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, say 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. It is our view, based on the number of organisations that have failed to implement what we believe are cyber basics,

Editor's Recommendations

Australian organisations today are more vulnerable than ever to a cyber incident," Connory says.

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
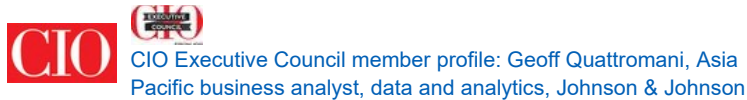
More from CIO Executive Council »

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.
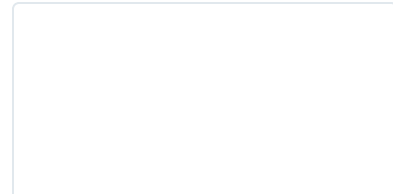

READ MORE
Why more CEOs will be fired after a cyberattack

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

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.

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.
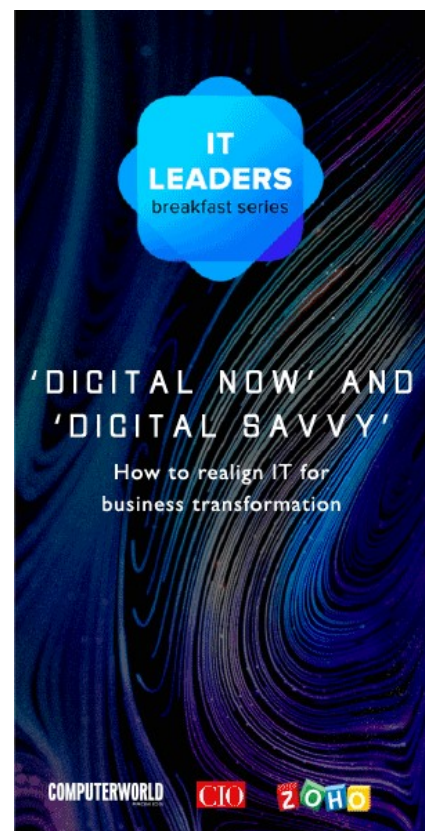
Human error

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.

Related Whitepapers

Customer Case Study: CEREBRAL PALSY ALLIANCE'S DIGITAL TRANSFORMATION

How to Sell Your Cloud Migration Strategy to Your Biggest Critics

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.

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

More about   Australia   Australia Post   Commonwealth Bank   PageUp   Tasmanian Government

0 Comments

Read next

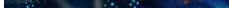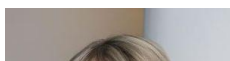**Atlassian exec apologizes to HipChat and Stride users for Slack decision**

The anthropologist asking critical questions around AI
CIO New Zealand

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

'They had hideous girly posters on the wall in the tea room'

Kim Wenn on her 37 years in IT

Byron Connolly (CIO)
13 August, 2018 16:02

0

0 Comments

Kim Wenn recalls her time as a young IT exec computerising manual processes at Australian Paper Manufacturers in Victoria in the 1980s.

"I used to go out to the paper mill in Maryvale and they had these hideous girly posters on the wall in the tea room. They had all of the Repco girly posters, it was hilarious.

"One of the guys that was involved in the program, he must have been a bit more new age than the others and he asked, 'do they bother you?' I said, 'I don't think they bother me as such but they are inappropriate. They were then taken down," says Wenn.

On July 1, Wenn officially retired after spending 37 years in technology industry, the last 12 at Tabcorp as general manager, wagering systems and more recently, chief information officer. Her retirement from the gambling giant coincided with its merger with Tatts Group. Former Tatts CIO Mandy Ross stepped into the CIO role following Wenn's departure.

"The merger with Tabcorp and Tatts meant we had two of everyone and I said to [Tabcorp CEO] David [Attenborough],'I'll work with you to ensure a low risk handover.' And he didn't have to choose between [Mandy] and me and all that sort of ugly stuff.

