The Australian
Tuesday 20/02/2018

Page:	25
Section:	IT Today
Region:	Australia, AU
Circulation:	94448
Type:	National
Size:	284.00 sq.cms.

press clip

slice
CUT STRAIGHT TO YOUR NEWS

Breach victims have themselves to blame

TOM KEMP

A consumer ratings agency, a cable network, a transport company and a web services provider. What ties them together? They were all hit by high-profile security breaches.

But if you dig a little deeper, you'll find these organisations had a lot in common before, during and after their respective breaches. And those commonalities can teach us valuable lessons.

A quick recap

Equifax became the latest poster child for cybersecurity when it announced criminals had gained access to the financial data of 143 million people.

Equifax inherited the "poster child" title from Yahoo, which suffered an attack in 2013 and took the following four years to come to the conclusion that every last user account — including Yahoo mail, Flickr, Tumblr and Fantasy — had been compromised. All three billion of them.

Other companies newly inducted into the Fox Business Cyber Hack Hall of Shame include HBO, where hackers claim to have stolen 1.5 terabytes of proprietary data and Uber, where cyberthieves taxied away with 57 million users' personal information.

So, what did they all have in common besides the obvious?

Breaches were avoidable

All these breaches, no matter how sophisticated the attack, could have been prevented.

Whether due to a lack of interest, focus and urgency or all three, bad decisions were the key culprit behind these breaches and thousands of others occurring every day. According to IT analyst Forrester, two-thirds of companies were breached an average of five times, despite spending $80 billion on security last year.

Those numbers tell us something: we're not setting priorities effectively.

Protecting the data of our organisations and our customers must be paramount to all other business issues, every single day.

And it's not. Companies take an average of 193 days to patch known vulnerabilities, which is why Equifax was breached in the first place.

Second, it tells us that most organisations are taking an outdated approach to cybersecurity.

In lieu of stringently following best practices, we're throwing vast amounts of money at the problem. We're carpet bombing and crossing our fingers rather than responding with effective surgical strikes.

Breaches' identity component

While most media reports focus on how the initial breach occurred, they miss the most crucial part of the story.

The great majority of successful breaches leverage compromised identities.

Access is just the first step. Once inside, cyberthieves install malware that listens for privileged user credentials. Once they have those, they can move unfettered throughout the network, gaining access to companies' most valuable information.

It's the credentials — and the privileged access that comes with them — that count.

According to Verizon, compromised identities were responsible for 80 per cent of data breaches last year.

It's time to pull the focus off the point of entry and start severely limiting the damage cybercriminals can do once inside.

Is security in an identity crisis?

Despite cybercriminals' focus on identity, most organisations aren't making the connection between breaches and compromised credentials.

Last year, companies spent less than 5 per cent their security budgets on identity and access management, the very technology that would help prevent these breaches.

Breaches were poorly managed

Hollywood and the political arena aren't the only places where bad behaviour has led to serious repercussions this year.

Once the neglect had resulted in a worst-nightmare scenario, Equifax turned itself into a case study in poor decision management and harebrained leadership.

It took weeks to announce the breach had even occurred and what followed was a comedy of errors that would make Shakespeare cringe.

The best way out of the current situation is a program of shared responsibility. Companies should implement a zero trust model which assumes users inside a network are no more trustworthy than those outside.

Everything (users, endpoints, resources) is untrusted and must be verified. Security vendors should implement machine learning for behaviour-based fraud detection that assigns a risk level of each individual transaction and responds accordingly.

Consumers should demand multi-factor authentication for every single account, or find new vendors that offer it. This is something that's going to take the entire village working together to solve. The sooner we get started, the better.

Tom Kemp is CEO of Centrify.

> "Protecting the data of our organisations and our customers must be paramount."
>
> TOM KEMP, CENTRIFY