大成 DENTONS KENSINGTON SWAN

A post-lockdown petri dish of data breaches – who's going to protect you?

JUNE 2020

Hayden Wilson
Partner

Hayley Miller
Partner

Campbell Featherstone
Senior Associate

The further we move into the digital world, the more obvious it becomes that you cannot leave your privacy management on cruise control. Your business needs a privacy breach plan. And you need to know which levers to pull in a crisis.

The latest developments in the Capital One saga – which involved a privacy breach that saw over 100 million people's data compromised across the US and Canada – are a lesson that crisis management expertise is indispensable when dealing with a breach.

What happened?

In 2019, a software engineer hacked a server holding Capital One's customer information, in the largest theft of data from a bank.

When Capital One confirmed the 2019 breach, it responded in accordance with its breach management response plan. Capital One had already engaged – some four years previously – security firm Mandiant under a master services agreement to provide security services, and incident response services where necessary. It also engaged lawyers to advise on its response – who instructed Mandiant to conduct security incident response, forensics, analysis, and remediation services.

The details of the resulting incident report laid bare the insecurities that had made it possible for the hacker to penetrate Capital One's cyber-security. In other words, it was not the sort of report you'd want to be made available in the context of a class-action suit. But that's exactly what a Federal Court held must occur, because, in the particular circumstance of their relationship with the security firm and the Capital One lawyers, the report Mandiant provided was not subject to the protections usually afforded by privilege.

Capital One had arranged protection, but not sufficient to block an enormous breach, and they had done so in a way that left them liable to have their shortcomings exposed to the fullest public gaze.

Why does it matter?

It's easy to dismiss international incidents as, well, just that – but the reality is that privacy breaches happen all the time, and they have the potential to wreak havoc. The agonies Capital One will be experiencing can play out in many forms, but one is especially dangerous: the deep harm that can be done to your reputation.

If it happens to your business, and you're not adequately protected, your shortcomings could be laid out for the world to see.

We've already made the case that life after lockdown means dealing with more data than ever before. What's more – especially where individuals' health is involved – very sensitive data.

For the majority of businesses, the rapid response to contact tracing requirements means that you'll already be responsible for more data than you might realise. And we expect this to only increase. We've also highlighted the potential for breaches given the number of businesses working from home. Less stringent procedures mean greater risk.

The upshot is that a post-lockdown New Zealand is a petri dish for breaches. When we talk about breaches, we don't just mean hackers exploiting major banks' insecurities. It could be as simple as an email sent to the wrong recipient, documents left on the bus, or an inability to access information because of a forgotten password.

And as we are set to finally see the introduction of New Zealand's notifiable privacy breach regime, you need to be prepared. On the commencement of the Privacy Bill on 1 December 2020, where personal information you hold is the subject of a notifiable privacy breach, you will have an obligation to notify the Privacy Commissioner and any individual affected or, in some cases, even give public notice. A failure to do so will be an offence, punishable by a fine of up to NZ$10,000.

But the main kicker for your business should be reputation. Research by the Ponemon Institute shows that data breaches are near the top of the list for consumers when considering impact on a company's reputation (beating out government fines and publicised law suits).

The true cost of a data breach – especially one mishandled – will be much greater than a NZ$10,000 fine.

What should we do?

Your best preparation is knowing who to call to avoid the worst outcome. The Capital One decision illustrates the need for expertise and care in a crisis – and highlights the value of engaging experts that will protect you in the long-run.

When a breach occurs, things move quickly, and not in synchronicity. Balancing competing interests like consumer opinion optics, regulator demands, and protecting your business' sensitive and confidential information can lead to bad decisions that could cause more of a headache than the breach itself.

Retaining crisis management experts will help steer you through the cloud of confusion.

But even before a breach occurs, there are some key steps your business should take:

- **Understand your weaknesses: It's very difficult for your business to plan for a breach – let alone execute that plan effectively – if you don't know what you're dealing with.** This means doing diligence early. Identify the 'crown jewels' of your business and then identify your weak-spots. What would an attacker's goals likely be? What sort of breach would make your business most vulnerable?
- **Make a plan: There's no 'one size fits all' approach to dealing with a breach. But most plans will have four steps at their core: identify, contain, respond, and learn.** Your plan should fit the nature of your business and the information you deal with – who should be in charge of overseeing a response? How will you know when a breach has occurred? At what point do you reach for that Big Red Button that calls in the experts?
- **Rinse and repeat: Data breach management is a moveable feast.** Your business and the data you manage is set to rapidly change, and so should your response plan. This means dusting off the plan for evaluation on a regular basis.

Key contacts

Hayley Miller
Partner
D +64 9 915 3366
M +64 21 870 477
E hayley.miller@dentons.com

Hayden Wilson
Partner
D +64 4 915 0782
M +64 21 342 947
E hayden.wilson@dentons.com

Campbell Featherstone
Senior Associate
D +64 4 498 0832
M +64 21 809 779
E campbell.featherstone@dentons.com