Think a cyber attack wouldn't happen to you?

Think again

PwC Cybersecurity Webinar for NFPs
24 Feb 2022

Please go to www.menti.com

Enter code 8268 6554

What we will talk about today?

The current business, technology and cyber threat landscape

Key threat scenarios for NFPs to consider - case studies

What can be done by NFPs to protect against these cyber threats?

Key takeaways and cyber resources at your disposal

01

Changing Cyber Threat Landscape

Consider this scenario

- It's a Friday afternoon, and you are about to go and pick up your kids or meet your friends after work
- You receive an email from your boss requesting an urgent payment be made to a priority client
- You download and open the email attachment titled "payment transfer information"
- After opening the attachment, a message pops up notifying you that a software update is required and prompting you to call the IT support desk for help
- You call the IT support team using the provided number and ask them to help you with the update
- The IT support team asks for your full name, email address, and password
- You start the update and leave your computer unlocked for the weekend
- On Monday, you go to log in to your account but can't access any of your systems or data

What red flags or potential indicators of a cyber threat you can see here?

NFP sector priorities: Digitisation is here to stay...

Increasing pressures to do more with less

Rapid digital transformation and cloud adoption

Future resilience and automation

Need for skilled and technical resources

...so is cybercrime

Cybercrime is evolving….

Improving **data and information security** is a **top 3 priority** for NFPs

400%

Increase in cyber attacks since COVID19

Health sector has the highest reporting rate of data breaches in Australia

Health care and social assistance industries had the second-highest reporting of ransomware-related incidents in Australia

$ Criminal attacks

Human error

System faults

...are the primary sources of data breaches

Typical motives and impacts of a cyber attack

Criminal
For the money

Cyber criminals are largely indiscriminate in who they attack as they simply seek to monetise their attacks. The range in sophistication of cyber criminals is vast, and include stealing data, extorting an organisation or outright theft of funds.

Espionage
For the nation

Espionage threat actors (often referred to as “Advanced Persistent Threats”, or APTs) typically seek to steal information which will provide an economic or political advantage to their benefactor.

Hacktivist
For the cause

Hacktivists conduct attacks to increase their public profile and raise awareness of their cause. This could include disruption of business services or stealing and leaking sensitive information.

Sabotage
For the impact

Saboteurs seek to damage, destroy or otherwise subvert the integrity of data and systems. Sabotage attacks are not always deliberate and have been used to mask other malicious activity.

What's the impact of these threats?

