GETTING THE BOARD “ON-BOARD” WITH DATA BREACH NOTIFICATION

With the passing of the Privacy Amendment (Notifiable Data Breaches) Bill 2016, Australian companies have more reason than ever before to take cybersecurity seriously. IT leaders can expect questions and concerns from board-members about what the new laws mean for their organisation. Here’s how to answer some of the most common ones and bring business decision-makers onside with your cybersecurity strategy.

WHO DOES THE NEW DATA NOTIFICATION LAW AFFECT?

Australia’s upcoming Data Notification Law will apply to businesses governed under the Privacy Act 1988 – including any with annual turnovers of $3 million, or businesses that collect and store sensitive user information like payments or personal data. If a breach of the personal data under your responsibility will likely result in “serious harm” to individuals – whether of reputation, finances, or even safety – you’ll be required to notify the relevant parties. Remind your board that failure to do so can be costly – earning fines of up to $1.8 million!

WHAT DO I DO WHEN I DETECT A BREACH?

Verified breaches must be reported to the Australian Information Commissioner and all affected individuals, along with descriptions of the breach, the nature of any compromised information, and recommendations to individuals on what they should do next. Make it clear to your business leaders that time is of the essence: the law gives organisations only 30 days to investigate any suspected breach, or plug any possible data loss, before notification is required.

WHY SHOULD THE BOARD CARE ABOUT THE NEW LAWS?

Your board needs to recognise data breaches not as an “if” scenario, but as a “when”: 1 in 4 organisations with top cybersecurity defences still experience data breaches.¹ For those who might play down the costs of a breach, inform them that 90% of a cyber-attack’s bottom-line impact is felt up to two years after an attack. The new data breach laws add hefty fines and heightened public scrutiny to many other consequences of a breach: loss of sales and contracts, compromised intellectual property (IP), and legal action. If necessary, remind your business leaders that customers and shareholders will hold them responsible for non-compliance to these laws.

KEY POINTS

- 30 days notification reaction time.
- Failure to comply could incur fines of up to $1.8 million.
- Third-party experts can bolster in-house resources.
- Effective investments need to focus on “security by design”.

“Your board needs to recognise data breaches not as an “if” scenario, but as a “when”…”

HOW CAN HACKERS BREACH OUR DEFENCES AND GET OUR DATA?

Modern-day hackers usually use multiple channels of attack ("vectors") to raise the chances of successfully breaching a company’s defences. Covering all these vectors requires a lot of manpower and investment, as does keeping up with the latest threats that malicious parties invent. With more new vectors than ever before – like Internet of Things (IoT) devices, unsecured personal smartphones, and even accessing public WiFi on corporate laptops – encourage your board to take cybersecurity spending seriously and consider bringing in third-party providers to bolster your in-house resources.

WHERE SHOULD WE INVEST IN BOLSTERING OUR CYBERSECURITY?

The most effective investments focus on “security by design”, not simply adding more security systems to your infrastructure. The best way to explain “security by design” to your board and/or team is as a bottoms-up approach to security: giving your firewalls, devices, monitoring platforms, and all other cybersecurity systems a common language and platform to work together. It also involves making cybersecurity an inbuilt part of IT management and business use policies, like regular updating and testing of systems. That’s something the board can play an invaluable role in promoting throughout the business – and with the new data breach legislation coming into force, it’s in their best interests to get everyone committed to keeping the organisation’s data secure.

“...making cybersecurity an inbuilt part of IT management and business use policies.”

IS IT JUST OUTSIDE THREATS WE NEED TO WORRY ABOUT?

Not at all. While executives may argue simply bolstering endpoint or outer-layer defences is enough to stop hackers, remind the board that a growing number of malicious data breaches – and almost all accidental ones – stem from within the organisation, not outside of it. That’s particularly true with so many employees, including most executives, opting for BYOD plans and using their many devices both at work and in less-secure settings.

HOW CAN WE REDUCE THE LIKELIHOOD OF A BREACH?

Monitor your networks. Some studies indicate that it takes an organization upwards to a year to realise that their data has been compromised. Explain to your board that a robust monitoring system not only helps you and your team identify and stop threats more consistently, but also makes compliance to data breach notification laws much simpler. The more visibility you have on your data and networks, the easier it is to give details to regulators and the public if a breach occurs.

VISIT FORTINET’S DATA BREACH NOTIFICATION PAGE FOR WHITEPAPERS AND OTHER RESOURCES TO HELP UNDERSTAND NOTIFICATION LAWS AND HOW TO BEST NEGOTIATE THEM?

Want to know more about the data breach notification laws and how to best negotiate them?

Visit Fortinet’s Data Breach Notification page for whitepapers and other resources to help you turn this new legislation into greater organisational support for cybersecurity.