

# Cyber Security

## Is the Risk Increasing? What Can We Do?

**Paul Ash**

*27 October 2020*



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA



# Global Trends...

**Technology is evolving quickly...**

**Covid-19 has increased our reliance...and vulnerability**

**Adversaries have noticed.  
Threats increasing, some more sophisticated.**

## Global ransomware attacks rise 110% in September

By StrategicRISK | 9 November 2020

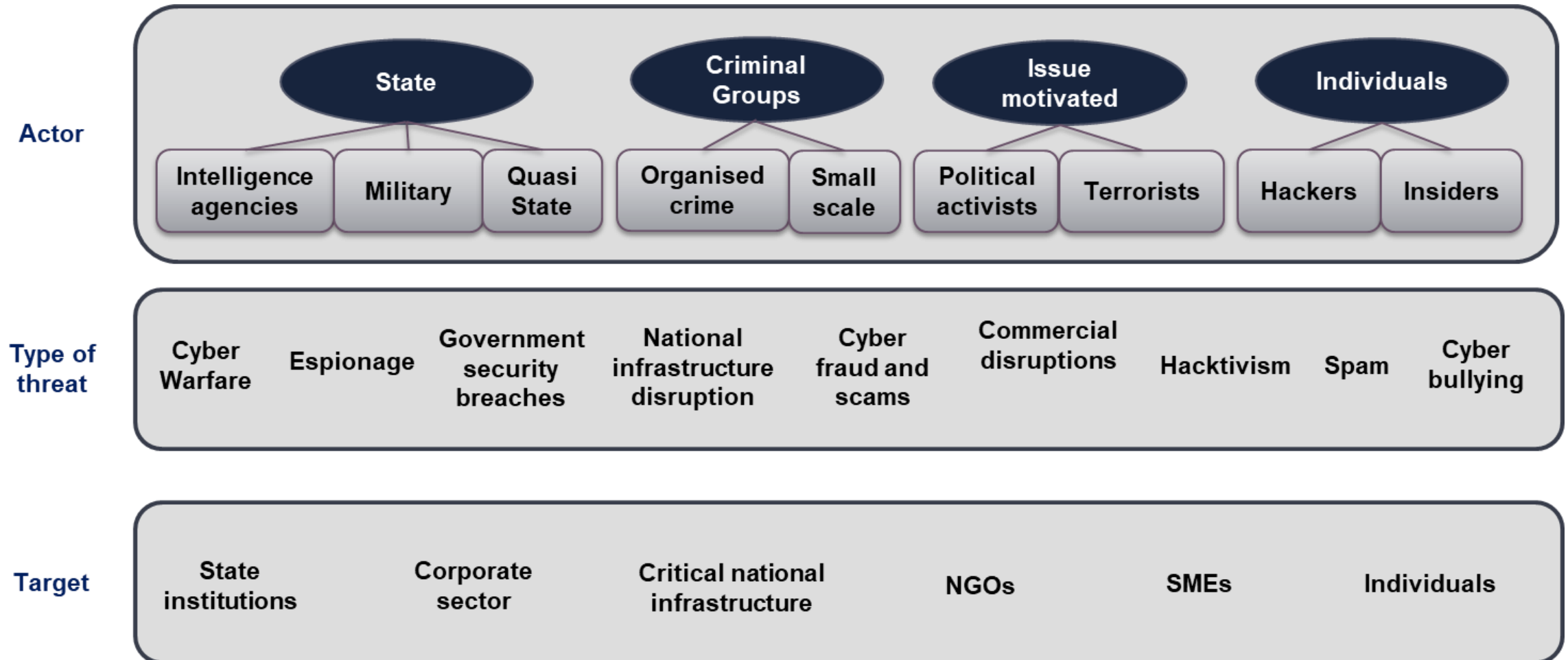


Overall, there was a 40% rise in ransomware attacks in the first three quarters compared to the same period last year

Ransomware attacks broke a two-year record in September of 2020. According to Atlas VPN, there were 34.11 million ransomware attacks detected this September compared to the same period last year when 16.21 attacks were recorded.