Direct Costs

- Investigation and remediation
- Regulation sanctions
- Cost of breach

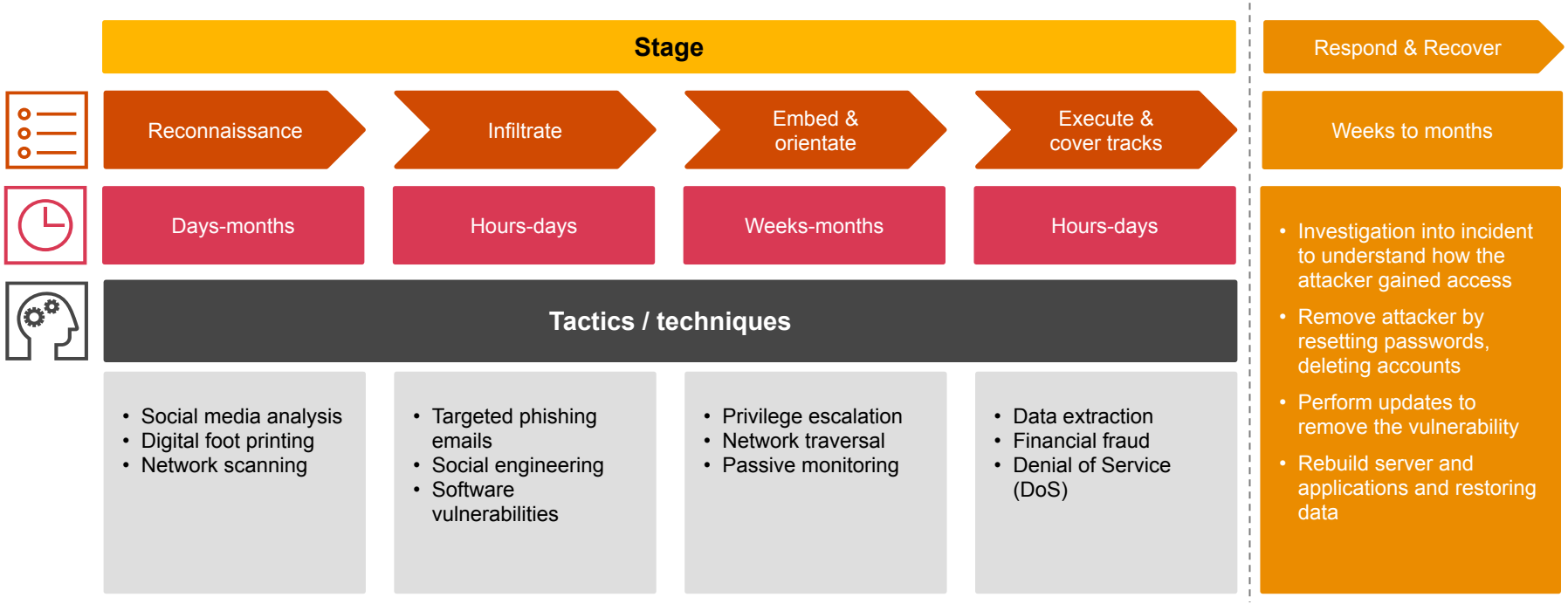
Indirect Costs

- Increased cyber premiums
- Customer fraud
- Class action lawsuit

Intangible Costs

- Brand reputation damages
- Loss of subscribers/donations
- Loss of trust
- M&A value decrease
- Firing of executives

What does a typical cyber attack look like?



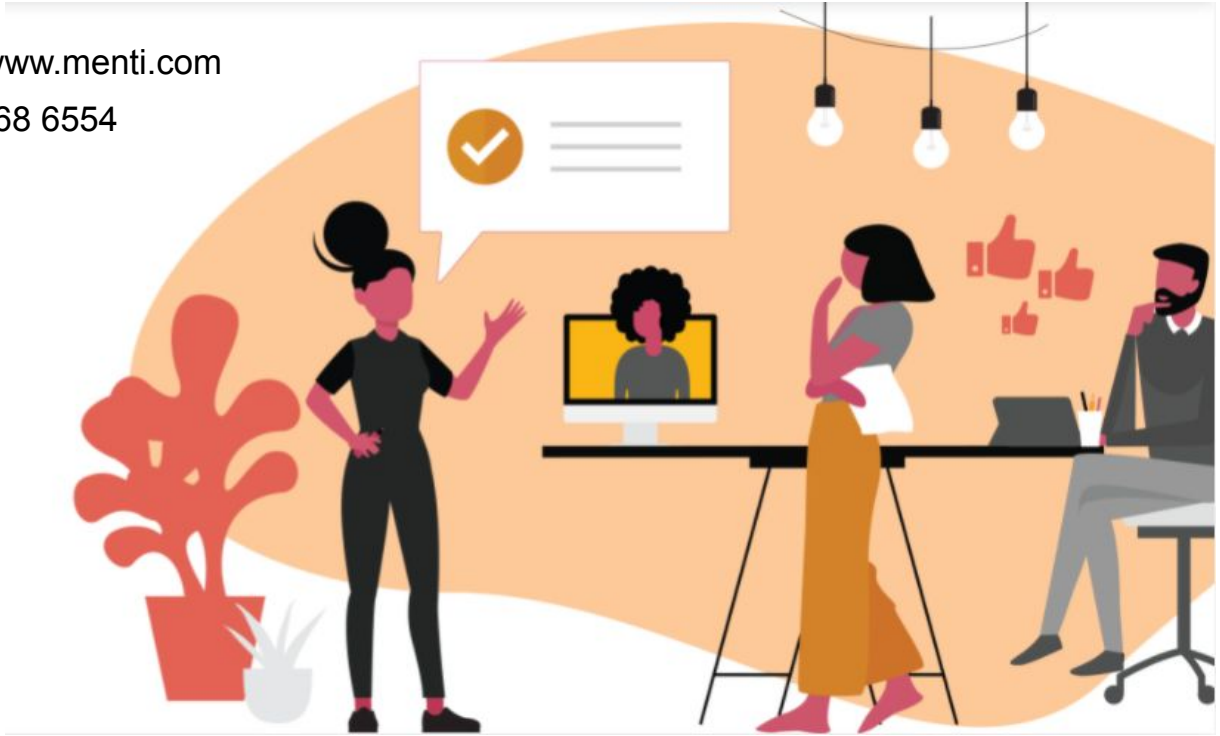
02

Key threat scenarios for NFPs to consider

Let’s do another activity

Please go to www.menti.com

Enter code 8268 6554



Business Email Compromise (BEC) resulting in loss of funds

What happened: **In 2020, an Australian hedge fund was the target of BEC attacks and forced to declare bankruptcy as a result.**

Fake Zoom invitations were sent to employees at the fund, which when opened planted malicious software on the network and allowed attackers to take control of the organisation's email system.

