CYBER SECURITY

RESPONDING TO A BREACH

Your Bell Gully team

Like many organisations, 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 clients/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 have a strong understanding of privacy in the public sector having advised a number of public sector clients on compliance with privacy law in the context of data breaches. 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

CYBER SECURITY

RESPONDING TO A BREACH

From crisis to control

The minutes and hours following a cyber attack on your business will determine whether the attack is repulsed with minimal or no loss or whether the business suffers serious – even fatal – damage. Here is a checklist for dealing with a cyber attack to be used in conjunction with your business's pre existing plans for managing such a crisis.

CRISIS

01 Detection of attack

Upon detection, staff should immediately inform the IT team.

02 Escalation

The IT team should initially assess the attack and determine whether notification should be escalated to senior management.

03 Assemble crisis team

If attack is escalated, the business should immediately assemble a pre-designated crisis team, consisting of the senior manager as convenor, head of the IT team, (in-house) legal counsel, in-house communications staff and external advisors as required (computer experts; legal counsel; a public relations firm).

04 Confirm organisational structure within crisis team

Leadership, objectivity and ensuring legal privilege over communications are important factors.

05 Intervene in computer systems

Computer experts should access the business's systems for the purposes of (a) stopping or neutralising the attack (if ongoing); (b) investigating the extent of the security breach and itemising lost data; (c) investigating the cause of the breach (while not prejudicing collection of evidence for later legal proceedings); and (d) making improvements required to prevent a repeat.

06 Implement internal and external communications management plan

Ensure that (a) communications are based on solid factual foundation; (b) the business speaks with one voice, delivered through designated spokespeople; and (c) external communications in particular are thoroughly vetted.

07 Initiate communications with public

If investigations reveal that client/customer information has been lost, the business should inform clients/customers immediately.

08 Comply with legal obligations arising from cyber attack

Legal counsel should advise the business on obligations arising from the attack, co-ordinating with overseas counsel where necessary. These obligations could include, for example, obligations to disclose the attack to regulators, law enforcement, securities markets and insurers.

CONTROL

09 Co-operation with law enforcement and GCSB

In some cases, state agencies may be able to assist the business's computer experts in ensuring that the attack has been defeated.

10 Litigation

In the short term, the business should consider whether legal steps are possible and appropriate to forestall further attacks, e.g. to source the attack. Over the longer term, the business will need to consider whether it can bring a claim for damages against the attackers or related parties such as ISPs. The business will also need to assess its exposure to claims from clients/customers and others.

11 Communication

Reassure clients/customers and general public that the business has brought the situation under control.