

RANSOMWARE DEFENCE STRATEGY



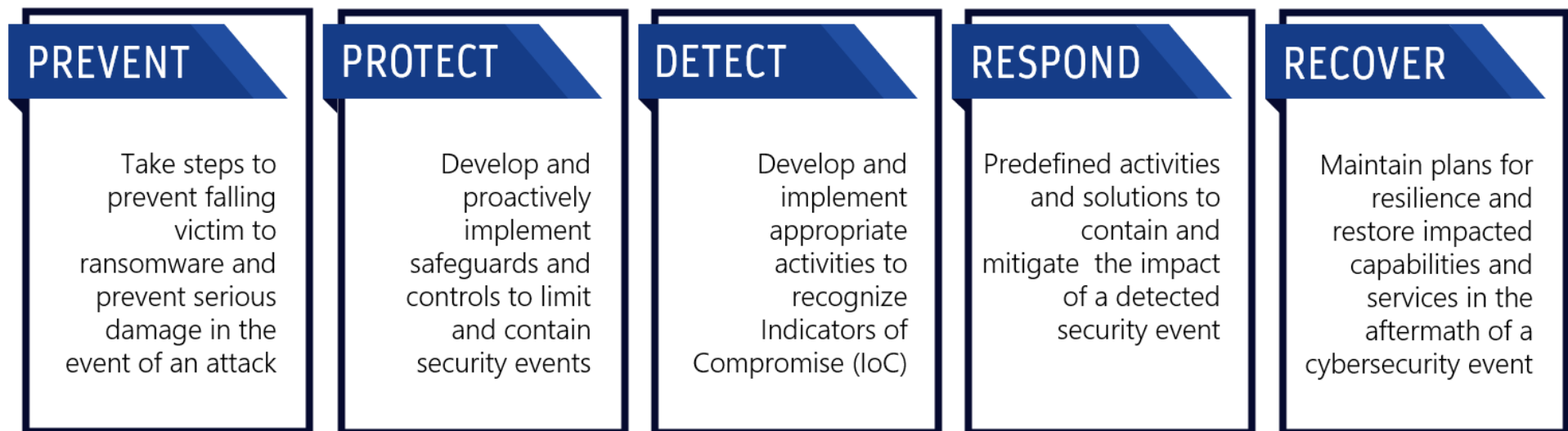
Traditionally ransomware attacks were carried out by the “bad guys” installing malicious software on your system to encrypt all your files and data. They would leave you with a ransom note offering to supply you with a decryption key when you paid their ransom. This commonly occurred by sending a malicious email with a payload that would deploy their malware when a user accessed the attachment. This is generally no longer the case.

Ransomware is no longer your biggest problem; It is the result of a broader security breach.

Attackers are now using multiple entry points by exploiting network and software vulnerabilities as well as continuing to use malicious email and many other methods to deliver malware to gain access to your systems and sensitive data. Ransomware is now a billion-dollar cybercrime industry.

Consequences for businesses are not only financial and can include temporary or permanent loss of critical data and services, downtime resulting in loss of productivity, loss of opportunity and loss of income and reallocation of resources to resolving the attack rather than performing their normal duties. Reputational damage can be caused by any cyber security incident which may result in customers or partners losing faith in your organization’s ability to protect their data and may be detrimental to the viability of your business.







Developing a Ransomware Defence Strategy including our five stages can put your business in a stronger defensible and recoverable cyber position.









RANSOMWARE

Defence Strategy Checklist






PREVENT

	Key Deliverables	Controls
	Impact Analysis Threat scenarios	Data Classification Policy <ul style="list-style-type: none"> Identify sensitive data and classify it according to sensitivity and document - identify where PII is held.
	3-2-1 Backups	Backup Policy <ul style="list-style-type: none"> Backups should be carried out on all servers, VM's, cloud storage, cloud applications, websites and web apps, accounting, payroll, and endpoints using automated tools. Critical data and services must be backed up daily. One backup should not be connected to the main corporate network and be secured using a separate administrator account with an extremely strong, unique password with very limited access.
	Backup Test Report	Disaster Recovery Policy <ul style="list-style-type: none"> Test backups & DR sites as well as restoration procedures regularly.
	User Awareness Training	<ul style="list-style-type: none"> Phishing Simulation. Cyber Security Training. Reporting process for suspicious activity for users. Use regular communications to your users to highlight the importance of personal and business cybersecurity practices as well as the recent statistics regarding the prevalence of ransomware attacks and methods of infiltration. Acceptable Use and Password Policies.
	Business Continuity Plan	Business Continuity Plan Disaster Recovery Policy
	Incident Response Plan	Incident & Data Breach Response Policy Cyber Event Activation Plan <ul style="list-style-type: none"> Test the plan regularly so in the event of an attack your response team is familiar with the procedures.