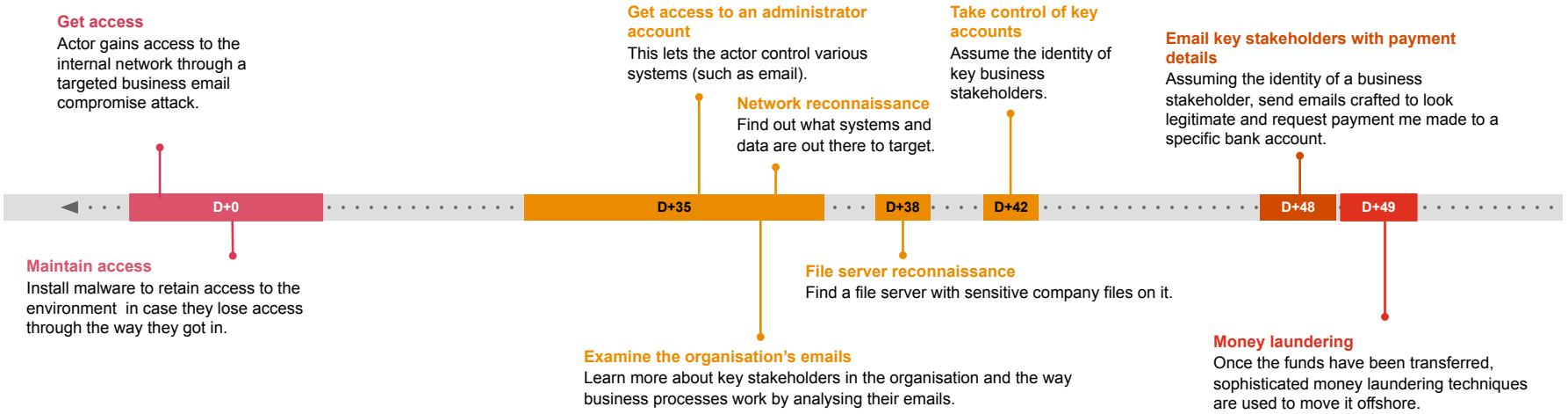
The attacker then used their access to **exploit trusted relationships** between the fund's trustee and administrator. This resulted in $8.7m in payments being made to different bank accounts.

The Hedge Fund was able to stop most payments, but $1.2m was successfully transferred, of which $800,000 was **stolen by a 'money mule'** before they flew offshore.

Impact to the business:

- $8.7 million of funds stolen.
- Significant reputational damage and impact to trust and confidence, including the withdrawal of the fund's main client.
- Hedge fund was forced to go into receivership and declare bankruptcy.

An example of how a BEC attack like this can occur...



