Software companies keep making these same cyber security mistakes

Cyber Assurance Risk Rating (CARR) has exposed gleaming flaws in the way that corporates operate and manage data protection.

Michael Connory (CIO)
29 April, 2019 14:32

Albert Einstein once defined insanity as doing the same thing over and over again and expecting different results. This is exactly the way corporate organisations in Australia are approaching how they manage and protect their data.

Our organisations, either through lack of education or information, have the view that investing large amounts of money into technology and ignoring the imperative role humans play will protect them against data breaches and attacks – a mistake they consistently make.

And yet it took a once little-known but now world leading Australian cybersecurity scoring initiative known as CARR (Cyber Assurance Risk Rating) to expose the gleaming flaws that repeatedly exist within how corporates – software companies in particular – operate and manage data protection.

rough the implementation of the CARR program, organisations are now arting to ensure each company they share information with has cyber

Scroll down to read: Dominos serves up a slice of tech innovation

processes to protect the data shared. This has helped uncover a number of flaws in the way organisations are approaching this issue.

Firstly, CARR discovered that only 27 per cent of Australian software companies have dedicated certified security specialists employed to manage and implement cyber security best practices.

This reflects a lack of serious security expertise that exposes the challenge of creating software that is designed to cut organisational costs and enable individuals to be more productive without understanding the consequences of how someone might use the application to access confidential information.

Secondly, 38 per cent of these organisations implement 'security by design' into their software development lifecycles practices. Most of the applications currently developed may fulfil business objectives but not always measure up to security standards. This means that the applications we use daily are vulnerable to a cyber incident. The ability to incorporate 'security by design' is more prevalent for smaller software companies due to increasing costs.

Meanwhile, only 52 per cent of Australian software developers have implemented a secure infosec foundation such as COBIT5, NIST or ISO 27001 as a basis for their organisation and program.

Upon examining the ease to socially engineer a hack on a software company, only 13 per cent of organisations reviewed were capable of understanding how to respond to a request for information based on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 – or the encryption bill.


READ MORE
Darknet market bundling card details with device fingerprints to beat fraud detection

Finally, when organisations were asked how they respond to a technical assistance request from an agency such as ASIO, 87 per cent said they would not know how to do so. Further, 11 per cent said they would need to obtain advice from outside council.

Imagine this scenario. A staff member of an Australian software company could be approached by a person claiming to be from ASIO. This individual could advise an employee or a contractor that under current law, they have a technical assistance notice. The scammer then asks for the individual's assistance to spy on someone else.

This requires no paperwork and the person representing ASIO could simply present actual legislation to support this requirement with a threat of five years prisonment if that individual communicates this to another party.

Scroll down to read: **Dominos serves up a slice of tech innovation**

Editor's Recommendations

Share


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


Australian companies suck at data analytics


Ice Bucket Challenge co-founder gets his voice back

This legislation leaves the door open for anyone keen to gain easy access to confidential information, through socially engineering the legislation and individuals to access confidential information on another individual.

READ MORE
ASIO seeks Microsoft Azure partner for large-scale IT transformation

The technical assistance notice could include:

- Decrypting communications where a DCP already has the ability to do so
- Installing agency software of the DCP's network.
- Modifying the characteristics of a service or substituting a service provided by the DCP.
- Facilitating access to the relevant facility/equipment/device or service
- Handing over technical information such as source code, network or service design plans, and the details of third party providers contributing to the delivery of a communications service, the configuration settings of network equipment and encryption schemes.
- Concealing the fact that agencies have undertaken a covert operation.

Few organisations understand the legislation and fewer individuals understand their legal rights, which begs the question: What would you do if an individual claiming to be from ASIO advised of an imminent terrorist threat and had to help implement a piece of spyware immediately? If you failed to help or communicated this information to another party, you would be prosecuted and potentially receive five years imprisonment.

Australian technology companies in general have a long way to go on the cyber security front. Smaller companies, in particular, are finding it hard to manage the complexity of cyber security with the increased costs of expert staff.

READ MORE
Budget 2019-20: Defence CIO Group costs to hit $1.7B

The CARR process and the ability of all organisations to now review and understand the practices of the companies they are sharing critical information will help businesses understand the different risks around sharing information.

What's certainly now true is that all organisations need to improve practices around sharing their information. They can no longer walk away from their obligations, the risks are just too high.

Michael Connory is the CEO of Security In-Depth.

Read more: Government's $156M cybersecurity pledge a "drop in the bucket": White hat hacker

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

Tags cyber security ASIO Albert Einstein

re about ASIO Assurance Australia Bill ISO

Scroll down to read: **Dominos serves up a slice of tech innovation**

Read next

Dominos serves up a slice of tech innovation

Finance CIOs must review security controls now

Don't become addicted to cybersecurity gambling
CSO Online

In pictures: Grappling with ERP: Are rising costs stifling innovation - Melbourne ...

In pictures: Digital workplace: If we build it, will they come? - ...

Dominos serves up a slice of tech innovation

Michael Gillespie discusses the impact of technology on the franchised pizza retail chain

1. The week in security: BEC, scams netting billions for cybercrims
2. McAfee: Watch out for LockerGoga, a ransomware in the making
3. Mystery data breach reportedly exposes 80 million names, addresses, ncome info
to evaluate SOC-as-a-ce providers

1. Class action targets Vocus
2. Brave browser debuts working BATs-for-ads concept
3. South Australia rolls out locked-down desktop for prisoner education
4. Popularity of cryptocurrencies among scammers grows

1. Datacom brings hybrid cloud to North Queensland businesses
2. Ixup expands channel reach with new partnerships
3. Vocus served with class action
4. Government's $156M cybersecurity pledge a 'drop in the bucket': White hat hacker

1. Cisco goes all in on WiFi 6
2. JDK proposal takes aim at verbose Java syntax
3. Venerable Cisco Catalyst 6000 switches ousted by new Catalyst 9600
4. Brave browser debuts working BATs-for-ads concept
5. Slack partners with Zoom to boost video capabilities

1. Ricoh: B2B CX needs to model B2C
2. Former Telstra and IBM marketer joins KPMG
3. Fresh Stikeez campaign drives Coles revenue growth
4. How Accolade Wines lifted its email marketing success
5. Kennedy returns to Cotton On

Scroll down to read: **Dominos serves up a slice of tech innovation**

5. The blame game in security needs to stop
5. Business leaders don't care about the cost of downtime
5. New Relic adds 40 staff to its Australian team

Software companies keep making these same cyber security mistakes

Share

Send Us E-mail - Privacy Policy [Updated 16 May 18] - Advertising - CSO - Subscribe to emails - IDG registered user login - Subscribe to IDG Publications - Contact Us

Scroll down to read: **Dominos serves up a slice of tech innovation**