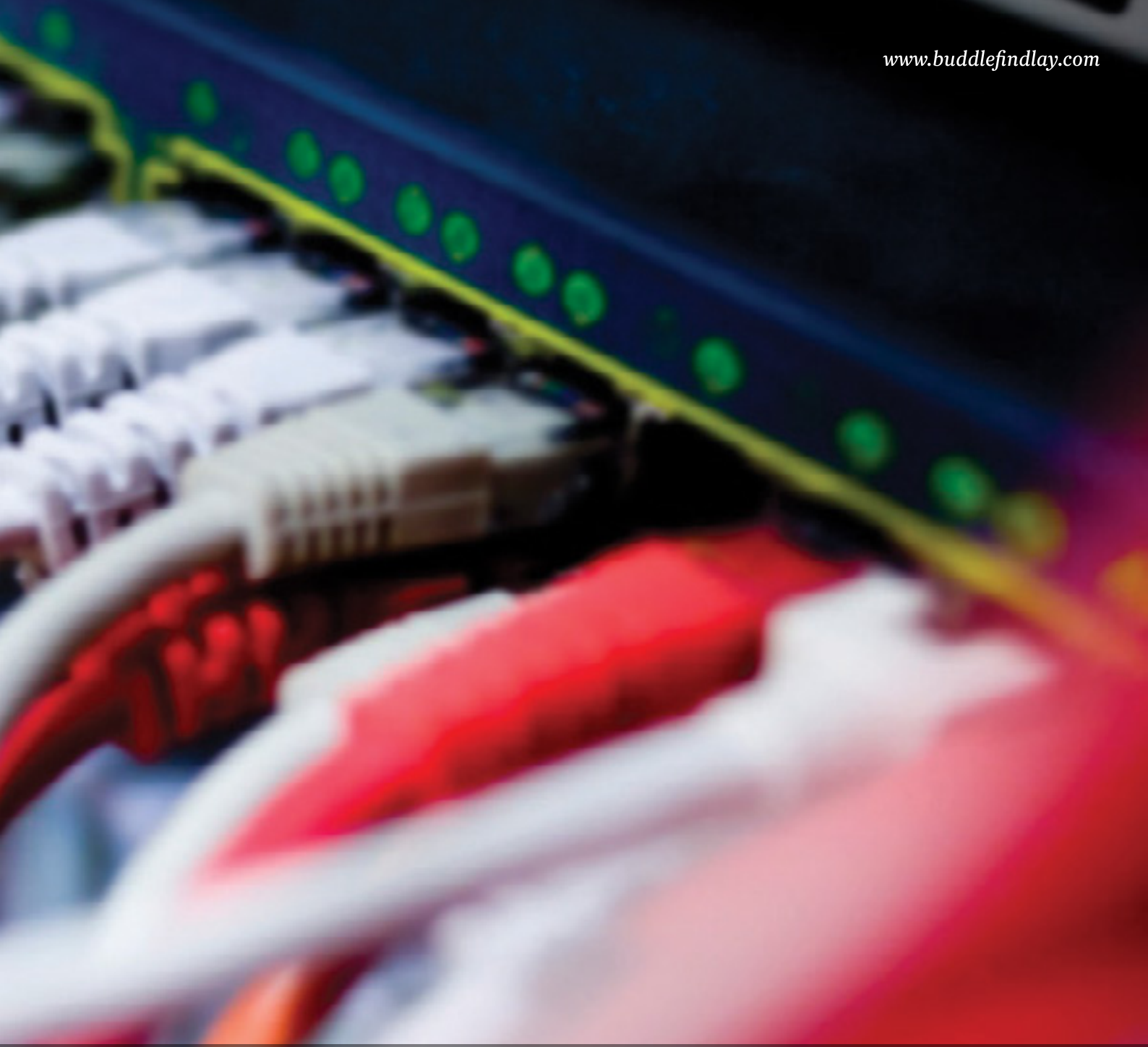


Safe and sound

A guide to keeping information secure

BUDDLE FINDLAY
NEW ZEALAND LAWYERS

March 2015

Auckland

PwC Tower
188 Quay Street, PO Box 1433
Auckland 1140, New Zealand
DX CP24024
P. 64 9 358 2555
F. 64 9 358 2055