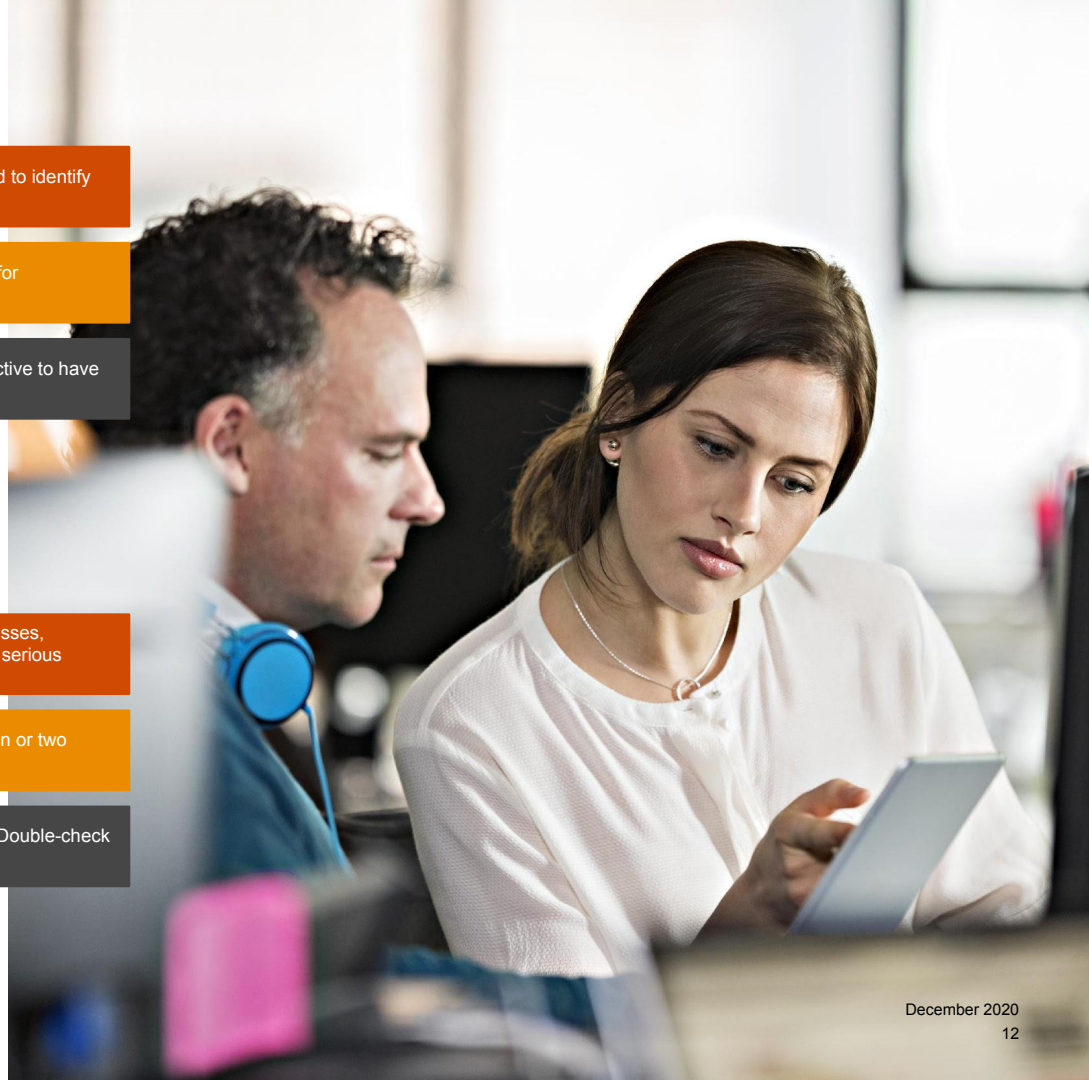
Note: the diagram above is a fictitious example based on the techniques of a real actor. This demonstrates a typical BEC attack.

Lessons Learned

1. Many cyber incidents occur through human error. Employees that are not trained to identify and respond to suspicious activities can provide an open door to cyber attacks.
2. The failure of business checks and balances can have dramatic consequences for organisations and their customers.
3. Prevention trumps detection and recovery. It's much simpler and more cost effective to have controls in place to prevent BEC than it is to deal with the consequences.

Simple Steps to Improve Security

1. Ensure workers are aware of the warning signs, such as misspelled email addresses, unexpected changes to bank details, urgent payment requests and/or threats of serious consequences if payment isn't made.
2. Implement verification processes for financial requests (e.g. phone call, in-person or two person verification).
3. Check communication details such as the spelling of a sender's email address. Double-check by comparing to previous correspondence.



Data breach resulting in customer data disclosure

What happened: In 2021, attackers stole the personal information of supporters of one of Australia's largest not-for-profit organisations, including names, addresses, dates of birth, emails, phone numbers, gender and in some cases, donation history.

