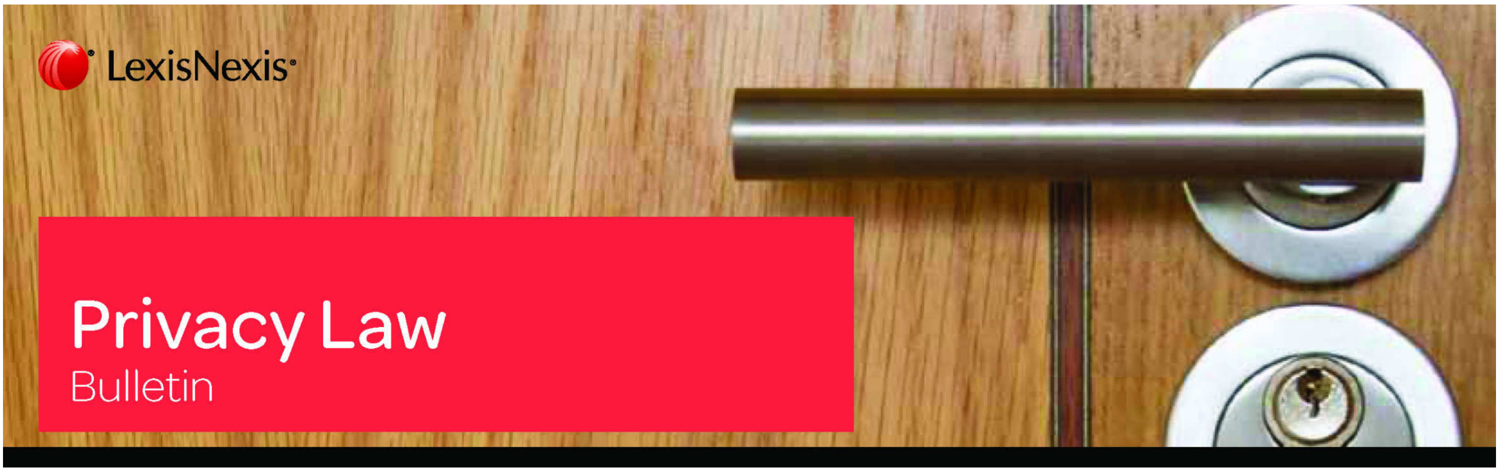

Privacy Law
Bulletin

2018 . Vol 14 No 9 & 10

Contents

Information contained in this newsletter is current as at January 2018

LexisNexis
Butterworths

Lost in cyberspace — "Danger, Will Robinson!"

Stephen Williams, Mike Baldwin *and* ***Daniel Coster*** *KOTT GUNNING LAWYERS*

"Cyber attack", "hacker", "ransomware" and "malware" have entered the common parlance due, at least in part, to a massive increase in media stories on the issue. The dangers of the internet-connected world have become increasingly apparent, and an estimated $300 million was lost to scams and fraud by Australians in 2016 alone.

This greater cyberthreat comes at a time when businesses are increasingly moving their assets into the digital world, with some retailers even closing physical stores in favour of an online presence.

The explosive proliferation of internet-connected devices in recent years perhaps explains this trend. By some estimates, there are more than 100 new devices being connected to the internet every second.

However, recent events have shown just how dangerous it can be for businesses in today's online environment. Successful cyber attacks seem to be making headlines almost on a weekly basis. It doesn't seem to matter how big you are either, with major law firms, retailers and health providers all targets:

> Australians could be caught up in an enormous hack of sensitive personal financial data that has left nearly half the American population at risk of identity fraud … [after] Equifax [confirms] the personal data of 143 million people has been hacked.[1]

One could be forgiven for thinking about closing up their shop, moving to the bush and going "off-grid". As appealing as rural life may be, it is probably more sensible to take some simple risk management steps before making such a momentous decision.

In no particular order, here are some measures you may wish to consider for your business:

