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

8

0 Comments

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

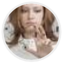
"Implementing these [cyber awareness and governance] programs is like home insurance – high cost with no guarantee anything will ever happen – so why pay the price? How many houses burn down every year, compared to how many people buy house insurance?"

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. 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," Connory says.

Editor's Recommendations

Why CIO tenures in Australia are getting shorter


Australian companies suck at data analytics

Ice Bucket Challenge co-founder gets his voice back

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.

CIO Executive Council member profile: Geoff Quattromani, Asia Pacific business analyst, data and analytics, Johnson & Johnson

More from CIO Executive Council »

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. 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?

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

Priorities

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

"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. 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," he adds.

READ MORE
Why more CEOs will be fired after a cyberattack

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

"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.

What happened to Facebook's 'revenge porn' prevention pilot?

Facebook privacy scandal widens as data leak hits 87 million users

CIO roundtable: How tech chiefs are overcoming digital transformation hurdles

Tweets by @CIO_Australia

CIO Australia
@CIO_Australia

Spotlight on Alibaba CEO Zhang as Jack Ma starts retirement countdown cio.com.au/article/646519…

Spotlight on Alibaba CEO Zhang as Jack…
Unlike his charismatic boss, Alibaba CEO Da…
cio.com.au

Embed View on Twitter

Web Events

CIO Live Webinar - Future of Work: How to meet the demand of digital

How to create a new, more agile digital workspace

CIO & Computerworld Live Webinar | Why cyber resilience is your best defence

Read more

Latest Jobs

IT Service Desk Analyst
MPAU Technology
Sydney NSW 2009

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
AustCyber: Time to 'harmonise' bamboozling government cyber advice

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.

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.

Join the CIO Australia group on LinkedIn. The group is open to CIOs, IT Directors, COOs, CTOs and senior IT managers.

Related Whitepapers

CHOOSING THE RIGHT UC FOR YOUR BUSINESS

Customer Case Study: CEREBRAL PALSY ALLIANCE’S DIGITAL TRANSFORMATION

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

More about Australia Australia Post Commonwealth Bank PageUp Tasmanian Government

0 Comments

Read next

NSW birth certificates, property titles and motor rego headed for the blockchain

Data breach hits British Airways; 380,000 payments affected

The anthropologist asking critical questions around AI
CIO New Zealand

Updated: In pictures: CIO Networking Dinner: ANZ CIO Forum on 'Make it ...

In pictures: Securing customer data: Are you prepared for an attack? - ...

Why is a digital strategy so important?

Agile methodology for IT delivery doesn't have a place in strategic planning says Dr Malcolm Thatcher

1. The week in security: Poor security habits perpetuate poor security defences
2. Users' poor home IoT security could become your next headache
3. Cisco swats dangerous Struts flaw, and two more critical bugs
4. Business email compromise fraud is growing faster than your profits are
5. Eight years on, half of Australian companies still haven't implemented ASD's Top 4 mitigations

1. Microsoft pushes machine learning to the edge
2. Tech companies issue warning over government's surveillance bill
3. Firefox calls it quits on antiquated Windows XP, Vista
4. A new phone-like device from Redmond? Why, Microsoft, why?
5. NSW digital licence rollout driven by blockchain

1. Cloudera appoints Tech Data as first A/NZ distributor
2. Ingram Micro taps JB Hi-Fi talent in executive swoop
3. Telstra's cyber security leaders exit
4. Cloudera taps Citrix talent to lead A/NZ business
5. EDGE 2018: Employee centricity key to customer centricity

1. New Python app profiler uses Rust for speed and safety
2. Microsoft Azure Devops Services puts devops in the cloud
3. Firefox calls it quits on antiquated Windows XP, Vista
4. A new phone-like device from Redmond? Why, Microsoft, why?
5. Atlassian's tips on embracing open work practices

1. How category design is helping the customer chief at hipages find growth
2. Youi CMO takes back the CEO role
3. Starcom: Amazon Prime Day doesn't trigger Australian growth spurt
4. Juniper Networks brand relaunch: standing out from the crowd
5. The Coffee Club owner appoints its first chief brand officer