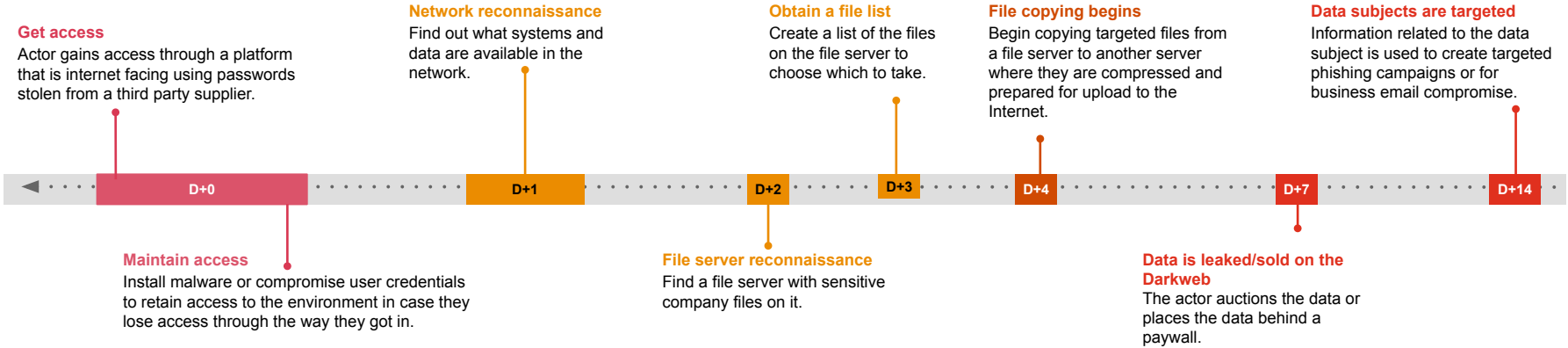
Approximately 1.7million charity supporters were impacted by the data breach, including campaign participants and charity shop customers, with personal information being published on the dark web.

The organisation was required to notify all affected parties, including providing warnings that victims were at heightened risk of suffering phishing attacks and telephone scams and steps to take to protect against further impacts.

Impact to the business:

- Suspension of fundraising activities while an independent IT forensic investigation was being undertaken
- Notifiable data breach requirements
- Supporters were at risk of increased targeted phishing as a result of the breach
- Negative media coverage and reputational damage

An example of how a data breach like this can occur...



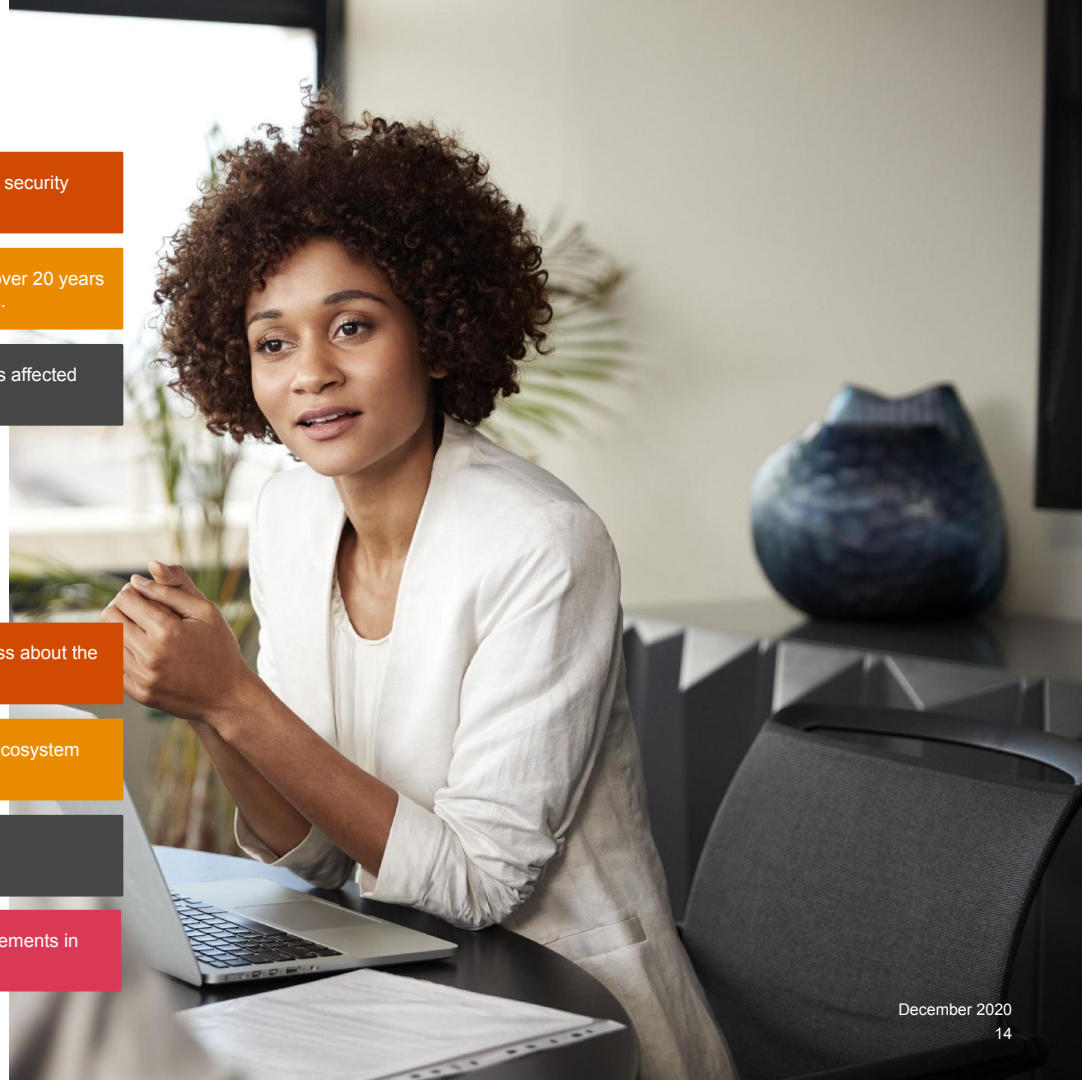
Note: the diagram above is a fictitious example based on the techniques of a real actor. This demonstrates a typical data breach attack.