PROTECT

	Key Deliverables	Controls
	Email - this is still one of the main attack vectors	Secure Email Gateway <ul style="list-style-type: none"> Email filtering inbound - anti-spam and anti-phishing. Email filtering outbound.
	Web	Web filtering and Layer 7 scanning should occur at the perimeter including: <ul style="list-style-type: none"> L7 inspection at WWW perimeter. L7 inspection on all access points. DNS-SEC & WAF enabled across domains and websites/web apps. i.e., Cloudflare.
	Endpoints	NGAV must be active and scanning across all devices. <ul style="list-style-type: none"> PC, mobile, tablets & servers.
	Patch Compliance Report for all servers and endpoints at all locations	Patch Management Policy: All devices must be patched regularly: <ul style="list-style-type: none"> Software, firmware, applications and security and cumulative updates. Endpoints (servers - both physical and virtual, PC's and mobile devices), network devices (LAN, WAN and Wireless), peripheral devices (NAS, MFP's etc.), smart devices (TV's etc.)
	Encryption & Remote Access	Remote Access Policy Information Security Policy, Remote Access Policy, Cryptography Policy. All data must be encrypted at rest or in transit - use a VPN for remote access.
	Cloud Configuration	Check use and configuration aligns with recommended best practices of the provider. <ul style="list-style-type: none"> Restrict Internet access to only the protocols/sources/destinations required. Restrict ports inbound/outbound to only services required. For cloud storage containers, prefer the use of "write once" identity/access controls where possible. Enable versioning for cloud storage containers. Minimise identity/access levels provided to cloud services to reduce the possibility of lateral movement.
	Network	<ul style="list-style-type: none"> Make sure you are using a firewall. Check your configurations and rules. Zero-trust architecture in place or separation of networks and access by subnetting. Use Access Controls (ACLs) to grant access on a need-to-know basis. Ensure there is a guest network to keep casual users off the main corporate network. Change default SSIDs and default passwords on Wireless Access Points and other networking devices. Remote access of the corporate network must be through a VPN




DETECT

	Key Deliverables	Controls
 	Threat Responder	Threat Response Team <ul style="list-style-type: none"> • Perform active threat hunting. • Check email gateway for alerts and threats. • Check NGAV dashboard for alerts and threats. • Check network perimeter looking for abnormally high intrusion attempts. • Check Active Directory (AD) to look for elevated user and/or matching account failed logins. • Look at newly installed, unauthorised applications or services on computer devices. • Look at File Server for large number of changed/alterd file extensions or automate with FSRM. • Engage a Managed Service Provider for additional expertise.
  	Automated Tools	Policy or tools to look for larger number of changes to files. <ul style="list-style-type: none"> • FSRM function (windows file server resource manager). • Altered file extensions. • High disk-write metrics. IDS/IPS and Layer 7 scanning <ul style="list-style-type: none"> • Ensure all possible UTM functions are active across all internet ingress/egress points to provide. Incident/Detection Alerting on Indicators of Compromise (IoCs) <ul style="list-style-type: none"> • Ensure automated alerting to appropriate persons is configured and active. • Log management tools such as SIEM to collate logs from various devices and services and tune/filter alerts. • Monitor cloud storage write container metrics, incremental backup sizes, CPU utilisation across fleet for anomalies and use metrics provided by the cloud platform for writes/utilisation as these cannot be faked or modified by an infected tenant.
	User Reporting	<ul style="list-style-type: none"> • Establish a process for users to report suspicious or anomalous behaviours in their devices, applications, or emails. • Implement phishing email reporting using tools that embed into the email client.

DETECT

	Key Deliverables	Controls
	Security Event Response Playbooks	<p>Use the scenarios identified in the Business Analysis in the Prevent phase and develop a set of incident response playbooks with procedures of how to respond to security events. Use the NIST Incident Response Framework for guidance on steps. Incident Response Playbooks should include:</p> <ul style="list-style-type: none"> • Named threat responders and their contact details. • Accountabilities and responsibilities of threat responders. • Clearly defined attack/threat types. • Containment strategies according to the threat type. • Eradication measures for each threat type.
	Isolation	<p>Isolate infected devices to contain the scope of infection and mitigate damage.</p> <ul style="list-style-type: none"> • Remove it from the network by unplugging. • Turn off any wireless functionality including Wi-Fi, Bluetooth & NFC.
	Investigate	<ul style="list-style-type: none"> • Check logs and Data Loss Prevention (DLP) tools for signs of data breach. • Locate any unidentifiable code & tools or files that may be related to the attack. • Look for unexpected large archival files containing confidential data. • Check mapped shared drives, mapped or shared folders on other devices, network storage devices, any connected peripheral storage devices such as external hard drives and thumb drives, connected devices such as phones and cameras, cloud storage platforms. • Attempt to identify the ransomware strain - some malware and ransomware is programmed to delete itself when it detects reverse engineering attempts.
	Eradicate	<ul style="list-style-type: none"> • Run scans on endpoints and utilise the EDR capabilities of NGAV to assist in eradicating the threat. • Research eradication steps for the specific threat - removal and decryption tools may be available online for older versions of malware and ransomware. • Use playbooks, tools, and security intelligence to implement eradication measures

DETECT

	Key Deliverables	Controls
  	Recovery Plan	Build a recovery plan into the Incident Response Policy appropriate to the critical systems impacted in a cyber response scenario, embracing the response steps to ensure no resurgence of the threat in the restored environment.
	Restore from Backups	<ul style="list-style-type: none"> • Ensure the integrity of your backups and that they have not be compromised by malware. • You may need to go back several months as often attackers can sit in your systems and compromise backups months before an attack is implemented.
	Fortify	<ul style="list-style-type: none"> • Ensure there is no APT or backdoor remaining in your environment to provide an attacker with re-entry point. • Determine the infection vector/entry point and implement measures and control to prevent future exploitation of the same vulnerability. • Implement further controls from the Defence Checklist if any are lacking.
	Report Data Breach	Contact the appropriate reporting authority if there has been a breach of the New Zealand Privacy Act 2020 (Data Breach) during the attack to notify the of the incident.

Want to understand your cyber risk profile and pave the way toward a defensible cyber posture?
 Visit www.minimumviableprotection.com today.

MVP

Minimum Viable Protection

A Capacitate Group Company

Let us take the pain out of policy and policy management and equip your users with cyber security defence skills.
 Visit www.cybertribe.co.nz for more info.

Cyber Tribe

A Capacitate Group Company