Wellington

State Insurance Tower
1 Willis Street, PO Box 2694
Wellington 6140, New Zealand
DX SP20201
P. 64 4 499 4242
F. 64 4 499 4141

Christchurch

83 Victoria Street
PO Box 322
Christchurch 8140, New Zealand
DX WX11135
P. 64 3 379 1747
F. 64 3 379 5659

Setting the *scene*

Allan Yeoman
Partner, Buddle Findlay

New Zealand's Privacy Act turned 21 last year. It seems appropriate that its coming of age has coincided with an awakening in the public consciousness of privacy issues and a general shift in public attitudes towards privacy.

For much of those 21 years, data privacy was regarded as a stale topic but the pervasiveness in the last decade of the internet, social media platforms, smart phones, 'big data' and vast customer databases has changed that. More and more often, privacy is seen as a human right and privacy stories are increasingly prominent in mainstream media. We hear a lot about growing frustration with opaque and ever-changing Google or Facebook privacy practices; and about high-profile data security breaches, involving everyone from government departments, to global retail and e-commerce giants such as eBay, Target and Home Depot, or Hollywood players like Sony Pictures and Jennifer Lawrence.

Breaches of this magnitude and profile were not conceivable when New Zealand's Privacy Act first came into force in 1993 – the intervening years have seen vast swathes of data and records moved online, creating attractive targets for hackers and data thieves, and exposing organisations to amplified compliance obligations and vulnerabilities.

The upshot of this sharper focus on privacy is that any organisation that chooses to store information online (whether in its own systems or through a hosting provider) runs the risk that they will one day need to respond to a security breach, and deal with the inevitable reputational fall-out.

And yet, despite the changing landscape and the heightening of awareness of privacy and security risks, two things have remained constant.

First, New Zealand's Privacy Act (and many other equivalent pieces of legislation in other countries) has not evolved much in the last two decades, instead relying on broad principles which agencies must – with the help of guidance from the Privacy Commissioner and limited case law – interpret and apply.

Second, a culture remains among many organisations that 'it won't happen to us'. So while the public and the regulators will be quick to judge and react if a privacy breach occurs, many New Zealand companies and agencies are under-prepared for guarding against and responding to a security breach.

In this Guide, we address recent developments in security and information privacy, and look at international guidance to see what practical steps organisations can take to keep valuable information safe and sound.

The rise of the data breach.

An unfortunate but real side-effect of living in a connected world is that the valuable information we store online – trade secrets and strategy documents, intellectual property and personal information – will be accessible to others, unless we take steps to secure it.

As more and more information moves online, so do attempts to gain unauthorised access to it. PricewaterhouseCooper's (PwC) Global State of Information Security® Survey 2015 reported that, globally, there were 42.8 million detected cyber security incidents in 2014, an increase of 48% over 2013 and a year-on-year increase of 66% since 2009. Alarmingly, PwC notes that figure of detected incidents is probably conservative – the most successful attacks go undetected, and many detected attacks go unreported for fear of regulatory action, reputational damage or financial impact.

The causes behind this trend are several: the external groups behind some of the threats have become more sophisticated, better organised and better funded; it is easier than ever to access malware and other tools; the trove of information to target continues to grow in volume and value; and the range of devices and services we use to funnel information into servers continues to expand, from social networks and smartphone apps, web mail, iCloud and other cloud storage services, to baby monitors, fridges and other household devices as the 'Internet of Things' takes off.

"small and medium organisations are increasingly at risk of attack for the very reason that their security practices and defences are unlikely to be as mature or sophisticated as those of a larger organisation."

