

Between hope and possible

OPINION: Human factor weak link in health data security

Privacy not a game of poker for corporates to play, says Security in Depth's Michael Connory

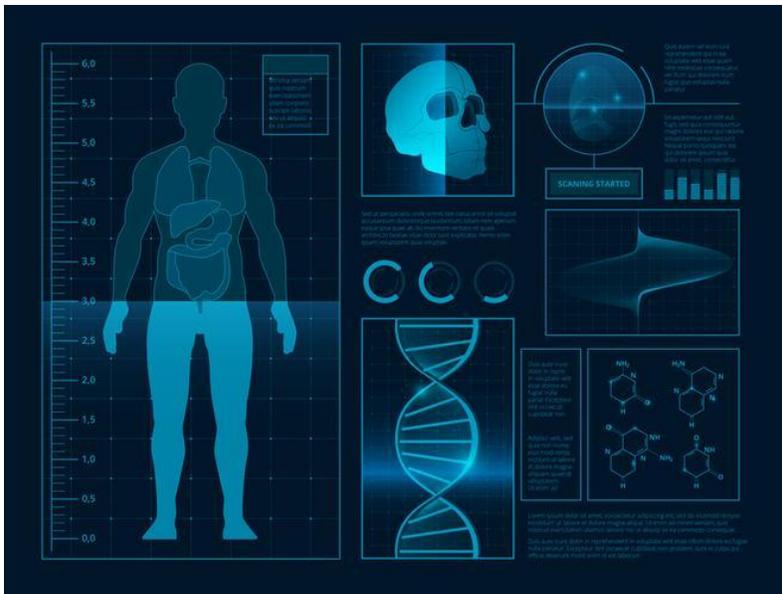


Michael Connory (CIO)
12 December, 2018 10:50

0



0 Comments



[If you can imagine it, we will build a bridge to get you there.](#)

Watch now



Editor's Recommendations

Crystal ball gazing is an art usually left to mediums and psychics who profit off the hope of the true believers.

It's the ability to sell a belief that makes what a medium has to say an interesting story, and yet, there is something to be said about forecasting events with credibility and foresight while armed with the right information.

Being an oracle is more convincing when the story told is a message of intellectual rationality and indisputable fact.

Data breaches, cyber threats and attacks, have dominated media headlines throughout 2018 – a growing trend has emerged. The country is a weakened fortress where the walls of strength should have been buttressed with the right armoury. But our defensive guard is in a shambolic state; a problem for Australians.

- Why CIO tenures in Australia are getting shorter
- Australian companies suck at data analytics
- Ice Bucket Challenge co-founder gets his voice back
- 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

Australia is staring down a dark hole and – if it does nothing to address what has become a tipping point towards disaster and falls into it – it may never scale the walls back to freedom.

OPINION: Human factor weak link in health data security



BRANDPOST

Getting a handle on your data to gain insights and drive competitive advantage

More from Information Builders »

As a country, we are in a crisis of security failings – 2018 proved corporate Australia refused to understand the importance of safeguarding our privacy – setting up 2019 to be a year where record privacy breaches reach a zenith and the courts and lawyers will become the casino and croupiers. Australians' privacy is not a game of poker for corporates to gamble with.

Our health sector is the largest employer of Australians, employing more than 15.7 per cent of the workforce. This year, some 20 per cent of all known data breaches have come from the health sector – the biggest and most targeted of all sectors.

The attacks will grow to 23 per cent come 2019 because:

- 65 per cent of all health employee's have never undergone cyber awareness training – troubling considering 70 per cent of all data breaches relate to human error
- 82 per cent of health organisations do not have a dedicated individual or group focusing on security
- 79 per cent of health organisations do not have a fully prepared and tested incident response plan in case of a cyber incident
- 91 per cent of health organisations have never reviewed security policies and practices of a third party they share data with
- Staff across the health sector, who have been with an organisation longer than 18 months, have a 31 per cent chance their credentials have already been compromised.



READ MORE

[Clues in Marriott hack implicate China: sources](#)

Playing the role of oracle sees Security in Depth's research team predicting 2019 will be a year of high drama for the health sector as an increase in cyber risks will impact the sector directly where major attacks will come via:

- Improved Ransomware attacks
 - Cyber criminals are now researching systems ahead of time, often through backdoor access, enabling them to encrypt their ransomware against the specific antivirus applications put in place to detect it.
 - Healthcare systems are prime candidates for targeted attacks, since they handle sensitive data from large swathes of the population.
- Improved and targeted phishing attacks
- Improved business email compromise attacks

Attacks are likely to target individual devices as well as cloud-based systems where the primary objective will be to access user credentials.

No matter how much cybersecurity improves, the weak link in the armoury of defence remains the human factor. Strengthening the link requires an investment in training where corporate Australia must focus its strategic counsel.



