CYBER SECURITY

Cyber security is fast becoming one of the most significant concerns facing businesses, government and individuals. This is not surprising: cyber attacks are increasing in scale and sophistication just as many businesses are moving data and systems to cloud services providers and other online solutions. Concern is also fuelled by well-resourced and high profile businesses publicly falling prey to cyber attacks. As a result, in addition to commercial concerns, businesses and boards of directors are increasingly questioning: what are our legal obligations and tools relevant to cyber security?

The key cyber security legal obligations and tools for New Zealand businesses can be grouped into two broad categories:

1. PREVENTION AND MITIGATION

Relevant issues include:

- **Satisfying directors' duties and corporate governance obligations**
- **Implementing effective cyber policies and procedures**
- **Including safeguards in employment contracts and policies**
- **Considering cyber risks in mergers and acquisitions' due diligence and agreements**
- **Protecting IP assets**
- **Privacy Act obligations and policy compliance**
- **Ensuring contractual protections in supplier and customer contracts**
- **Cyber insurance**

Directors must adequately manage cyber risk in the "best interests of the company" by exercising "the care, diligence and skill that a reasonable director would exercise". Assessing whether directors have met that standard will depend on the potential harm to the company as a result of a cyber breach. For example, a higher level of skill and care would be expected from the board of a bank than from the board of a building company. Boards must ensure they have adequate expertise and oversight to discharge these duties.

"...there are only two types of companies: those that have been hacked and those that will be."

Robert S. Mueller III, Director, Federal Bureau of Investigation

Have you considered cyber threats in the context of your confidentiality, privacy, force majeure and security undertakings to your customers? Are the security commitments from your suppliers sufficiently robust?

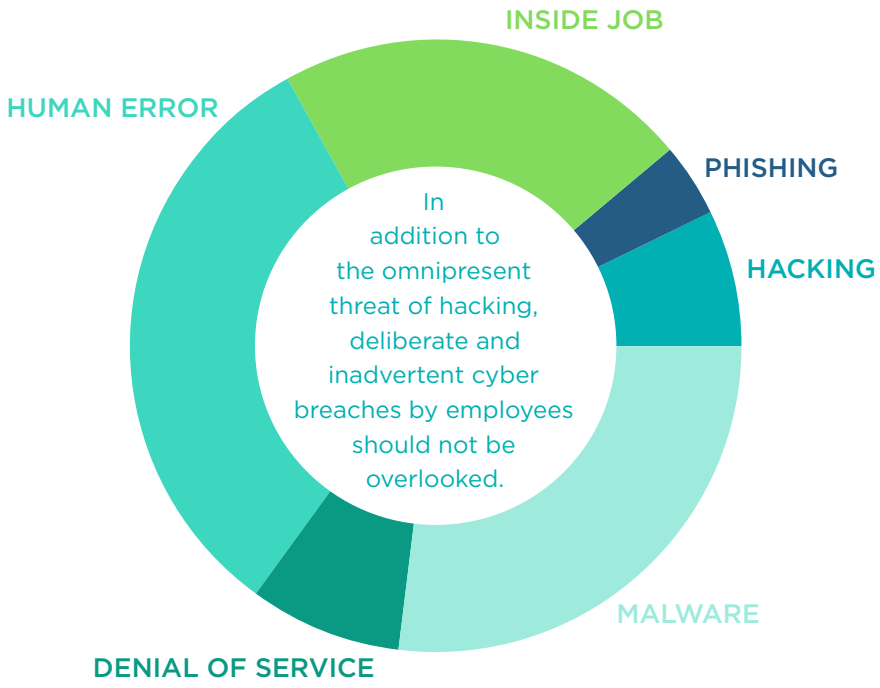
There are no mandatory reporting requirements for cyber incidents in New Zealand. However, the Privacy Commissioner's guidance advises notification in certain circumstances. Mandatory notification is an international trend, and is a focus of proposed reform of the Privacy Act.

"Put cyber security on the agenda, before it becomes the agenda."

Institute of Directors

"Security is a business issue. Not a technical issue."

World Bank Working Paper No. 26



2. RESPONDING TO A BREACH

Relevant issues include:

- Compliance with Privacy Act and related guidance
- Crisis/incident management to address reputational priorities as well as legal obligations
- Contractual and consumer law obligations to customers
- Contractual obligations from suppliers
- Cyber insurance claims
- Asserting rights against hackers, employees and suppliers
- Defending claims including potential class actions from customers, employees and shareholders
- Listing Rules, including disclosure obligations
- International regulatory obligations

The importance of cyber security at board and management level seems clear when looking at the drop in share prices at some major U.S. companies within a month of significant cyber attacks. But share prices rarely tell the full story: even where declines are limited, companies affected by a cyber breach face a range of direct and indirect costs including reputational damage and lost business.

CYBER SECURITY CONTACTS

Like many businesses, Bell Gully recognises that cyber security is much more than a technology issue. We have a cross-practice team experienced in cyber security issues.

Our cyber security team brings together privacy and data protection, employment, corporate/commercial, consumer, technology and e-commerce, intellectual property, insurance and risk, financial services, crisis management and litigation expertise.

Our practice ranges from advising New Zealand and international clients on cyber security issues in the context of directors' duties and governance, customer and supplier contracts, mergers and acquisitions, IPOs, listing rules, employment agreements, privacy policies and requests for personal information, through to managing cyber breaches, communicating with the Privacy Commissioner and customers and responding to complaints and investigations.

Privacy is a rapidly developing area of the law and cyber issues are the focus of upcoming Privacy Act reform. We are closely monitoring developments to keep our clients abreast of developments that will affect their business.

KEY CONTACTS:

Laura Littlewood
PARTNER

DDI +64 9 916 8928 MOB +64 21 828 429
laura.littlewood@bellgully.com

Tania Goatley
PARTNER

DDI +64 9 916 8766
tania.goatley@bellgully.com

Dean Oppenhuis
PARTNER

DDI +64 4 915 6921 MOB +64 21 317 697
dean.oppenhuis@bellgully.com

Kristin Wilson
SENIOR ASSOCIATE

DDI +64 9 916 8913 MOB +64 21 658 320
kristin.wilson@bellgully.com

Richard Massey
SENIOR ASSOCIATE

DDI +64 9 916 8824 MOB +64 21 208 2355
richard.massey@bellgully.com