gadens

Profiles In Privacy

Justin Geri
Director, Forensic IT
Ferrier Hodgson

In our Profiles in Privacy series, we profile prominent players in privacy and data protection in Australia. Justin Geri is Director - Forensic IT at Ferrier Hodgson in Melbourne. He has been with Ferrier Hodgson for nearly 13 years. Justin's services are in high demand amongst organisations that suffer a cybersecurity breach – or that are trying to avoid one.

Gadens Partner, David Smith recently asked Justin about some topical privacy issues.

What are the common elements in the cybersecurity breaches you are seeing?

There are three recurring elements that lead to breaches: a malicious third party, a malicious internal party such as a disgruntled employee or human error. Or it might be a combination of these elements.

Most of the attacks we are seeing are not sophisticated. They rely heavily on impersonation techniques to gather credentials. But they are surprisingly successful, because many organisations do not have "two-factor identification" security technology in place.

Two-factor identification requires a user to enter a unique code – for example, a code sent by SMS to their mobile device – in order to confirm their access to a system. It is not a silver bullet, but it will go a long way to preventing these attacks.

Are there any particular industry sectors that are potential targets for fraud?

One potential target is the construction industry. This industry receives large payments for stages of work, which can be targets for interception by fraudsters. These companies do not always have adequate IT infrastructure in place. Also the companies in the industry often publicise their projects online, so there is a significant amount of publicly available information for fraudsters to work with.

If fraudsters are succeeding with fairly simple techniques, is there any hope for organisations to win?

Organisations can certainly increase their defences by taking some fairly simple steps.

What we will see is increased training, and a change in security processes as a result of the nature of the attacks that are occurring.

The training needs to convey to staff how careful they should be to avoid clicking on fraudulent emails that in some cases, are quite good at appearing "legitimate".

Staff need to develop a healthy level of scepticism about any situation where they may be sharing data with another person, or where they receive important information or instructions in what appears to be a genuine email.

We are advising businesses to pre-emptively say to their clients that they will never change their bank account details via email communication. This may help avoid some cases where the client is tricked into paying money into a fraudster's account. If that happens some very uncomfortable relationship issues can arise between the business, which has not been paid, and the client.

Working from home is another emerging risk area. The personal systems that staff use typically don't have firewalls and other security measures in place, comparable to those their employer uses. Organisations need to put more controls in place around this.

Are you seeing an increasing number of malicious cybersecurity breaches?

Definitely. We work with a number of good sized organisations, who you would not think would have an issue, who have been successfully targeted by hackers. In those cases, hackers effectively used very simple impersonation techniques in order to gather credentials. The simplest of security measures were not in place at the affected organisations.

Until the mentality of organisations changes from a password being sufficient security, they are going to be at significant risk.
An interesting issue is that when an external "intruder" gains access to an email account, they may have had access to thousands of emails. Some of those emails will contain personal information, but there may be no way of knowing if the intruder read particular emails. So in terms of deciding whether there is a legal obligation to notify of a data breach, we sometimes just have to "assume the worst".

Should you ever pay a ransomware attacker?

Absolutely not. There is no guarantee if a ransomware attacker is paid, that the organisation will receive their data back. And paying them only encourages and empowers them. In our work we have generally been able to recover much of the data that has been impacted by the ransomware infection without having to pay the attacker. Recent studies have shown that only around 20% of ransomware victims who pay actually get data back.

David Smith, Partner
Intellectual Property & Technology
T: +61 3 9252 2563
E: david.smith@gadens.com