Key learnings

1. It's important to limit access to your most valuable data, including the access and security controls applied to 3rd parties working with your organisation
2. All sensitive data requires appropriate security measures as personal data from over 20 years ago can still cause damage via phishing campaigns and other malicious activities.
3. Providing clear and accurate details of the breach as soon the business can gives affected parties more notice to protect themselves.

Simple Steps to Improve Security

1. Strong password protection strategies are critical, including raising staff awareness about the importance of protecting credentials.
2. Conduct periodic risk assessments to ensure your valuable data and third party ecosystem have appropriate security controls.
3. Enable multi-factor authentication and suspicious-activity detection.
4. Establish clear internal and external cyber incident reporting and response requirements in the case of a security or data breach.



Ransomware resulting in data loss

What happened: In 2020 an Australian aged-care provider was targeted in a cyber attack by an overseas third party which resulted in the theft of personal and organisational data.

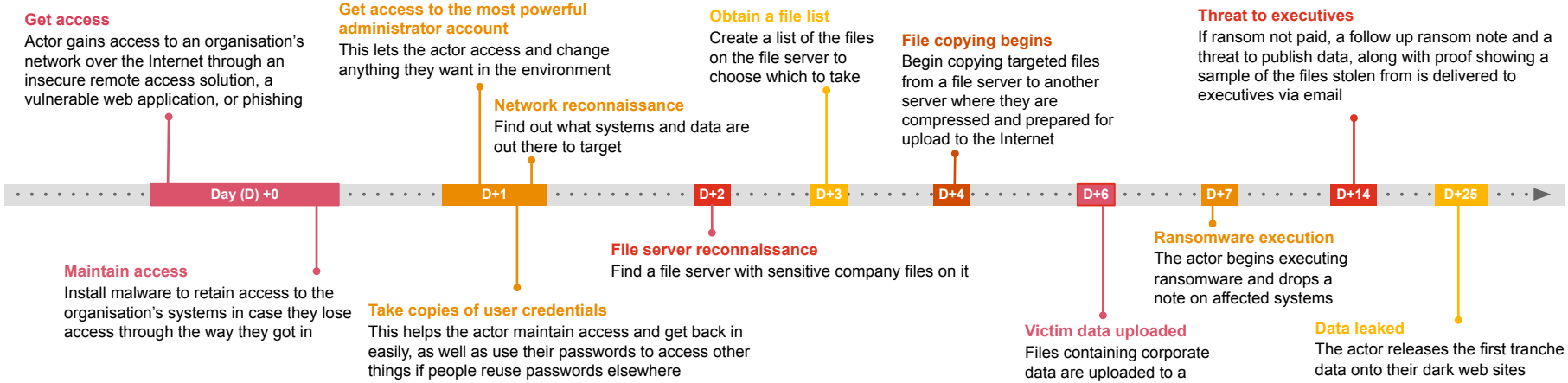
The incident was part of a targeted campaign of 'Maze' ransomware by financially motivated cyber criminals, looking to exploit the sensitive and medical information held by organisations in the healthcare industry.

