- The business should produce a policy detailing how employees should use its systems in the most secure manner.
- Employees should be given appropriate internal training (both for new joiners and regular refresher for existing employees) so that everyone understands their role in keeping the business secure.
- Businesses should put reporting processes in place to enable employees to raise concerns about other members of staff that they think are failing to comply with the policy.
On-going security management issues

- Ensure that all IT systems and networks are continuously monitored against attack, either through appropriately qualified third party providers or internally.
- Test, monitor and improve security controls on a regular basis.
- Remove any software or equipment that is no longer used, ensuring that any sensitive information stored on it is deleted before it is disposed of.
- Review and manage any change in user access, such as the creation of e-mail accounts when new employees arrive and the deletion of accounts when they leave.

Responding to a cyber attack

What actions should I take?

When a cyber attack occurs often the initial reaction is one of panic. Ideally you will have a business continuity and response plan in place, which include the following actions:

- Work with your in-house or contracted IT professionals to protect evidence of the attack, identify and remove any on-going threats (for example, malware), and address gaps in the business’s security that have been identified due to the incident.
- Report the incident to the police and to NetSafe/The Orb - NetSafe, which is a multi-stakeholder partnership made up of organisations such as government, law and industry, provides a reporting facility at www.theorb.org.nz.
- Notify your insurer.
- Contact your legal advisor to discuss the implications of the attack from a contractual and liability perspective.
- Consider taking professional public relations advice, particularly where customers’ or suppliers’ data has been lost or compromised.

Contact us

Technology and commercial advice

Mark Cathro  
Partner, Christchurch  
d +64 3 372 6446  
m +64 21 226 3541  
mark.cathro@duncancotterill.com

Chris Linton  
Partner, Auckland  
d +64 9 374 7157  
m +64 21 885 559  
chris.linton@duncancotterill.com

Dan Winfield  
Partner, Wellington  
d +64 3 372 6446  
m +64 21 226 5179  
dan.winfield@duncancotterill.com

Scott Moran  
Partner, Wellington  
d +64 4 471 9438  
m +64 21 905 511  
scott.moran@duncancotterill.com
Cyber insurance and litigation

Duncan McGill
Partner, Auckland

d +64 9 374 7151
m +64 21 226 3530
duncan.mcgill@duncancotterill.com

Jonathan Scragg
Partner, Wellington

d +64 4 471 9422
m +64 21 878 972
jonathan.scragg@duncancotterill.com

Disclaimer: the content of this update is not intended as a substitute for specific professional advice on any matter and should not be relied upon for that purpose.