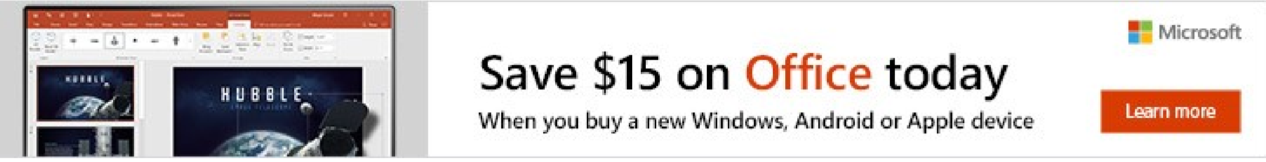

Burning down the house: CEO attitudes to cyber security all wrong

Executives fail to prioritise cyber security, leaving IT teams struggling to secure their businesses, says Michael Connory

George Nott (CIO)

10 September, 2018 10:54

0

0 Comments

A CEO of a major Australian company put it to security consultant Michael Connory like this:

“Implementing these [cyber awareness and governance] programs is like home insurance – high cost with no guarantee anything will ever happen – so why pay the price? How many houses burn down every year, compared to how many people buy house insurance?”

This attitude towards is all wrong but not rare, says Connory whose firm Security In Depth has just published the results of research which found 83 per cent of Australian companies have no policies or plan in place for a data breach and 41 per cent said they “did not understand” what an ICT security framework was.

“We look at what has been said and done and companies and executives are more often than not complacent with cyber,” Connory says.

"It is our view, based on the number of organisations that have failed to implement what we believe are cyber basics, Australian organisations today are more vulnerable than ever to a cyber incident."

Security in Depth surveyed 722 organisations across Australia, each with 50 or more staff members. While most (71 per cent) had a business continuity plan, and a cyber security strategy (57 per cent) and roadmap (56 per cent) less than half (44 per cent) had any kind of cyber security governance structure. Fewer still (30 per cent) had a response plan in case of a cyber incident.

A quarter reported having ‘none of the above’.

The unnamed CEO was clearly wrong when he told Connory that a cyber attack or data breach was like a house fire, that is: “highly unlikely an event will actually occur”.

The number of data breaches is rising, with 305 reported to the Office of the Australian Information Commissioner (OAIC) since February.

READ MORE
Branches, call centres remain part of CBA’s ‘digital leading’ future

Earlier this year Jetstar, the Tasmanian Government, Telstra, Australia Post, Commonwealth Bank and scores more suspended their use of software-as-a-service provider PageUp following a possible data breach that took place in May.

Worldwide, attacks against businesses have almost doubled in five years, according to the World Economic Forum. So why aren’t executives and boards responding to the rising threats?

Priorities

It’s down to competing priorities and security teams that lack a strategy, says Connory.

READ MORE
Why more CEOs will be fired after a cyberattack

“Executives are focused on so many other parts of the business that cyber still falls way behind in priorities,” says Connory.

“Asked what would limit their ability to reach goals, regulatory requirements came up a strong first, followed by reputational issues, even supply chain requirements had higher visibility on executives agendas than cyber," he adds.

"You take into account other issues such as retaining talent, regulatory requirements, competition, innovation, customer demands...

it becomes quite clear why executives perform poorly when cyber is raised."

Another issue is that ICT teams typically lack security knowledge and struggle to influence the ways employees work at an organisation.

READ MORE
AustCyber: Time to 'harmonise' bamboozling government cyber advice

“Executives expect and pay their ICT teams to manage these, they trust these teams and expect it to be done," Connory says.

“Those teams tend to focus on the technology more than governance and almost always are tactical rather than strategic. Let’s patch better, let’s get a more up to date firewall, improved malware protection. They also do not generally have access to structuring how employees should conduct business on a day to day level.”