For organisations, it can be tempting to read about incidents involving Target, Sony Pictures or eBay and conclude that the risk of a security breach is only relevant to global corporate giants or those operating in particularly sensitive sectors, such as healthcare, telecommunications or financial services. But as those traditional targets continue to take more effective security measures, small and medium organisations are increasingly at risk of attack for the very reason that their security practices and defences are unlikely to be as mature or sophisticated as those of a larger organisation. PwC's Survey also points out that smaller firms may become targets as a foothold into larger organisations with which they partner and have interconnected their systems. For those larger organisations, looking at a partner or supplier's security practices should form a critical part of third party due diligence.

A focus on threats from hackers, organised criminal syndicates or other external groups also fails to recognise that security incidents can come from within – an opportunistic employee, service provider or someone else who we let in to our systems is just as likely to be behind a security incident as a rogue nation state or Russian cyber criminals. Insiders are also unlikely to be too choosy about the size or profile of the organisation whose information they are accessing, making this a relevant threat to an organisation of any size.

As the threat and the stakes rise, the need to keep information secure is clear; the logical next question is **'how do we do that?'.**

The bigger picture.

To design and implement an effective security plan, organisations should take a broad view of what the plan should cover, how it should be prepared and what sort of risks need to be guarded against.

Good practice, not just good law.

For New Zealand organisations, there are reasonably limited prescriptive, legal obligations when it comes to implementing and maintaining security measures. The Privacy Act 1993 requires that "reasonable" security measures are taken (more on this later). Public sector agencies (and their service providers) have available additional guidelines, such as the New Zealand Information Security Manual, which sets out requirements and recommendations depending on the classification applied to various types of information.

Healthcare, telecommunications and financial services providers can be subject to additional sector-specific regulatory requirements and/or guidance, but – across all of these reference points – the onus is typically put on the organisation to determine what the risk is and what it should be doing.

However, focusing only on limited prescriptive legal requirements, and doing just enough to meet them, is unlikely to lead to a successful or effective security strategy. Instead, organisations need to think about not only what they should be doing as a matter of good legal compliance, but also about what good practice would involve. To understand what that would look like, a broader world view – taking on board international guidance – is necessary.

"the onus is typically put on the organisation to determine what the risk is and what it should be doing."

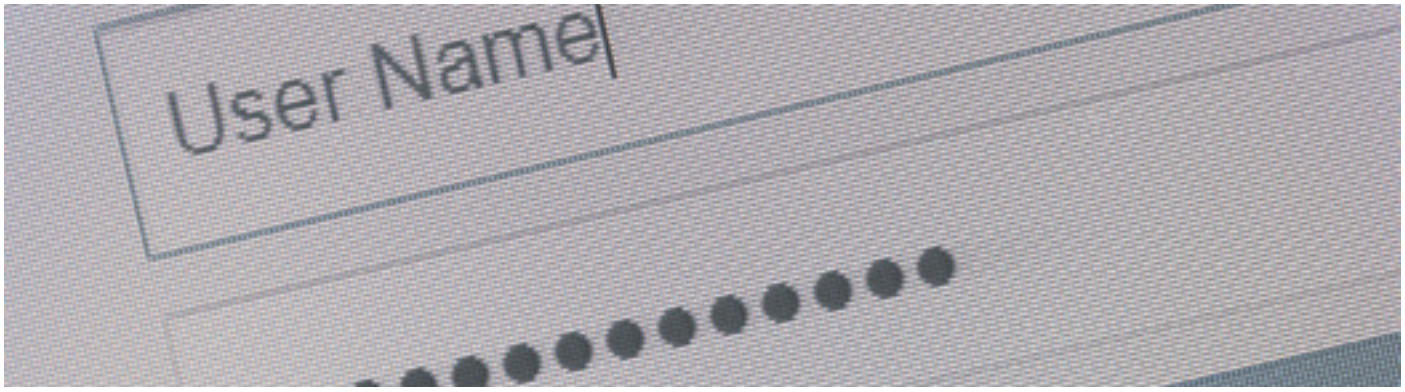
The human factor.

