Cybersecurity – Protecting your data in an era of information sharing

The 47th One Stop Update for the Accountant in Business

Incident Response

FORENSIC & CYBER

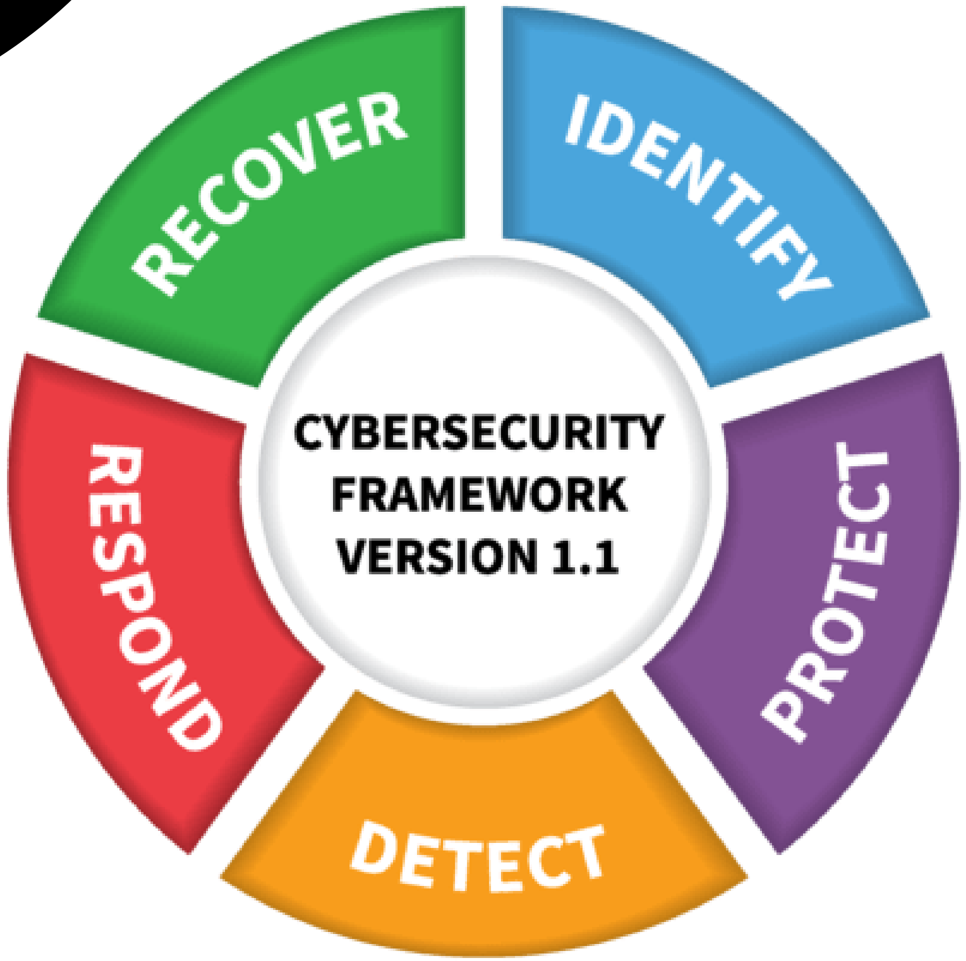
Agenda

Protecting data and information from malware attacks

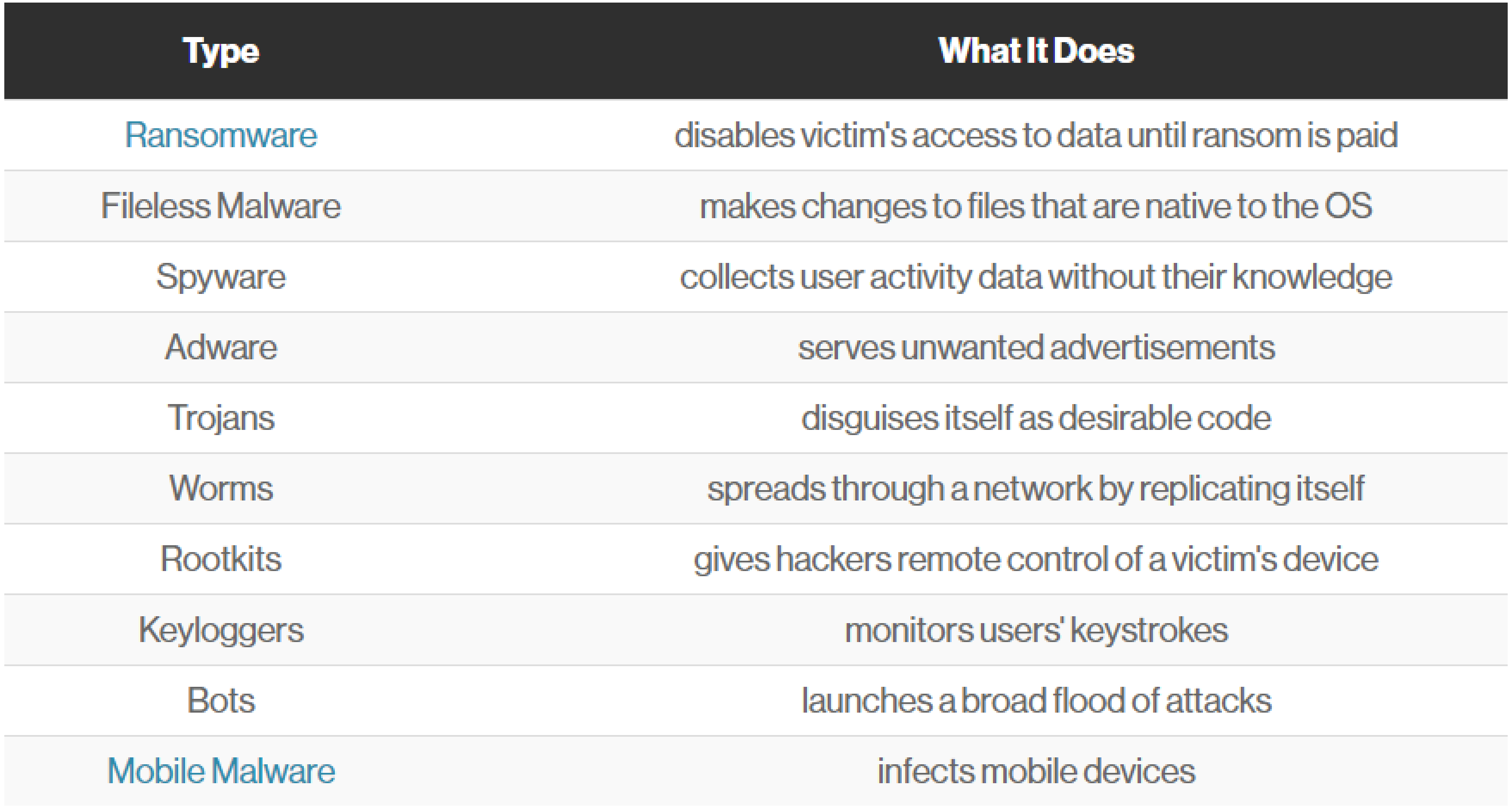
Solutions to allow distribution and access to sensitive documents when working remotely

Cyber and the finance function

NIST


CYBERSECURITY
FRAMEWORK
VERSION 1.1
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Types of Malware



Type	What It Does
Ransomware	disables victim's access to data until ransom is paid
Fileless Malware	makes changes to files that are native to the OS
Spyware	collects user activity data without their knowledge
Adware	serves unwanted advertisements
Trojans	disguises itself as desirable code
Worms	spreads through a network by replicating itself
Rootkits	gives hackers remote control of a victim's device
Keyloggers	monitors users' keystrokes
Bots	launches a broad flood of attacks
Mobile Malware	infects mobile devices

Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks.