The attack prompted the Australian Cyber Security Centre to publish a warning about the ransomware campaigns targeting aged care and healthcare sectors.

Impact to the business:

- Stolen data including personal information and operational documents such as care and accommodation agreements was released on the dark web
- The business launched an IT investigation into the incident and was able to enable business continuity plans to maintain critical operations
- Attack occurred during the COVID-19 pandemic, when health and aged care services were particularly critical

An example of how a ransomware attack like this can occur...



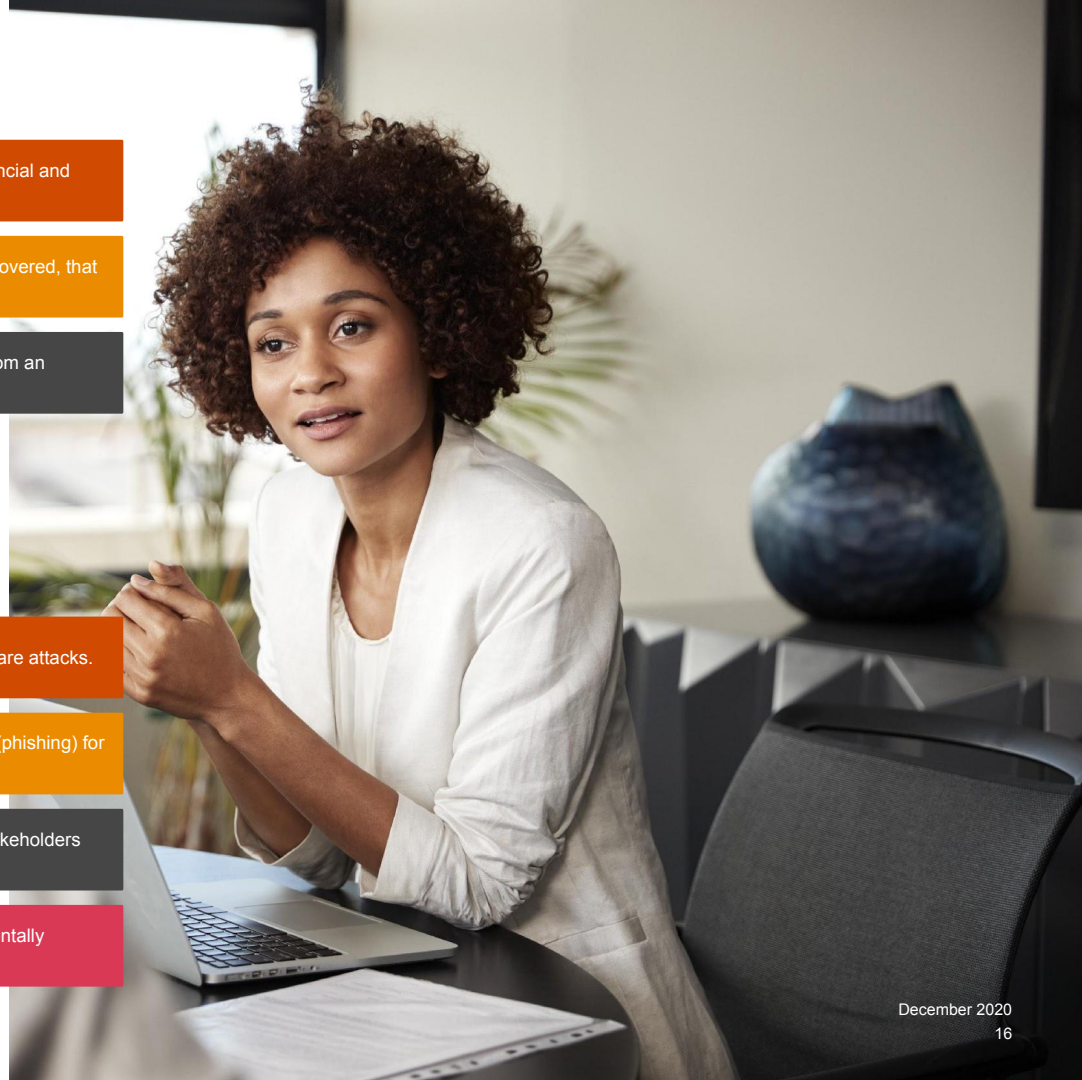
Note: the diagram above is a fictitious example based on the techniques of a real actor. This demonstrates a typical ransomware attack.

