

Hisco replaced: ANZ has ap

SUBSCRIBE NOW

Shaw, 2019

'Arms race against cybersecurity': New Zealand businesses need to take threats seriously: expert

12 Apr, 2019 5:00am

5 minutes to read



NZ Herald's Chris Tarpey talks cyber security with Colin James from Vodafone

By: **Aimee Shaw**

Aimee Shaw is a business reporter focusing on retail, small business
aimee.shaw@nzherald.co.nz
@AceeyShaw



IN PARTNERSHIP WITH



The threat of a cybersecurity breach is not a matter of 'if' but rather one of 'when' and so businesses of all sizes need to be alert to mitigate risk, experts say.

Colin James, head of cyber security for Vodafone across the Africa, Middle East and Asia Pacific region, likens the urgency of imminent cyber threats to that of the arms race -- as organisations work to protect

their data and assets, hackers and scammers are increasingly coming up with elaborate ways to break through security systems.

"The arms race is effectively what we're seeing with escalation between the way we put in defences and the way people try and circumvent those defences and it's constantly elevated," James said at a PWC Herald Talks event held at Auckland's Victory Convention Centre this morning.

"What you see with the arms race where people are building better bombs and weapons the same applies in the cyber world where we're putting in bigger walls or better defences but someone's finding ways around that."

Though tough to stay on top of ever-evolving threats, James said businesses need to understand which assets they want to protect -- and work back from there.

"Know what your data is, where it is stored, how you're accessing it and make sure you have the right controls around that."

He said security needed to become the DNA of an organisation, part of strategy, and not just the role of the IT department.

"[Security] is an enabler not a back office function, it needs to work with the executive, the CEO, the board of directors, security needs to be visible across the whole organisation."


More than 3400 cyber security incidents were reported to Cert NZ last year, accounting for more than \$14.1 million in financial loss, of which around 35 per cent of the loss effected organisations.

The volume of cyber security incidents reported in the last calendar year increased by 205 per cent, up from around 1100 a year earlier. Phishing and credential harvesting made up the majority of breaches, followed by scams and fraudulent activity, then unauthorised access.

Related articles:

BUSINESS

Fran O'Sullivan: Why NZ must walk an independent path

10 Apr, 2019 5:00am
 minutes to read

PROPERTY

Boom's big impact on industrial property

10 Apr, 2019 5:00am
 4 minutes to read

BUSINESS

Former executive to pay \$150,000 for insider trading

9 Apr, 2019 6:01pm
 4 minutes to read

BUSINESS

World, Trelise Cooper, Farmers faulted in fashion ethics report

10 Apr, 2019 11:00am
 6 minutes to read

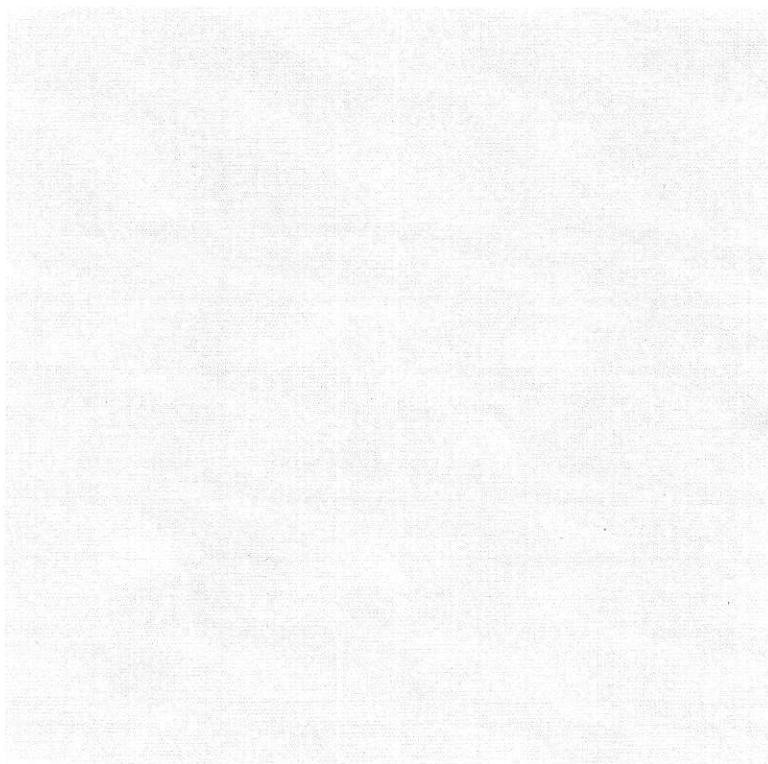
Most cyber attacks that occur prey on holes in vulnerabilities so it was important business ensured systems were patched and up to date, James said.

"Our data has gone feral, it's not longer in data centres within our networks protected by barriers, it's sitting out on mobile devices and tablets and cellphones and smartwatches even, our information has spread well beyond the organisation so we need to rethink the strategies we take and how we protect ourselves.

"We need to move away from a seige mentality and towards what we call submarine warfare - where we start hunting for threats within our organisation, actively looking for where the risks are."

The Internet of Things (IoT), increased network speeds and the 5G roll out would only make the risk of cyber security breaches even more imminent, James said.

Cyber security entrepreneur Kendra Ross said many New Zealanders were oblivious to threat of such breaches, particularly through things like IoT and smart devices.



Cybersecurity experts talk during the PwC Herald Talks Q&A panel. Photo / Supplied

"We bring these Internet devices into our business and bring them into our homes and they are set on a default.

"We're very lazy, we don't read our terms and conditions, we just accept and want instant gratification... meanwhile we've accepted that we can now share our contacts with this organisation and turn on the camera and microphone on the TV and through apps."

It was recently discovered that more than 300 apps in the Google Store contained malware which had been downloaded over 100 million times.

Ross said businesses that were aware of potential breaches in such technology and built security into their products and services would have a competitive advantage in the market.

"Utility trumps security" is the perception of many New Zealand businesses, PwC New Zealand cyber leader Adrian van Hest said during the event.

He also said security needed to be built in products.

"The perception there is very little risk in not securing something," van Hest said.

Our data has gone feral, it's not longer in data centres within our networks protected by barriers, it's sitting out on mobile devices and tablets and cellphones.

"When you're launching a product you are really focused on what does it achieve and the need for it to be secure is kind of an after thought. The

challenge with that is you've got to put it in so that security is utility so the security is easy to use."

He said cyber security was beholdent on anyone in a senior position within an organisation to understand technology and the risk associated.

Stephen Kraemer, Ports of Auckland chief information security officer, said businesses needed to invest between 5 and 10 per cent of their technology budgets on cyber security.

"If I was a small business I would consider using mainstream cloud services like Microsoft 0365 and accounting systems that are in the cloud because you get security backed into that," Kraemer said.

Ports of Auckland is in the process of automating its business and investing close to 10 per cent of the multimillion-dollar project costs on cyber security, he said.