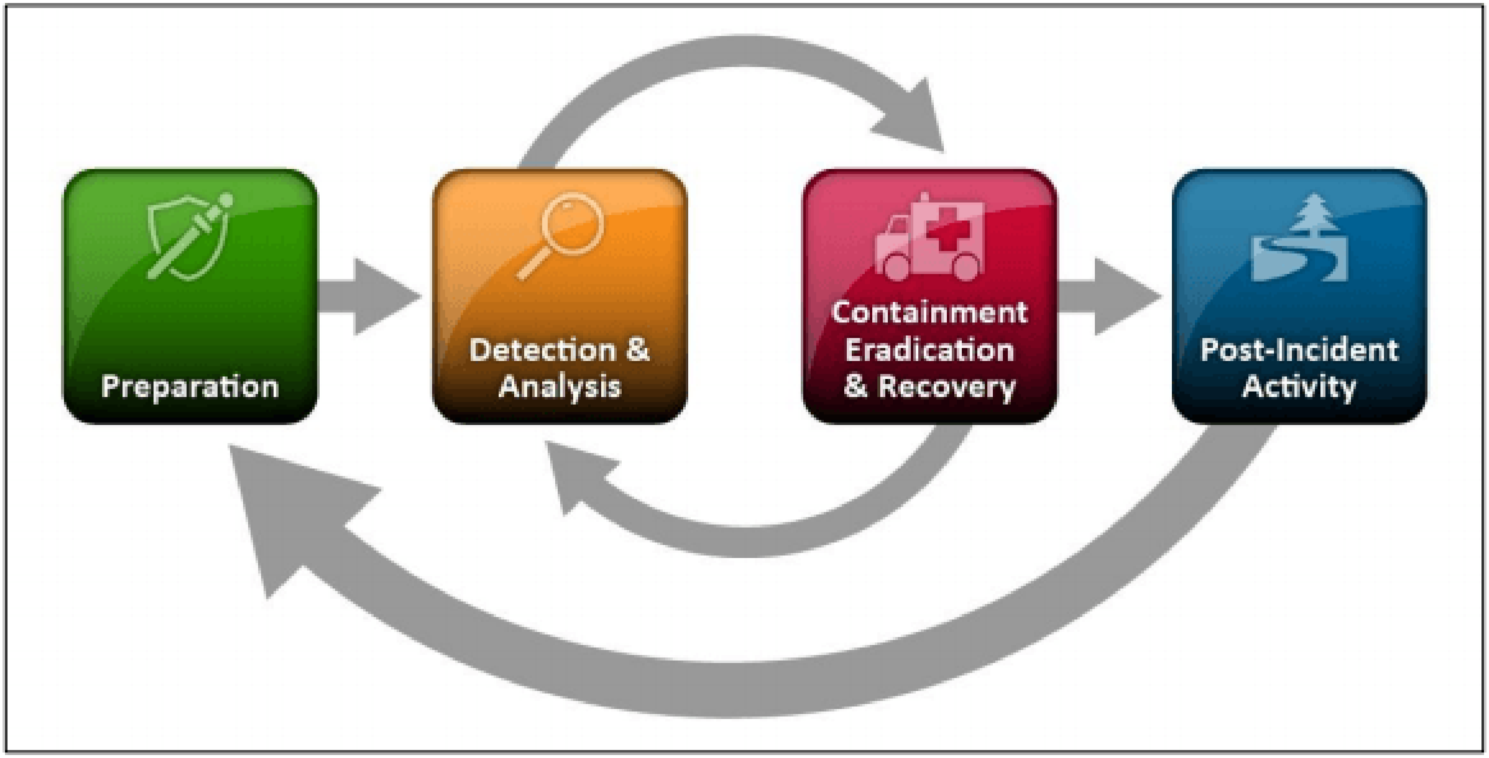
The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

Ransomware Prevention Checklist

Key Best Practices		Additional Best Practices
• User Education • Allowlisting • Account Control • Backups • Workstation Management • Host-Based Intrusion Detection / Endpoint Detection and Response • Server Management • Server Configuration and Logging • Change Control	• Network Security • Network Infrastructure Recommendations • Host Recommendations • User Management • Segregate Networks and Functions • Physical Separation of Sensitive Information • Virtual Separation of Sensitive Information	• Vulnerability assessments • Encryption of sensitive data • Create an insider threat program • Review logging and alerting data • Complete independent security (not compliance) audits • Create an information sharing program • Maintain adequate documentation - QRH

Preparation

Your Incident Response processes should analyse security events to learn how to prevent future attacks and attempt to recover stolen data.