Some 85 per cent of companies surveyed by SID said they did not have dedicated security staff. While 100 per cent of teams had implemented antivirus software, 92 per cent had implemented firewalls and 28 per cent anti-spam and phishing solutions; a third had not completed any penetration testing on their systems, and few gave staff training on cyber hygiene.

There is also a lack of influence and effective communication from ICT teams to the wider business. And if they are successful at implementing company-wide initiatives, it may not get executive buy-in.

READ MORE
The Missing Link strengthens focus on industrial cyber security

Connory recalls a CISO within a health organisation who created a new rule disabling USB ports across a site.

“It was agreed at an executive level and was communicated to all staff and external consultants. Two days later a surgeon was preparing for surgery and had brought in a USB device with X-rays on it. Of course it wouldn't load and the surgeon made two phone calls and within an hour USB devices were allowed again – never to be turned off," he says.

Human error

According to the OAIC, human error is the second most common cause among the data breaches reported to them during the second quarter of this year. Human error – be it clicking on a link in a dodgy email or falling for a phishing scam – is cited as one of the leading security vulnerabilities in numerous reports.

READ MORE
First CEO and refreshed board at RegTech Association

Despite this, nearly half of the Australian businesses surveyed (48 per cent) provide no training whatsoever to staff about cyber security. Six per cent do, "but only where mandated by law or regulation".

The finding that 36 per cent of companies do provide "through general training" information about cyber security, isn't reassuring, says Connory.

"If we take out the large organisations – multinationals etc – then the number does increase dramatically. You take out organisations who spend ten or twenty minutes training staff on web usage and company policy on email usage then the number jumps up again," he says.

Most of the training can be described as the "bare minimum", Connory says.

"Our concern is that these programs do not show or teach individuals how to spot a phishing email, what to do if they receive a phishing email – and that's just one aspect of the training," he says.

Effective training can cost as little as $20 per person and take place over a lunchtime with measurable results, Connory adds.

FOLLOW US

JOIN THE NEWSLETTER!

Email address

Join

Or

Sign in with LinkedIn

Sign in with Facebook

Sign up to gain exclusive access to email subscriptions, event invitations, competitions, giveaways, and much more.

Membership is free, and your security and privacy remain protected. View our privacy policy before signing up.

Tags CISO governance compliance regulation training human error cybersecurity secure cyber Security in Depth Michael Connory CIO hygiene

READ NEXT

RXP Services wins $6.8M deal with Vic Health and Human Services

Customer demands form around hybrid, yet shift around open source

Inside the experience economy: what's the partner play?

0 Comments

FOLLOW US

DISTRIBUTOR DIRECTORY

YOUR ESSENTIAL GUIDE TO AUSTRALIAN DISTRIBUTORS

AQUION

Search distributors

FIND DISTRIBUTORS BY NAME - VENDOR - LOCATION

VENDOR DIRECTORY

YOUR ESSENTIAL GUIDE TO AUSTRALIAN VENDORS

paloalto NETWORKS

Search vendors

FIND VENDORS BY NAME - CATEGORY

MICROSITES

Microsoft **From desktop to web and everything in between, Microsoft Office delivers the help you need to work anytime, anywhere. Pick the Office that's right for you.**

APC by Schneider Electric **Take advantage of oppportunities IoT creates for micro data centers at the edge**

SLIDESHOWS

Inside the experience economy: what's the partner play?

ARN Platinum Club celebrates leading partners and start-ups in 2018

Innovation in Australia: which technologies will take over the nation?

Latest Jobs

Infrastructure Architect

Hays Information Technology
Sydney NSW
Read more

Information Architect

Hays Information Technology
Brisbane QLD
Read more

Level 2/3 Support - Managed Service Provider

MPAU Technology
Sydney NSW
Read more

POWERED BY

Post a Job

View all jobs

RELATED WHITEPAPERS

Managing Technicians in an MSP Business for Profitability

Vodafone NZ goes large on tech security in Telstra deal

There's a large new security play brewing as Vodafone NZ teams up with Telstra