Preventing and responding to cyber breaches

Patrick Fair, partner at Baker & McKenzie

KC Today we're talking about cyber breaches and how companies should respond, and I'm joined by Baker & McKenzie partner Patrick Fair. Thank you for joining us.

PF Hi Kat.

KC It feels like we've been talking about cyber security for a long time now. How are companies progressing in terms of handling that risk?

PF Look I think that culture is really under a major sea change. It's been a slow transition from physical systems and physical delivery. We're getting to the point now where I think Australia has the largest hybrids cloud internal infrastructure arrangements of any country on Earth – I heard that from a centre provider recently.

Where we used to have internal systems we now either have it out in a data centre or we have distributed between the internal systems and the data centre and this creates greater security challenges. It means that we've got higher levels of cooperation between service providers and diverse parts of our network and this means more interconnection, more places where data can be lost, and we're also more dependent on these systems for our reputation and the standing of our organization with our customers. So I think there's a major change really happening. It's been going for a long time but it's really happening now where small businesses are being subjected to data compliance profile checklists before their customers will deal with them or interconnect with them, where there's attention being paid to privacy policies and internal security arrangements, where your data security posture is really critical to your ongoing business success and your standing with your customers.

KC What infrastructure and systems should all companies have in place to reduce the risk of a cyber breach?

PF The infrastructure part of that question is a bit tricky because it depends on what kind of business you're running and of course it's a matter for the technical expertise of your Chief Information Officer or your Chief Security Officer, depending on the scale of your operation. Most businesses nowadays have the basic virus protection on all their PCs and monitoring. The sexy stuff is the security information management software and event management software, sometimes referred to jointly as SIEM and that stuff monitors the overall system, collects information, alerts when there are anomalies in behavior or traffic that indicates that there could be some kind of breach. They present the information by dashboard, there's compliance reporting, they retain information and they're very handy for forensics so a lot of businesses of any scale now are putting in place that kind of technical solution.

In terms of systems more broadly, I mean the main challenge for a modern enterprise is to create a sort of compliance culture within the organization and that can have a lot of elements to it. I mean the key things you need to have in place are basic policies, there are certain policies required by law, your privacy policy, but not

a lot of organisations have an internal privacy policy dealing with their employee information, which is not exempt from the Privacy Act and there is a category of information like that dealing with IT security, dealing with bring your own devices. Then there's kind of a structure around contracting which is really important in this area. The supplier security posture questionnaire, are your suppliers secure? If you connect with them, share your information with them, are they going to be a vulnerability?

Then there's terms and conditions in your contract. Some companies lately are changing the way they deal with information in their contracts so that you don't talk about just confidential information or private information, but you talk about business information more generally and you deal with issues such as the stats and information that arises from your information and taking control of that secondary category as well as dealing with incident responses and cooperation there.

Then you've got to have training in your organization. There's no point setting up all of the technical solutions if people are easily victims of phishing attacks and letting malware into your system because they've been fooled or your physical parameter security is weakened so people can plug things in on the wrong side of your network.

And then there's also board reporting and supervision. The new culture is to have a data map that shows where information is stored, what's offshore, what's outsourced, where it's being held and to ensure that there are reports to the board on security aspects of outsourcing and transactions that the business might enter into as well as prompt reporting of incidents and an ongoing monitoring of the updating and training that goes on in the organisation.

KC **What does a best practice response to a cyber security breach look like?**

PF Well the traditional four elements of a cyber security breach response are discovery, control and analysis, notification and then eradication and prevention. So a best response firstly has the systems in place and the procedures to identify when a breach has taken place and to report that to the right people internally. Does the CEO need to be told? Does the public relations person need to be told? Is risk management involved? At what level does this need to go? And as you'd appreciate it can be a bit of pressure for the information officer to keep the breach close to his chest until he knows exactly what it is.

Then there's notice for control and analysis, that sort of triage of the breach and doing an analysis of what happens. The challenge here is to make sure you don't destroy the information and evidence you need to take action. You might need external forensics to do the analysis, you need to shut down systems that might be leaking information.

Then there's notification and there might be quite a few people that might be notified in the case of a breach: the regulator, law enforcement, data subjects, insurers, the service providers that you're connecting with your business partners if their information might be affected. Working out what you want to say to the media and other stakeholders who could be involved, and the final step is eradication and prevention: looking at the analysis and saying "well how do we stop this from

happening again, what are we going to change so that we're not vulnerable in the future?"

KC **Patrick, let's talk about notifying customers who may be impacted by a breach. The recent news of Yahoo's data breach related to an event that occurred in 2014 – what's your take on this?**

PF Look I can't talk specifically about the Yahoo matter but there are a couple of features of that that at a broad level I think are worth comment. One is the apparently the long lead-time between the breach and discovery of the breach. Verizon does this brilliant data breach investigations report annually which constantly shows that the time for the bad guy to get in versus the time it takes to discover the breach are at extreme ends of one another. The time for the hacker to get in is getting shorter and the time that it's taking to discover the breach and act on it is getting longer. So in some ways it's not surprising to learn that it has been a delay between the breach being perpetrated and it being discovered.

The second thing to say is there's a state actor involved there by a report and this is a live issue: to what extent do national security agencies and enforcement take a role in protecting private information and private systems from attack. Can a commercial organization really be expected to maintain the high degree of military-level security that might be required in order to prevent a hack from a nation state? So a very serious breach and there have been a number recently but the features of it a very much of the time and a warning to organisations, I think.

KC **Thank you for your time today.**

PF My pleasure.