"The merger was the catalyst and the timing was perfect because my husband had just retired and we were pretty keen to enjoy life a bit more. I've never had a gap year, my kids had gap years, doing all this lovely stuff and travelling around; I never did that so we are doing it now."

Wenn began working in 1981 after finishing high school. Her first job was as a goods receivable clerk in Knoxfield, Victoria at manufacturing company Rosella Lipton. The company was acquired in 1988 by Unilever.

"I annoyed the IT manager so much in the first three months that he said, 'ok, come and work for me.'

"I would walk through the factory at Rosella in Tatura and everybody would look at me like I had three heads. They never saw a female walk through the factory unless they were putting the onion powder in the vat and on the line," she says.

Wenn had a real passion for manufacturing and worked during an era of technology-led automation across the sector. Technology was a family affair; her father had been chief information officer at The Royal Hong Kong Jockey Club.

"It's all a bit odd that I ended up as CIO for Tabcorp. Dad had a big influence on me in terms of me getting into IT.

"Both of those jobs [APM and Rosella Lipton] were fun. I loved manufacturing and it was in the era of automation; you could see what you were doing, automating recipes to make tomato sauce, for instance. You could put in the orders and [the system] would spit out the ingredients whereas previously someone had taken months to calculate it," Wenn says.

During those early days, Wenn attended school at night, completing a Bachelor of Computer Science at Monash University and then a Masters of Management and Technology at The University of Melbourne.

"I was a rare commodity in the computer science degree; I think I was one of about four girls. I've just retired from a male dominated industry and [looking back] I wasn't ever bothered by it; I was lucky because I was pretty resilient," Wenn says.

An early lesson

Web Events

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

vmware   How to create a new, more agile digital workspace

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

Read more

Related Whitepapers

While at APM (now Amcor), Wenn was part of a team that rolled out IBM 'green screen' mainframes across the plant in a vintage digital transformation initiative that didn't consider the cultural impact of computer automation. The tech team wrongly assumed that staff members were literate and could read the screen and enter the correct dimensions for paper weight. Computer literacy levels across the entire plant were so low that the program initially failed.

"There was no training and no recognition that literacy levels of people on the floor in the paper factory [was low]. We spent a couple of years on it, we never withdrew it, we just repositioned people into different roles if they couldn't read [the screen]. There was a whole workforce strategy and replanning exercise that had to go with it," Wenn says.

Wenn then found her wings, spending five years as a computer programmer at life insurance and pensions company Scottish Widows in Edinburgh during the early 1990s at a time when 'tea ladies' were still being employed to wheel the trolley around at 11:00am each working day.

Wenn came back to Australia where she was hired again by APM. It was at this time that she began climbing up the ranks, eventually ending in a different division as general manager, logistics at the company. Between 2000 and 2005, Wenn was vice president, research and development at Quest Software before joining Tabcorp, initially as GM, wagering systems before being elevated to CIO in May 2009.

Wenn is adamant that she has been lucky enough during her career to identify industries that were set to be transformed through technology; she saw 'the art of the possible' and wanted to be a part of it.

"It [her move to Tabcorp] had nothing to do with Dad or my knowledge of the industry. In 2000, it was the early days of the internet and a change in how consumers interacted with [gambling] products and I just thought it was going to be an industry that would go through a lot of transformation. It would be fun to be part of that whole change from men walking into a betting shop to women [betting] on their phones."

Tabcorp is now one of Australia's largest technology companies. Its core competency is technology, betting is simply how it makes money, she says.

Biggest career mistake

When pressed about her biggest mistake over the past 37 years, Wenn says persevering with an outsourcing arrangement at one stage had ended in disaster.

"My predecessor outsourced most of the IT function," she says. "You can't take a bunch of Indians in another country with a cultural difference and a language gap and get them to deliver your products. And betting is illegal in India. It was a total disaster and I spent years clawing it all back over here.

"Someone else had outsourced it and I spent a lot of time trying to make it work ... we should have gone faster and brought it back straight away. Outsourcing has a place depending on what you are doing, if it's routine stuff, I think it has a place."