The second area where it is important to take a broad view is in the scope of an effective security strategy. It is tempting to classify information security as an IT issue, but this neglects the reality that a huge proportion of security incidents are the result of human error (or human malice) – documents being attached to the wrong email, emails being sent to the wrong address, snoopy employees looking up their neighbour's health records and laptops being left in parked cars are all brought about by lax security practices and attitudes. IT can provide a safety net to limit these events occurring, or mitigate the damage when they do, but the starting point should be about educating and monitoring staff to make sure that they are aware of their responsibilities as well.

Laura Bell, founder and lead consultant at SafeStack, an information security advisory practice, rallies against use of the word 'cyber' for the very reason that it misleadingly narrows the focus of security practices into an online threat, and something that can safely be left to the IT department to worry about. She uses the analogy of safety systems in a car to illustrate why the human factor is so important – a car may have ABS brakes, airbags and the most sophisticated crash-detection systems and warning features available, but if the driver is distracted, or tired, or has had too much to drink, then accidents will still happen. Information security systems are no different – the biggest vulnerability is the person interacting with them, or actively looking for a way around them to make their job easier.

The same point was made in KPMG's report into the ACC privacy breach in 2011, in which an employee accidentally dragged and dropped into an email a spreadsheet containing sensitive details of almost 7,000 ACC claimants and their medical conditions. KPMG found that, while the breach was a result of human error, the human error was able to happen because of systemic weaknesses in culture, processes and accountability for privacy issues.

Guarding against that means that a security strategy needs to involve more than just the IT department putting in place encryption, SSL and firewalls – it needs to come from the boardroom table down, reflect itself at all points where an organisation collects, uses and stores valuable information, develop and foster a culture of privacy awareness, and weave itself into the fabric of an organisation's practices and attitudes towards privacy and information security.



Privacy as principles.

Information security should focus on more than just personal information – the Sony Pictures hacking scandal in late 2014 involved access to personal email correspondence, but far more financially damaging in that instance was the leaking of unreleased movies. However, it's essential to understand what privacy legislation requires regarding security – breaches involving personal information affect thousands if not millions of individuals whose personal details are compromised (rather than just one entity looking to protect confidential or proprietary information), and while stolen credit card numbers can be changed, names, health information, and other sensitive personal information can not.

New Zealand's Privacy Act, like many other similar pieces of legislation around the world, relies on 12 Information Privacy Principles to set the bar for what organisations need to do to ensure the integrity and security of personal information they collect and use. That approach – rather than a set of codified or highly prescriptive requirements – has meant that the Privacy Act has remained workable over the years, despite huge growth in the volumes of personal information collected and exchanged, the actors using it, the technology and devices used to process and store it, and the business models built around it. However, it also means that organisations need to rely heavily on what guidance is available, in order to understand how those principles should be applied and interpreted.

Information Privacy Principle 5, which deals with security measures, is a perfect illustration of this. It would be almost impossible to be prescriptive about what security measures need to be put in place given the pace of technological change, and so instead Information Privacy Principle 5 states that agencies holding personal information must ensure:

"that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against: (i) loss; (ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and (iii) other misuse."

The agency's obligations therefore turn on what is reasonable in the circumstances. From that starting point, and even with the benefit of regulatory guidance, many organisations find it hard to know where to begin.

Filling in the gaps.

Concepts of "reasonable", "adequate" or "appropriate" security measures abound in data privacy legislation around the world. To help understand what those concepts mean, and what regulators expect of organisations, it's useful to look more closely at some of the international guidance that's available.

Australia

The Office of the Australian Information Commissioner's (OAIC) **Guide to securing personal information: 'reasonable steps' to protect personal information** (January 2015) offers perhaps the most relevant guidance to complement that available to New Zealand organisations.