Preparation

Manage the risk posed by ransomware and support your organisation’s coordinated and efficient response to a ransomware incident.

Create, maintain, and exercise a basic cyber incident response plan (and playbooks) and associated communications plan that includes response and notification procedures for a ransomware incident.

Run regular cyber simulations to evaluate the effectiveness of the incident response plan, and drill the training into the CSIRT team.

Clearly define and allocate roles and responsibilities in advance, and have a backup option for each.

Roles and Responsibilities

An incident response plan clearly sets out the roles and responsibilities of those involved in the incident response.

Privacy officer

Information security and ICT

Legal

Communications

Risk and assurance

Service delivery/operations

Senior leadership team

Ransomware Response Checklist

Detection and Analysis	Containment and Eradication	Recovery and Post-Incident Activity
• Determine which systems were impacted, and immediately isolate them. • If possible, power down devices to avoid further spread of the ransomware infection. • Triage impacted systems for restoration and recovery. • Develop and document an initial understanding of what has occurred based on initial analysis. • Engage stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.	• Collect system images, memory captures and relevant logs. • Research the ransomware variant and follow recommended steps. • Identify the systems and accounts involved in the initial breach. • Contain systems that may be used for further unauthorized access. • Examine IDS systems. • Rebuild systems based on a prioritization of critical services. • Issue password resets for affected systems and address vulnerabilities. • The designated authority declares the ransomware incident over.	• Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services. • Document lessons learned from the incident to inform updates to incident response plans, and procedures and guide future exercises of the same. • Consider sharing lessons learned and relevant indicators of compromise with your sector for further sharing and to benefit others within the community.

Remote Working

- Make a list of all the important systems. Add your email, chat, communications and document storage systems
- Note where those systems can be accessed from - can they be accessed from anywhere on the internet
- Designate someone as the go-to person to call when there is an incident
- Configure remote access software that connects your staff to your office network and use two-factor authentication
- Set long, strong, unique passwords
- Back up any documents they are working on locally to the office network or document storage systems
- Keep any devices or data with you when you are in public spaces
- Configure devices to download and install software updates automatically
- Configure built-in operating system antivirus and hard-drive encryption software

Financial
Review

Cyber and
the CFO

Key Findings from the CAANZ Report

- 54% were either not aware of whether their organisation had suffered an attack or thought they had not been.
- In just 8% of organisations, the CFO was responsible for the strategic direction of cyber security.
- The annual cost of cybercrime to the global economy will double from US$3 trillion in 2015 to $US6 trillion in 2021.
- Many organisations pinpoint cybercrime as one of their most significant threats.
- There are key reasons for the CFO to step up and play a leading role in cyber security.

https://www.charteredaccountantsanz.com/news-and-analysis/insights/research-and-insights/why-cfos-should-take-the-lead-on-cyber-security

1. Cybercrime is finance

- 76% were financially motivated (Verizon – 53,000).
- Damage is measured in financial terms – which the CFO quantifies and manages risk.
- The CFO has the skills and oversight to take a broader and longer-term view of the financial impact of an attack.
- The CFO looks beyond immediate issues of data loss and disturbance, to reputational/ regulatory/shareholder concerns.

2. Data custodians

- The CFO is one of an organisation’s key custodians of data. They increasingly assess its value and manage its lifecycle.
- They are also responsible for some of an organisation’s most sensitive and valuable data, so they have an important role in identifying information that is vital to protect.

3. Highly trusted

- The CFO and the finance department are highly trusted, which can be used to promote cyber security within their organisation.
- The CFO can discuss cyber security with the board, the wider organisation and outside stakeholders. They can position it as a business and commercial risk that needs to be mitigated.
- Finance has the skills to oversee audit, inventory, testing and compliance, and will take the lead in assessing and underwriting cyber insurance.

4. In the front line of attack

- The CFO will be on the front line if cyber criminals attack. The target is most often financial data, but also the finance department and its personnel.
- After the attack, CFOs will be expected to accurately assess the damage, lead internal reactions, and communicate with stakeholders.

Thank you

Campbell McKenzie

0800 WITNESS

campbell@incidentresponse.co.nz

incidentresponse.co.nz

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents

Incident Response
FORENSIC & CYBER