Tech sector doing a 'shit job'

Wenn doesn't mince her words when asked about the tech sector's ability to promote IT careers to young people, particularly women.

"I think it does a shit job to be honest. I think there is no sales and marketing engine. A lot of people still refer to technology as ICT which is just a barrier to entry.

"I think the whole integration of technology into schools comes up short … there's still a lot of work that needs to be done. There are pockets of great activity … being driven mainly by women but there's no consolidated approach from the government or education [sector].

"We are our own worst enemies."

She agrees that despite ongoing rhetoric, the government has lost its way when it comes to creating an 'innovation nation.' Investing in and supporting start-ups alone is not going to solve the problem, she says.

"They [kids] are going to grow up and find that the education system is lacking in terms of its support for technology."

Last year while still at Tabcorp, Wenn conducted a survey with 1,000 female year 10 students and their parents. A key finding was that girls would only consider doing a STEM-related degree if their parents or someone else in the family such as an aunt was already involved in the sector.

"Even worse, those girls that didn't have any direct contact [with people in IT] were actively discouraged by their parents. A young woman could be a user experience designer, project manager, business analyst or architect – anything in IT – and still have a family. The whole culture around technology and flexible working is just perfect but a lot of people don't understand what they can do."

Wenn believes that in the workforce of the future, there is barely going to be a role that doesn't involve technology.

"Marketing, it's all search engine optimisation and Google Analytics, it's not colouring in and posters that you print. Roles are changing and if we look at the

workforce of the future, 70 per cent of the roles will be at least technology-based and we are not preparing the kids for it," she says.

"I think there's less than 25 per cent female participating in STEM degrees so how are we ever going to have a diverse workforce with that level of participation."

Her final message for female computer science graduates?

"Be brave, work hard and you can have an amazing career. You can raise a family and do anything that you want."

Follow CIO Australia on Twitter and Like us on Facebook… Twitter: @CIO_Australia, Facebook: CIO Australia, or take part in the CIO conversation on LinkedIn: CIO Australia

Follow Byron Connolly on Twitter: @ByronConnolly

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

More from CIO Executive Council »

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

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   Monash University   Melbourne University   TabCorp   Kim Wenn

Unilever   Mandy Ross   The Royal Hong Kong Jockey Club

Australian Paper Manufacturers   Rosella Lipton

More about   Amcor   APM   Australia   Australian Paper   Facebook

Google   IBM   Monash University   Quest   Quest Software   Repco

Technology   Twitter   Unilever   University of Melbourne

0 Comments

Read next

'They had hideous girly posters on the wall in the tea room'

Atlassian exec apologizes to HipChat and Stride users for Slack decision

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? - ...

AI to become next Australian Prime Minister?

Research shows some Australians believe AI would make better decisions than elected government representatives

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

1. Atlassian's tips on embracing open work practices
2. What is a smart city? How to define a smart city
3. Alibaba's Jack Ma prepares to unveil succession plan
4. Microsoft plans to sell post-2020 support for Windows 7
5. How to make an old Android phone feel new again

1. Telstra's cyber security leaders exit
2. Cloudera taps Citrix talent to lead A/NZ business
3. EDGE 2018: Employee centricity key to customer centricity
4. Mobility spending expected to hit $1.8T by 2022
5. Google appoints new trans-Tasman leader

1. Atlassian's tips on embracing open work practices
2. What is a smart city? How to define a smart city
3. Microsoft plans to sell post-2020 support for Windows 7
4. Social media and trolls: The end is near
5. Breakthrough: Python reaches Tiobe index Top 3

1. Starcom: Amazon Prime Day doesn't trigger Australian growth spurt
2. Juniper Networks brand relaunch: standing out from the crowd
3. The Coffee Club owner appoints its first chief brand officer
4. ASX-listed GrowthOps appoints inaugural CMO
5. Aussie on the hunt for chief digital officer

5. Watch out for fake MDM
   and 'age restriction' attacks
   on iPhones