

Into the breach

How to prepare your organisation for the recent sweeping changes to Australia's privacy requirements.

In February, with little fanfare, new federal legislation came into effect with enormous ramifications for how large associations handle their member data. Private sector organisations, including not-for-profits, with an annual group turnover of more than \$3 million are now required by law to report data breaches to both the Office of the Australian Information Commissioner and any affected individuals, or face severe penalties.

According to Tom Crampton, head of Trusted Impact, a leading information security consultancy, it's not a matter of if you'll be hacked. It's when.

This issue is of concern to association executives as their database is one of their most valuable assets – and something very attractive to hackers.

Crampton says there are five things you can do to prepare for an attack.

1. Expect it

Most companies who get hacked are shocked that it happened. They weren't expecting it. "Forewarned is forearmed," Crampton said.

"If you expect it, you will have systems in place to deal with it. You'll be faster to act, and you can possibly stop it before it goes viral." This means ensuring your virus protection and software is kept completely up-to-date.

2. Talk about it with your team

Get the cyber-hacking conversation started with key members in your team – the board, the IT department, the management team. Everyone needs to be aware that it can happen to them.

Richard Stokes, Executive Officer at Australian Boarding Schools Association has a cautionary tale to tell. "My colleague Tom and I were in a meeting. Tom leans over and shows me an email I had 'supposedly' sent him requesting authorisation to transfer a large amount of money. He asks if I sent it. I said, 'no, I did not'.

"Clearly it was a cyber-hack but if Tom had not checked-in with me, he could easily have assumed I had sent that email. The email looked very authentic."

If you have a small team it's easy to cross-check but for larger teams, that is not possible. Stokes said, "If there is any doubt about the legitimacy of the email and it's to do with money, or an important issue, ask the sender to confirm their

request by resending the email to you. This will short-circuit the issue quickly."

3. Know what to look for

Hackers are brilliant at making their emails look legitimate.

But there's often tell-tale signs that give it away so if you know what to look for, you are more likely to spot it. Crampton has some tips on what to notice. "The image resolution of the logo may be poor. There could be an obvious typo. The titles of people may be slightly wrong," he said.

In isolation they may not give the game away but if you know what to look for and can see multiple issues with one email, you can alert your IT Department.

4. Have an escalation policy in place

Have a plan in place so that if or when it happens, you can respond quickly, professionally and calmly.

For example, does everyone know who to turn to if they think an email is fake? What's the correct procedure for reporting it and what information should be passed on? What should you do if you believe you have clicked on something inappropriate? At what point are the cyber-security experts called in?

If there's a clear plan in place for what to do when something is wrong, you'll be better able to stop it spreading.

5. Create a communications plan

Nothing creates panic like having the crew from A Current Affair show up on your doorstep. Be prepared so that if and when it happens, you've got all your bases covered.

Actions to consider include: Have you pre-written the emails that will alert your clients that a hack has occurred? Do you have a committee formed in advance, so they can convene quickly to deal with it? Have you brainstormed the questions (and possible answers) that members (or pesky journalists) are likely to ask if you've been hacked?

Having answers to tricky questions pre-written and rehearsed can help minimise the fallout and mitigate the loss of trust that may occur.

Cyber-attacks are a clear and present danger for every company, small and large, so take the time to create a plan in case it happens to you. It will be time and money well spent.