The OAIC's Guide encourages organisations to design physical and technical information security measures which **prevent, detect** and **respond** to potential privacy breaches and describes the circumstances that should be taken into account in determining what security measures are "reasonable":

- The nature of the entity holding the personal information
- The amount and sensitivity of the personal information held
- The possible adverse consequences for an individual in the case of a breach
- The practical implications of implementing the security measure, including the time and cost involved
- Whether a security measure is itself privacy invasive.

The OAIC Guide goes on to outline a range of security measures that could be implemented, depending on an organisation's assessment of risk.

New Zealand

The Privacy Commissioner has published a **Data Safety Toolkit** (May 2014) which provides guidance to organisations on how to prevent and deal with security breaches.

It provides practical recommendations for steps that can be taken to guard against security breaches, and contains a number of real-world case studies to highlight common failings and the Privacy Commissioner's regulatory responses to those incidents. It also offers guidance on how to respond to a data breach, including by reminding organisations of the Privacy Commissioner's stance on notifying the Commissioner and affected individuals. While, at this stage, organisations are strongly encouraged to notify, the Privacy Act is due to be reformed over the next 1-2 years, and it is expected that breach notification will become a mandatory requirement.

There are a range of additional resources available to public sector agencies – please see the Additional References at the end of this Guide.

European Union

The 7th Principle of the EU Data Protection Directive does a good job of reminding us that security needs to be about more than technical measures, by referring expressly to **organisational** measures, as well as requiring agencies to ensure the "reliability" of any employees who have access to personal data. Measures taken must be **appropriate** to the nature and sensitivity of data in question, and the harm that could result, taking into account both the state of technological development and the cost of implementing security measures.

The extent to which this Principle has been elaborated on by national privacy regulators within EU Member States varies greatly – for example, Spanish and German Data Protection laws contain comprehensive and prescriptive security measures which must be implemented, according to the sensitivity of the data in question.

The guidance issued by the UK Information Commissioner's Office is the most relevant in a New Zealand context and includes:

- **A practical guide to IT security**, targeted mainly at small businesses
- Specific guidance on security for **Bring Your Own Device (BYOD)**
- **Guidance on the use of cloud computing**.

United States

Data privacy and security obligations in the United States tend to be piecemeal, with various states setting requirements and obligations applying to specific sectors or groups of individuals (such as financial services, health information and children). However, the Federal Trade Commission's (FTC) **Protecting Personal Information: A Guide for Business** (November 2011) encourages businesses to build a data security plan on five key principles:

- **Take stock:** Know what personal information you have
- **Scale down:** Keep only what you need for your business
- **Lock it:** Protect the information you keep
- **Pitch it:** Properly dispose of what you no longer need
- **Plan ahead:** Create a plan to respond to security incidents.

For further **FTC guidance** on data security see the FTC website.

Steps for implementing and maintaining an effective security plan.

A common theme to emerge from this guidance is that implementing an effective security plan needs to involve two distinct stages: first, organisations need to carefully consider the risk that they face, and what that means in terms of threats that may arise and their security and legal obligations; second, they should design and implement a security plan that is appropriate and responsive to those risks, and adaptable to others that may emerge.

Know your data.

Real privacy compliance is about more than posting a privacy policy on a website. An organisation should regularly audit what personal information it is collecting and holding, so that it has a clear understanding of what it needs to be doing to keep that information safe and secure.

An organisation needs to consider

What information is held, and what that means for its legal obligations – the extent of personal information (and the harm that could be caused if it is lost or stolen) will inform the level of security that is needed, and particularly sensitive information (such as health or credit card information) will trigger additional compliance requirements. If an organisation holds or has access to another party's commercially confidential information, then there will most likely be additional contractual security obligations to be met.

Why is the information needed, and – more importantly – is it actually needed? Under the Privacy Act, personal information can only be collected if it is necessary for a lawful purpose connected with a function or activity of an organisation. If that test can't be satisfied, then the information shouldn't be collected in the first place.

What could go wrong if the information fell into the wrong hands, and what harm (financial, reputational or embarrassment) could affected individuals suffer?