# ...Familiar Actors



# New Zealand's environment

- Part of a global network, dependent on it
- New technology changes risks...
- ...which have grown.
- Complacency costs...
- Making an attractive target



# New Zealand targeted...



## Incident Of The Week: New Zealand's Tū Ora Compass Health Discloses Security Breach Of 1 Million Records

Unpatched Web Servers Led To Four Separate Attacks On Primary Health Organization

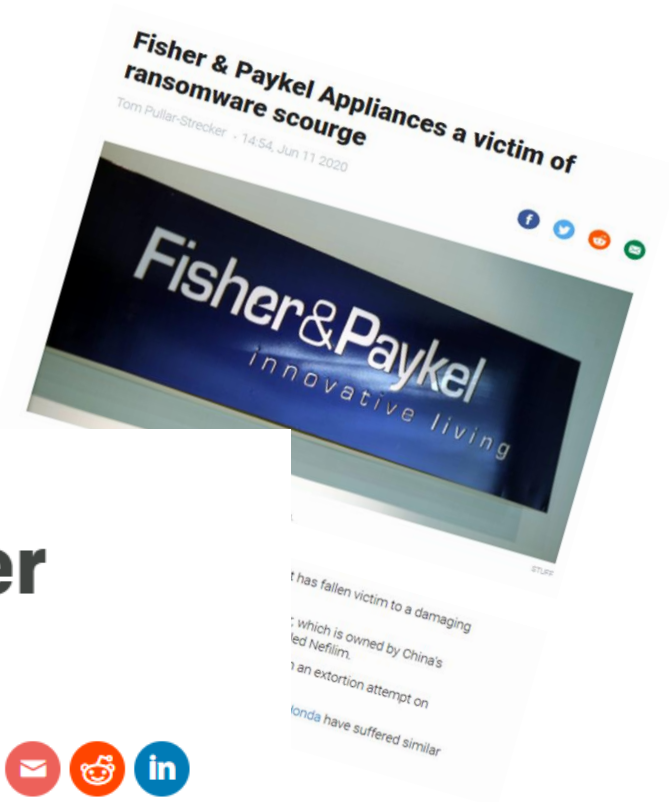
■ Add bookmark

Tags: Incident Of The Week IOTW New Zealand PHO GP Healthcare Medical Data Breach Attack Tū Ora PII



Jeff Orr

10/11/2019



BUSINESS

## NZX down again after another cyber attack

6:31 pm on 26 August 2020

Share this



The New Zealand stock exchange (NZX) has come under another cyber attack, bringing all trading to a halt.

# The tip of the iceberg...

## **CERT NZ 2020 Reporting**

3,102 incidents reported Q1/Q2

73% increase Q1 to Q2

42% increase from 2019

Most reported incidents: phishing and credential harvesting, and scams and fraud.

## **National Cyber Security Centre: Cyber Threat Report 2018-19**

339 incidents recorded to June 2019

38% of incidents linked to state-sponsored groups

# What we've done...

- Establishment of CERT NZ in 2017
- Delivery of CORTEX malware detection and disruption services
- Cyber Security Emergency Response Plan
- Capability building – Connect Smart, now Cyber Smart
- Protective Security Requirements for government agencies
- International engagement on cyber security issues
- Cyber Security Summit
- Establishment of NCSC
- 3 Cyber Security Strategies (2011, 2015, 2019)
- Attributed malicious cyber activity to state actors

**There's more to do...**





# How prepared is New Zealand?

The National Cyber Security Centre surveyed 250 organisations of national significance

- 61% providing cyber security reporting to senior management
- 63% have an incident response plan
- 64% considered IT security as part of vendor contracting
- 36% have no means to confirm vendors are delivering agreed level of IT security

**THINKING  
AHEAD.  
BEING  
PREPARED.**

Cyber Security Resilience of New Zealand's  
Nationally Significant Organisations 2017-2018

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government





# Government in the public eye...

NEW ZEALAND | Politics

## MSD shuts Winz kiosks after lax security exposed

15 Oct, 2012 12:45 AM

3 minutes to read



Photo / File

APNZ



Thousands of files on the Ministry of Social Development's computer servers, including the personal details of at-risk children, have been accessed through a Wellington Work and Income job seeker kiosk.

## Public sector an attractive target...

- Major digital presence
- Provider of critical services
- Sensitive information (citizen or government data)
- Disruption of service (DDoS, RDoS, Ransomware)