Tweets by @CIO_Australia



CIO Australia
@CIO_Australia

Huawei CFO seeks bail on health concerns; Canada wants her in jail [cio.com.au/article/650633...](#)



Huawei CFO seeks bail on health concern...
A top executive of Huawei argued that she sh...
[cio.com.au](#)

[Embed](#)

[View on Twitter](#)

Web Events



CIO Executive Council WebEvent |
Enterprise Agility – Facilitation,
Integration and Enablement



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



How to create a new, more agile digital
workspace

Read more



NTT Data Zone



OPINION Human factor weak link in health data security
Aussie cyber co's get \$4M boost from AustCyber

Enormous volumes of data are shared between a variety of health professionals – factor in most health organisations aren't hospitals – the recipe for major security issues escalate exponentially by [Avogadro's number](#).

When protected health information (PHI) is stolen, attackers are able to steal identities and gain access to medical information, which is used to sell or obtain prescriptions to be traded or sold. In 2019, Australia will witness an increase in cyber extortion – where cyber criminals will use the health records of Australians to extort money directly from citizens.

The threat of cyber extortion looms as a real danger and requires the need for a strategy to deal with the problem to be an integrated play factored into the Australian Digital Health Strategy. The strategic digital health priorities lead to a potential cacophony of citizen complaints as

- Every health care provider can communicate with their patients and other health care providers



READ MORE
[How DiData and Telstra are dealing with the tech skills crisis](#)

- All prescribers and pharmacists have access to electronic prescribing and dispensing by 2022
- Maximum use is made of digital technology to improve accessibility, quality, safety, and efficiency of care
- All health care professionals can confidently and efficiently use digital health technologies

Which means potentially more than a million individuals may have access to Australian citizen health records.

More often than not, answers to the problems we seek are in sight of all we can see, and yet, we can be blinded by the complexities, seeking a solution in all the wrong places.

Michael Connory is CEO and Founder of Security In Depth

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

Tags [privacy](#) [Healthcare](#) [health](#) [cyber](#) [Security in Depth](#) [Michael Connory](#) [security](#)
[data](#)
[More about](#) [Australia](#)

0 Comments

Share ▾

[If you can imagine it, we will build a bridge to get you there.](#)

Watch now

[The bridge to possible](#)



Latest Jobs

Technical Solutions-Senior Specialist

Telstra
Melbourne VIC
[Read more](#)

Digital Account Manager

s2m Digital
Sydney NSW
[Read more](#)

IT Manager

MPAU Technology
Melbourne Region VIC
[Read more](#)

POWERED BY

[Post a Job](#)

[View all jobs](#)

Related Whitepapers



[Only Adobe Acrobat](#)



[Acrobat DC security overview](#)

If you can imagine it, we will build a bridge to get you there.

Watch now

The bridge to possible



Read next



Teachers Mutual Bank welcomes new CIO



Huawei CFO seeks bail on health concerns; Canada wants her in jail



How to Tell if Your System Has Been Cryptojacked
CSO Online



In pictures: CIO Executive Council Pathways graduation



In pictures: Turning insight into action - and your competitive edge - ...

Between hope and possible

CIO50 2018 #9: Jeremy Hubbard, UBank

- 1. The evolving threat landscape – What to look out for in 2019
- 2. Supermicro third-party motherboard audit finds no spy chips
- 3. Google+ leak affects 52 million users and G Suite users
- 4. Microsoft's big Windows Defender ATP update: bad macros, fileless malware and faster response
- 5. Singapore's central bank launches S\$30 million
- 1. Telstra unveils new tech support service for small businesses
- 2. Super Micro says review found no malicious chips in motherboards
- 3. Competition watchdog prepares for new ruling on Telstra wholesale prices
- 4. Dense Air plans to offer small cell 5G services in Australia
- 5. ACCC prepares to gather more NBN data from telcos
- 1. Telstra announces premium ICT channel for small business customers
- 2. Cohesity appoints Nexion as cloud service provider
- 3. Telstra extends Vita Group master licence for one extra year
- 4. Design Industries partners with Alibaba Cloud
- 5. Canadian court grants bail to Huawei CFO
- 1. Microsoft Teams gains ground on Slack
- 2. Review: 4 wireless chargers for both smartphone and watch
- 3. How to tame enterprise communications services
- 4. Using a password manager: 7 pros and cons
- 5. With Google Chromium move, Microsoft raises white flag in browser war
- 1. Report: Reputation commands a price premium
- 2. Rakuten Marketing CEO: Knowing your audience three-dimensionally is the holy grail
- 3. How a real-time customer feedback loop is helping OFX gain agility
- 4. Media and marketing industry applaud the ACCC's wide-reaching digital platform report
- 5. Report: Voice commerce represents vast untapped market for Australian brands

[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](#)

Copyright 2018 IDG Communications. ABN 14 001 592 650. All rights reserved. Reproduction in whole or in part in any form or medium without express written permission of IDG Communications is prohibited.



IDG Sites: [PC World](#) - [GoodGearGuide](#) - [Computenworld](#) - [CMO](#) - [CSO](#) - [Techworld](#) - [ARN](#) - [CIO Executive Council](#) - [IDG Education](#) - [IDG Government](#) - [IDG Health](#)