Think globally.

The smallest of businesses can easily have a global footprint. If a business targets or supplies to overseas markets, privacy practices, regulations and expectations may be stricter than they are in New Zealand. Even if there are good legal reasons why US or European privacy laws won't apply, customers in those markets may expect an organisation to meet the same privacy practices and standards as everyone else, so it's important to understand what additional obligations or requirements there might be under local law.

The data lifecycle.

The assessment of security risks and measures needs to apply through the whole data lifecycle – from collection, use, sharing and storage, all the way through to destruction. If you use a third party storage provider, SafeStack's Laura Bell recommends testing their deletion features to make sure that data is in fact being permanently and securely destroyed. If the customer support desk can proudly restore it a few weeks later, then you may not be meeting your obligations.

Sharing your data.

If you engage a hosting or cloud provider to store data on your behalf, or share it with other partners or service providers (such as data analytics, marketing or research companies) you will still be liable under the Privacy Act for making sure that the information is kept secure while in their hands.

Do your due diligence on service providers and partners to make sure that they meet the standards you expect, and that they don't have a poor history when it comes to privacy and security incidents. Cloud providers won't offer much in the way of warranties or contractual recourse, but it's important to satisfy yourself about the steps they take to secure your information, where it will be stored and what redundancy measures they can offer.

What should a security plan look like.

Security measures.

An effective security plan should be a blend of technical, organisational and physical safeguards. An assessment of security risks (and legal obligations) will help determine how many of these should be implemented, and how sophisticated they should be, but good practice would include security measures such as:

- Ensuring that a culture of privacy and security awareness is fostered and developed, so that staff are aware of their obligations and take them seriously
- Putting in place internal policies and procedures that reflect the organisation's approach on potential privacy weak points (eg, clean desk policies and guidelines around BYO Devices and use of removable storage devices)
- Implementing IT security measures to protect systems and devices from intrusion, human error (such as accidental emailing of sensitive information), malfunctions and system failures, and which could include:
  - encryption
  - firewalls and other intrusion prevention and detection measures
  - regular software updates to address known security risks
  - regular backing-up of key systems
  - password requirements
  - audit logs and access monitoring
- Physical safeguards such as swipe cards, alarm systems and other means to control access to premises, physical segregation of staff handling sensitive information, and procedures for handling, storing and transporting information in hard copy form.

It's worth noting that only a minority of these measures would directly involve the IT department – while IT security can be an effective security net, locked doors and filing cabinets, and ensuring that staff know their responsibilities when it comes to handling personal and sensitive information, are just as important.

Plan for the worst.

A good security plan should focus not only on prevention, but should also envisage that a security incident will happen and ensure that the organisation is prepared for when it does. Part of that response will be operational in nature and dovetail with a disaster recovery plan – such as ensuring business continuity and restoring key systems and datasets – but Laura Bell also recommends that organisations prepare for the external fallout:

- Know what experts you're going to call in – security consultants, IT forensics, lawyers and PR advisers
- Have a press release ready to go and know what your organisation's strategy in dealing with the media will look like
- Know when you need to notify the Privacy Commissioner and other stakeholders, such as the stock exchange, regulators or government ministers
- Test the response by doing a dummy run, in the same way you'd test a disaster recovery plan or carry out a fire drill.

Revisit and reassess.

Security threats and technology are constantly evolving, and so too should a good security plan. Take stock of security incidents and near misses (whether they happen to you or someone else), and apply the lessons learned to make sure that weaknesses are addressed and staff remain vigilant and proactive.

New business practices – such as a change of hosting providers, new products or services, or new systems implementations – can lead to additional privacy and security risks. Carry out a Privacy Impact Assessment (PIA) as part of your risk management processes so that any issues can be identified, assessed and addressed in your security plan.

About the author.