1. Review policies and procedures, with a particular focus on IT (all elements outlined below ought to be embraced within this framework). Do you have policies and procedures in place for cybersecurity and for responding to a breach of security? Is your staff aware of the policies and procedures and kept up to date when these change?
2. Check on processes, do you have adequate backups and what is your disaster recovery plan? Do you even have one?
3. Is your backup onsite or offsite? How often is your data backed up and is it checked for integrity?
4. Train staff on how to spot threats and deal with them at work, at home or on the road (if they work flexibly or bring your own device (BYOD)). Your employees can be your greatest asset or your greatest liability. Does your staff know how to recognise a dodgy email or will they blindly open the attachment "overdueinvoice.exe" and cause you a headache? Or pick up that tempting USB stick lying on the washroom floor and plug it into their work computer?
5. As noted above, as employees can often be the weakest link, they should not share passwords or login details. This includes not writing them down on a post-it note next to the computer!
6. In addition, insist on good password protocols or consider password managers. Consider requiring employees to change passwords at regular intervals. This prevents passwords from becoming "stale". A good password should include a mix of letters, numbers, capital letters and symbols, and should certainly not be "password" or "abc123".
7. Consider requiring two-factor authentication. Two-factor authentication requires a user to enter password and then another separate login method to gain access (commonly entering a code received via SMS). Many websites now offer two-factor authentication to protect your accounts, including online banking and LinkedIn.
8. Employees should be encouraged to report all breaches and potential breaches of security. Taking measures to detect and prevent security breaches can save time, money and embarrassment later on.
9. Employees should also be aware of external security risks, such as public wi-fi "hotspots". The old adage "there's no such thing as a free lunch" rings true here. Public wi-fi hotspots are potentially vulnerable and, if poorly maintained, can easily be used to steal sensitive data from users.
10. Limit access to data, consider the "need to know" rule. This includes not putting your private commercial data on an unsecured server, which has happened! If the data is sensitive, access should be restricted to only those who need to know it. In addition, if your employees don't need administrative access on their work computer, consider

providing restricted accounts which are unable to make system-wide changes (and which could be exploited by malware).

11. Hardware should be adequately protected, whether in the server room, on the desk, or in the briefcase or pocket, and consider data encryption/remote tracking and remote wipe on portable devices. USB drives are a particular vulnerability, both in the spread of malware and in relation to the potential loss of sensitive data (whether accidentally or maliciously).
12. Ex-employees' access should be restricted as soon as they leave and all business related hardware returned immediately (including USBs).
13. Crisis management protocol (do you have one and is it well understood by all players?). This goes back to point 1 above and is essential to avoid a public relations disaster — and there have been plenty of these to watch and learn from.
14. Think about what you might say to employees, clients and the market/your industry if you were unlucky enough to have a data breach or hacking event, don't wait until after it's happened.
15. Limit media appearances until you are across all issues — do it once and do it right and make sure anyone affected by your breach can take action to protect themselves. Trying to cover it up will be a mistake and you will most likely have the problem blow up in your face!

The above measures are of course not exhaustive. The Australian Signals Directorate has a more detailed (but also more technical) guide to mitigating cybersecurity incidents.[2] You should check with your IT service provider whether the top four strategies mentioned there have been implemented and, if not, when they will be.

In short, cybersecurity requires a two-pronged approach. Firstly, managing your systems and processes, including ensuring software and hardware are adequately protected and locked down. Secondly, managing your staff to ensure that they are not inadvertently unlocking the gates and letting in the trojan horse.

Finally, whatever you do, do something! Malicious hackers will target the most vulnerable systems and the significant worldwide increase in cyber attacks makes cybersecurity a priority for all businesses with internet access.

The online environment is only going to get more complex for businesses. Mandatory data breach notification laws take effect in Australia from 23 February 2018, and thereafter the Office of the Australian Information Commissioner and any potentially affected individuals will have to be informed of an "eligible data breach". In addition, the European Union's (EU) General Data Protection Regulation comes into effect from April 2018; and if your business collects or processes the personal data of EU residents, this law will apply to you. We recommend you get professional IT help and that you ensure you have adequate cyber insurance cover in place by contacting a reputable broker.

Stephen Williams
Partner
Kott Gunning Lawyers
swilliams@kottgunn.com.au
www.kottgunn.com.au

Mike Baldwin
Special Counsel
Kott Gunning Lawyers
mbaldwin@kottgunn.com.au
www.kottgunn.com.au

Daniel Coster
Associate
Kott Gunning Lawyers
dcoster@kottgunn.com.au
www.kottgunn.com.au

The information published in this paper is of a general nature and should not be construed as legal advice. Whilst we aim to provide timely, relevant and accurate information, the law may change and circumstances may differ. You should not therefore act in reliance on it without first obtaining specific legal advice.

Footnotes

[1] S Smiley "Equifax: Australians' sensitive financial information at risk in data breach of US company" *ABC News* 8 September 2017 www.abc.net.au/news/2017-09-08/smiley-credit-check-australians-financial-information-at-risk/8887198; see also N Hopkins "Deloitte hit by cyber-attack revealing clients' secret emails" *The Guardian* 25 September 2017 www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails; "Uber boss says a data breach exposed 57m users' data and the company didn't tell anyone" *ABC News* 22 November 2017 www.abc.net.au/news/2017-11-22/uber-data-breach-was-not-disclosed-ceo-says/9179168.

[2] Australian Signals Directorate "Strategies to mitigate cyber security incidents: a new cyber security baseline" (5 February 2017) www.asd.gov.au/infosec/mitigationstrategies.htm.