Data sharing practices in Australia are 'appalling': report

It's hard to understand the attitude and level of naivety, says Michael Connory

Samira Sarraf (CIO)
25 November, 2019 12:32

Credit: ID 73611677 © Weerapat Kiatdumrong | Dreamstime.com

Australian companies are failing to conduct formal reviews on the practices of companies they share data with, according to a study by Security in Depth.

The majority (84 per cent) of local companies surveyed for Security in Depth's *2019 State of Cyber Security* research said they had not completed these reviews, which was described in the latest report as "appalling."

More than half (59 per cent) of all companies surveyed for the report said they had experienced a third-party breach during the last 12 months, a three per cent increase on the previous year.

“With so much at stake, it’s hard to understand the attitude, or the level of naivety, even though our lives are governed by what we do daily in the cyber world," Security In Depth CEO Michael Connory said told *CIO Australia*.

"Australians seem content to remain as bystanders rather than be their own active security force. It’s simply a crazy attitude adopted."

Organisations have increased the number of dedicated IT security staff within departments, with that number increasing by 47 per cent compared to the previous year.

"It has become evident that over the past twelve months, many organisations have elected to have a dedicated department focusing on cyber security," the report said.

One of the greatest challenges of CIOs and CISOs is the ability to implement a strategic framework that can be executed effectively. According to the report, 88 per cent of CISOs focus on day-to-day tactical requirements of the business rather than being able to implement a strategic vision across the organisation.

Securing an organisation’s infrastructure has become one of the more stressful jobs with 92 per cent of CISOs saying they are not able to switch off work and 20 per cent stating to suffer burnouts. Also, 71 per cent claimed they do not have the people to support the job that is required.


READ MORE
ANZ, CBA call for better threat intelligence sharing

Meanwhile, less than 30 per cent of respondents said their network is sufficiently secure and 11 per cent claiming it to be highly secure.

Security in Depth believes one in four companies conduct penetration testing. More than 35 per cent of organisations have reported they do not provide cyber security awareness training, all other organisations provide some kind of training.

"More organisations are conducting cyber awareness training this year than last year. We have seen a significant improvement in the number of organisations who have adopted with an overall jump by approximately 10 per cent - which translates to an estimated extra 3500 organisations recognising the need for training and implementing a training program," the report said.

Other findings


READ MORE
IT leaders share top line predictions for 2020

There has also been an increase in the number of organisations with a dedicated department focusing solely on cyber security which has grown 1400 per cent in the past 12 months.

One of the findings in the report is the reasons behind cyber attacks. The report focus in five categories: financial; espionage; fun; grudge and other. The government sector had the highest rate of cyber attacks motivated by espionage and the least for financial benefit. The education, technology, manufacturing, professional services, retail, health, and the finance sectors all had high rates of financially-motivated cyber attacks. Both health and education suffered cyber attacks doen for "fun", the report said.

70%

Editor's Recommendations


AI judges readied for Tokyo 2020 gymnastics competitions


Lessons learned from a transformation: Bankwest


Does your company need an AI ethics committee?


How CIOs can prepare for a new world of open data


Mind your metaphors: Why CIOs’ choice of corporate jargon counts


Why CIO tenures in Australia are getting shorter

Tweets by @CIO_Australia

CIO Australia
@CIO_Australia

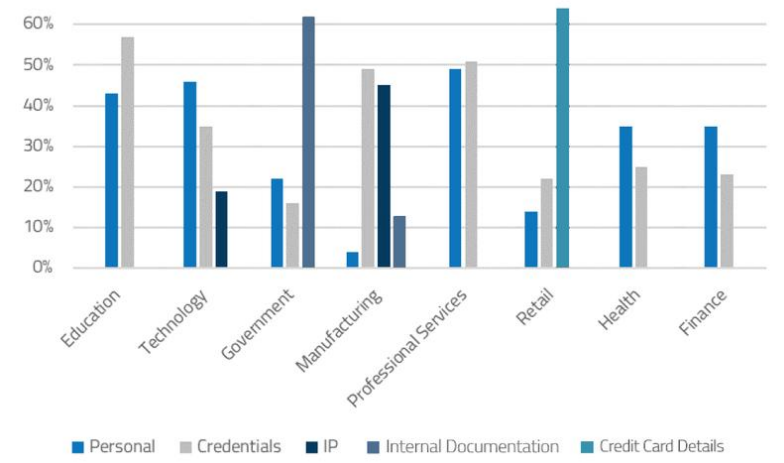
iiNet warned after leaving customer with no internet access for three weeks cio.com.au/article/669062…

iiNet warned after leaving customer with n…
iiNet will conduct an independent audit of its …

Embed View on Twitter

Read more

NTT Data Zone



Credit: Security in Depth

2019 State of Cyber Security, Security in Depth

The report found that 1.5 per cent of organisations made no investment in cyber in the past 12 months.