ALLAN YEOMAN
Partner
DDI: 64 9 363 1029 | Mobile: 64 21 766 312
allan.yeoman@buddlefindlay.com

Allan Yeoman is a partner in the TMT practice at Buddle Findlay. He has worked with public and private sector organisations in New Zealand and Europe to help put in place privacy compliance programmes, advise on regulatory obligations and prepare for and manage the fall-out from security incidents.

Additional contacts.

PHILIP WOOD
Partner
DDI: 64 9 357 9385 | Mobile: 64 21 624 356
philip.wood@buddlefindlay.com

STEVE NIGHTINGALE
Partner
DDI: 64 4 498 7312 | Mobile: 64 27 668 2832
steve.nightingale@buddlefindlay.com

ANDREW MATANGI
Consultant
DDI: 64 4 498 7315 | Mobile: 64 21 706 136
andrew.matangi@buddlefindlay.com

AMY RYBURN
Senior Associate
DDI: 64 4 462 0904 | Mobile: 64 21 242 5889
amy.ryburn@buddlefindlay.com

Acknowledgement.

We are grateful to Laura Bell, Founder and Lead Consultant at SafeStack, for her contributions to this Guide. SafeStack is a specialist agile information security firm, which provides consultancy, training and mentoring services to organisations at all stages of growth.

SafeStack
AGILE APPLICATION SECURITY

Sources

New Zealand

Data Safety Toolkit
https://www.privacy.org.nz/news-and-publications/guidance-resources/data-safety-toolkit/

Privacy Commisioner's guidance on PIA's
https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/

Australia

Guide to securing personal information: 'reasonable steps' to protect personal information
http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information

European Union references

A practical guide to IT security
https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Bring Your Own Device (BYOD)
https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

Guidance on the use of cloud computing
https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

United States

Protecting Personal Information: A Guide for Business
http://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

For further FTC guidance on data security, see
http://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

Additional references

Managing cyber risks in an interconnected world (October 2014) reports on and discusses the key findings of PwC's Global State of Information Security® Survey 2015, and measures New Zealand against the rest of the world across a number of key areas. It identifies some disturbing truths and trends in the rise and source of security incidents.
http://www.pwc.co.nz/PWC.NZ/media/pdf-documents/pwc-security/pwc-gsiss-2015-the-global-state-of-information-security-survey.pdf

KPMG's **Independent Review of ACC's Privacy and Security of Information** (August 2012) followed the highly-publicised data breach of 2011 in which an ACC staff-member inadvertedly sent a detailed spreadsheet to an ACC client. KPMG's report identified a number of systemic and cultural shortcomings, and is essential reading for anyone looking to avoid the same mistakes.
http://privacy.org.nz/assets/Files/Media-Releases/22-August-2012-ACC-Independent-Review-FINAL-REPORT.pdf

The New Zealand Government has launched the **Connect Smart programme**, which aims to educate businesses, home and school users on the importance of cyber security. Developed in collaboration with industry partners, they have published the **Connect Smart for Business: SME Toolkit** (June 2014), which provides accessible and recommendations and guidance for designing and implementing a cyber security plan.
http://www.connectsmart.govt.nz/assets/SME-Toolkit/Connect-Smart-for-Business-SME-Toolkit.pdf

The Department of Internal Affairs has produced specific guidance on **Cloud Computing: Information Security and Privacy Considerations** (April 2014). While primarily targeted at public sector agencies, it contains useful guidance on the kinds of issues that any organisation should be considering (such as security, data sovereignty and availability) when considering a cloud provider.
http://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf

The **New Zealand Information Security Manual** (NZSIM) is published and maintained by the GCSB. Last updated in December 2014, the NZISM provides "minimum technical security standards for good system hygiene, as well as providing other technical and security guidance for government departments and agencies to support good information governance and assurance practices."
http://www.gcsb.govt.nz/assets/NZISM-2014-December-2014-v2.2-PSR-Version.pdf

Further information on **Government initiatives and guidance on privacy and security matters** for public sector agencies.
http://ict.govt.nz/guidance-and-resources/information-management/privacy-and-security/