

DON'T LET A CRISIS GO TO WASTE

Lessons from a real life breach

Andy Pace, Network & Information Security Manager

mediaworks.

Talk Premise

- **Bad things happen to good people**
- **Businesses reluctant to share lessons learned**
- **Foster an open forum to discuss what worked well, and what could be improved**

Disclaimer

- **'Chatham House Rules' need not apply - only breach event details already in the public domain will be referenced.**
- **The views and opinions expressed in this presentation are those of the speakers and do not necessarily reflect the views or positions of any entities they represent.**
- **All characters and events are factitious. Any similarity to actual events or persons, living, dead, or undead, is purely coincidental.**

Before The Incident... Strategic and Tactical Planning

- Does the IT Strategy align with and support the Business Strategy?
- Do we have a current Business Impact Assessment?
 - Key systems and processes that support the primary business functions, and its associated risks
- Do we have a current BCP/DR plan? Has anyone read it?
- Do we have cyber incident Play Books? Have we tested them with a tabletop exercise?


Before The Incident... Covering Your Bases

- **NIST Cyber Security Framework a great way to identify any gaps in your Tools, Technologies, and Procedures and assess your overall capability maturity.**
- **Smaller environments - Essential 8**
- **Larger environments - MITRE ATT&CK**

What Happened?

[mediaworks.co.nz] 2,461,180 New Zealand citizens' data for sale
by OneERA - Thursday March 14, 2024 at 02:54 AM

OneERA



Breached

MEMBER

Posts: 1
Threads: 1
Joined: Mar 2024
Reputation: 0

10 hours ago

Thanks to BreachForums

Guys, we have stolen 2,461,180 New Zealand citizens' data from mediaworks.co.nz. We plan to sell this data, so please contact us as soon as possible if you're interested.

The data we successfully stole include:

- [Citizens' names, home addresses, mobile numbers, email addresses, dates of birth, home phone numbers, user postal codes, user genders, UserIds]
- [Citizens' private information, including some questionnaire answers, as well as some citizens' videos and music materials]
- [Information containing some voting and election details <The Block NZ 2017-The Block NZ 2020>...]

~ ...

Please contact us through the following means:

Email: [redacted]@proton.me

Example:

https://[redacted]

- 15th of March 2024 (Friday, 4pm) we became aware of chatter from the public domain about a potential breach

What Happened?

NEW ZEALAND / TECHNOLOGY

Alleged MediaWorks hack sees 2.5m Kiwis' data stolen

2:42 pm on 16 March 2024

Share this



- “It included people's names, addresses, dates of birth, email and phone contact details”
- HavelBeenPwned indicated there was actually 163k unique accounts.

Our Response

- **Activated Incident Response Team (IRT) and managed security services (Digital Forensics and Incident Response, DFIR) team**
- **Spun up internal MediaWorks Crisis Management Team, CMT**
- **IRT worked with CMT, DFIR, and external legal counsel to define comms plan**
- **Set up regular CMT meeting cadence**
- **External and internal legal teams liaised with the Police, CERT NZ and The Office of the Privacy Commissioner**

Our Response

- **DFIR team liaised with the Threat Actor to confirm the legitimacy of the claim and obtain a sample**
- **IRT worked with internal Devs to identify the source and take it offline**
- **Threat Actor claimed to have access to other data sources**
- **DFIR team ran pen test of our cloud environment**
- **Threat Actor began reaching out to those affected, offering to sell them their own data, as a means to put pressure on us to respond**

Our Response

- **MediaWorks Privacy team began reaching out to those affected**
- **MediaWorks' Cyber / IT teams began systematic review of all systems**

Lessons Observed...

- **Be prepared. Have your plans and playbooks in place**
- **Test the plan, improve, rinse & repeat**
- **Have a comms strategy**
- **Have IRT role backups in case key team members are unavailable**
- **Use a framework like CSF to find the gaps**
- **Engage with and trust the experts - your worst day is their BAU**

Lessons Observed...

- **Keep a very detailed log of the event and actions – get the whole team to contribute and update as they go. Include meeting updates, outcomes and action plans**
- **Keep your own staff informed – they'll have customers asking**
- **Keep the comms going and support each other**
- **You have about 6 months before life returns to BAU, so make the most of it**

Lessons Observed...

- **Cyber Awareness / training for staff**
- **Lunch & Learn covering sensitive data**
- **Get them to think about the data they have access to:**
 - **What data types do you have access to? Who else has access?**
 - **Why do you have it / What's the business requirement?**
 - **Where is it stored?**
 - **How long do you need to keep it for?**
- **Encourage empathy; how would they feel if their or their family's data was breached?**



[linkedin.com/in/nzandypace](https://www.linkedin.com/in/nzandypace)

Thank You Questions?

mediaworks.