READ MORE
American CIO counterparts 'play never-ending game of catch-up': survey

"This is also reflected in a significant spike in organisations investing up to 10 per cent of their annual IT budget in cyber from 53 per cent to almost 75 per cent," the report said.

"The challenge we see across the spectrum is how organisations are allocating funds – Security In Depth is finding more often than not, the decision has become more tactical to try and cover specific challenges requiring immediate attention, an example being requests for security information and maturity from the supply chain, and organisations implementing activities like training, penetration testing or improved technology such as malware solutions. Security in Depth would like to see organisations initially improve the strategic component of cyber security and start with a solid governance framework," the report said.

The report noted that about 40 per cent of organisations still have cyber security falling under the banner of IT, and 40 per cent reporting to either the CEO, CFO or directly to the board in certain circumstances.

"We infer, many of the challenges with data breaches and in particular human error, relate to a reporting line to IT. The challenge here is, IT has no real control or impact on people across the organisation and as such, the ability to change individual behaviour, is almost non-existent. Those organisations who have removed cyber risk from their IT operations, have seen significant changes in user behaviour resulting in a more mature, resilient and risk averse organisation," the report said.

A total of 1894 organisations employing between 20 and over 50,000 people were surveyed. The organisations are spread across all 14 major industries with all Australian finance organisations contributing to 27 per cent of all respondents, technology organisations 17 per cent and health organisations 16 per cent.

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

Latest Jobs

IT Specialist Traineeship
TABMA Apprentices and Trainees
Brookvale NSW 2100
Read more

Database Administrator
Glen Huntly VIC 3163
Read more

COMPUTER SYSTEM & NETWORK ENGINEER
Sydney NSW 2000
Read more

POWERED BY Post a Job
View all jobs

Related Whitepapers

The Expert Guide to VMware Data Protection and Disaster Recovery

CSO Security Buyers Guide 2017

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 report data breach CIO security

More about Australia

0 Comments

Read next

Monash University names Teresa Finlayson as its permanent CIO

Data sharing practices in Australia are 'appalling': report

CIO50 2019: #25 Bradley Blyth, flybuys

In pictures: CIO50 2019 launch dinner

Equinix opens largest Australian data centre, SY5

Watson IoT chief: AI can broaden IoT services

IBM's Kareem Yusuf talks smart maintenance systems, workforce expertise and some IoT use cases you might not have thought of

1. Global threat groups pose new political and economic dangers
2. The week in security: Australian industries vulnerable to hacking: "We are all Ukraine"
3. A new era of cyber warfare: Russia's Sandworm shows "we are all Ukraine" on the internet
4. Sustained attacks on Australian education reflect data's continued vulnerability
5. Google matches Apple's iOS bug bounty: will pay up $1.5m for a really tough Android Pixel hack

1. Food fight: Slack and Microsoft trade barbs, sling stats in collaboration app battle
2. DTA plans whole-of-government 'telco marketplace'
3. Westpac to close funds transfer platform LitePay
4. Why Cenitex turned to HCI, VMware Cloud on AWS for 'Program Fortify'
5. Roadshow, Netflix seek to block open source Popcorn Time app

1. Qualtrics appoints former Salesforce VP to lead regional growth
2. IBM urges review of Australia's anti-encryption laws
3. Govt calls on providers to fill new telco marketplace
4. ARN Women in ICT Awards 2019: and the winners are…
5. 5G Networks launches partner program under new channel chief

1. Food fight: Slack and Microsoft trade barbs, sling stats in collaboration app battle
2. GraalVM adds Java 11 support
3. Microsoft goes very small for Windows 10 1909's 'On' switch
4. Blackberry refreshes its UEM suite, focuses on zero-trust access
5. SAP user community focuses on move to S4/HANA

1. The B2C and B2B marketing transformation helping Invisalign win more smiles
2. V Energy launches new ANZ brand platform with distraction message
3. AuMake appoints new executive-level marketing leader
4. How a fashion brand has cast a spell over customer experience
5. Salesforce CMO: Modern marketers have an obligation to give customers control of their data

Send Us E-mail - Privacy Policy [Updated 13 Sep 19] - Advertising - CSO - Subscribe to emails - IDG registered user login - Subscribe to IDG Publications - Contact Us

IDG Sites: PC World - GoodGearGuide - Computerworld - CMO - CSO - Techworld - ARN - CIO Executive Council