5 December 2019

## Final Report

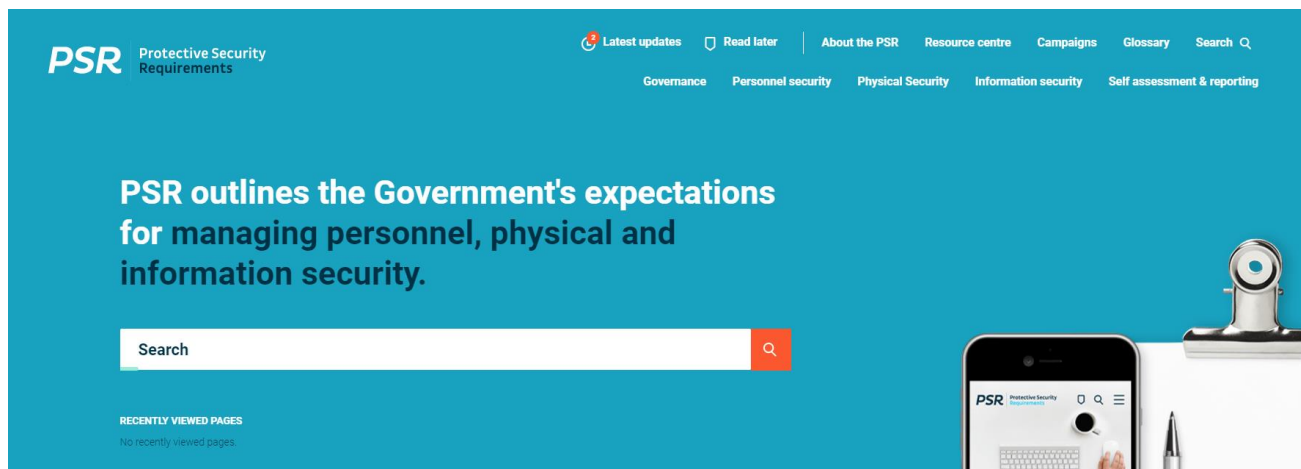
### Independent Review of the Tuia 250 Voyage Trainee Privacy Breach

**Manatū Taonga –  
Ministry for Culture and  
Heritage**

RDC Group Ltd

# ...leading to refreshed measures

- Government Chief Digital Officer (GCDO)
- Government Chief Information Security Officer (GCISO)
- Government Chief Privacy Officer (GCPO)
- Protective Security Requirements
- NZISM



# The Cyber Security Strategy



**Confident and secure in the digital world: Enabling New Zealand to thrive online**

# The new normal? Looking ahead

- Flexible working, engaging with the world
- Accelerated digital transformation
- What's critical?
- Grow the cyber security sector
- Strengthen resilience and awareness





# **The Cyber Security Opportunity**

**Cyber security crucial for  
recovery efforts**


**The value proposition:**

- **Trust**
- **Capability**



**Will require investment and vision...**

# You play a key role...

- Education and awareness
- Good cyber hygiene
- At home, work, and play
- Pandemic stress...
- ...does that email look suspicious?
- Seek help...no shame.

 **Top tips for cyber security** 

Online security is becoming more important than ever. While there's no bulletproof way to prevent a cyber attack, here are some easy tips to help you keep your personal information safe and secure.

<b>Back up your data</b>  Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.	<b>Keep your operating system up to date</b>  Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.	<b>Install antivirus software</b>  Free online antivirus software can be fake. Purchase antivirus software from a reputable company and run it regularly.	<b>Choose unique passwords</b>  Create unique passwords for each account – that way if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts.	<b>Set up two-factor authentication (2FA)</b>  Choose to get a code sent to another device like your phone when logging in online – it helps stop hackers getting into your accounts.	<b>Use creative recovery answers</b>  Common security answers like your pets name or your school can be easy for an attacker to find out. Choose novel answers that aren't necessarily real.
<b>Be cautious of free WiFi networks</b>  Be careful using free WiFi and hot spots - they are untrusted networks so others could see what you are doing.	<b>Be smart with social media</b>  What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.	<b>Don't give out personal info</b>  Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. Stop and check if you know who the email is from.	<b>Check bank statements regularly</b>  Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.	<b>Get a regular credit check</b>  An annual credit check will alert you if someone else is using your details to get loans or credit.	<div><p>To report a cyber security problem, visit <a href="http://www.cert.govt.nz">www.cert.govt.nz</a></p></div>



# Information and advice...

**Your Departmental Security Officer**

**CERT NZ** ([www.cert.govt.nz](http://www.cert.govt.nz) [@CERTNZ](https://twitter.com/CERTNZ))

**National Cyber Security Centre** ([www.ncsc.govt.nz](http://www.ncsc.govt.nz) [info@ncsc.govt.nz](mailto:info@ncsc.govt.nz))

**National Cyber Policy Office** ([www.dpmc.govt.nz](http://www.dpmc.govt.nz) [ncpo@dpmc.govt.nz](mailto:ncpo@dpmc.govt.nz))



**DPMC**