Key learnings

1. A cyber incident may not impact the delivery of services but still have severe financial and reputational implications.
2. There is no guarantee that the a ransom payment will lead to your data being recovered, that the data won't be on-sold, or that you will not be attacked again.
3. Appropriate security measures like backups allow for a more efficient recovery from an incident with reduced down time.

Simple Steps to Improve Security

1. Regularly backup data and develop a response strategy in the event of ransomware attacks.
2. Ensure that employees are aware and can identify common methods of delivery (phishing) for ransomware through training.
3. Regularly test your ransomware response plan with cross functional business stakeholders and technology teams.
4. Block harmful sites and applications to reduce the likelihood of employees accidentally installing malicious software.



03

What can be done by NFPs to protect against cyber attacks?

Five simple steps to improve security

Uplift cyber awareness and education: Raise awareness about key cyber threats and what can be done as a business or as individuals to protect yourselves, your customers and your suppliers.

1

Regularly update (patch) software and operating systems: This will greatly reduce the risk of attackers compromising a system through vulnerabilities in the software.

2

Multi-Factor Authentication (MFA): For access to any business critical applications ensure MFA is used (e.g. username/password AND one-time PIN code)

3

Understand your cyber risks: Conduct a risk assessment to understand which business processes and data repositories, if compromised, could have the largest impact.

4

Incident Response Planning: Have appropriate incident crisis management plans in place for cyber attacks (e.g. if a data breach occurred, what actions would you take?)

5

Note: ASD Essential 8 mitigation strategies refer to application whitelisting, patching applications, configuration of Microsoft Office macro settings, user application hardening, restriction of administrative privileges, patching operating systems, implementing multi factor authentication and performing daily backups

04

Key cyber resources at your disposal

Free resources for NFPs

General cyber security resources

Digital Transformation Hub

Infoexchange Digital Transformation Hub

Contains many links to guides, advices, and information that can help improve cyber security practices in your orgaintsions. Resources are broken down into three levels; Basic, Intermediate, and Advanced.

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

ACSC Small Business Cyber Security Guide

This guide has been developed to help small businesses protect themselves from the most common cyber security incidents.

ACSC Step-by-step Guides

The Guide to undertaking privacy impact assessments (PIA Guide) has been prepared by the Office of the Australian Information Commissioner (OAIC) to describe a process for undertaking a privacy impact assessment (PIA).

Australian Government
Australian Charities and Not-for-profits Commission

ACNC Governance Toolkit: Cybersecurity

Governance Toolkit - helps to understand cybersecurity issues - what they are, how they may affect charities and what charities can do to reduce risks of cyberattacks.

Free resources for NFPs

Understanding privacy obligations

Understanding the Notifiable Data Breaches Scheme

Fact sheet that contains information on the Notifiable Data Breaches Scheme, including how to notify and penalties for not complying.

Privacy Compliance Manual

Norton Rose Fulbright has provided Not-for-profit Law, a service of Justice Connect, with its Privacy Compliance Manual for use by charities and not-for-profits. The Manual contains an overview of new federal privacy laws and a template privacy policy.

Guide to undertaking privacy impact assessments

The Guide to undertaking privacy impact assessments (PIA Guide) has been prepared by the Office of the Australian Information Commissioner (OAIC) to describe a process for undertaking a privacy impact assessment (PIA).

Privacy Guide - A guide to complying with privacy laws in Australia

This guide is for not-for-profit organisations in Australia who want to understand more about their obligations under privacy laws in Australia. This guide describes obligations under the Privacy Laws.

Responding to incidents

Social Media Vandalism Toolkit

This document provides guidance, resources, and security practices that prepare users to respond to cyber-hijacking, make informed choices, and enact future policy.

Report Cyber Incidents

Use this website to report any cyber incidents to the ACSC.

Sample Incident Response Template

A Cyber Incident Response Plan template developed by the Victorian Government that can be leveraged to create a plan for any organisation.

OAIC Notifiable Data Breach

The website of the Office of the Australian Information Commissioner where Notifiable Data Breaches must be reported.


Any questions?

Thank you

www.pwc.com.au

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.

PWC200183781