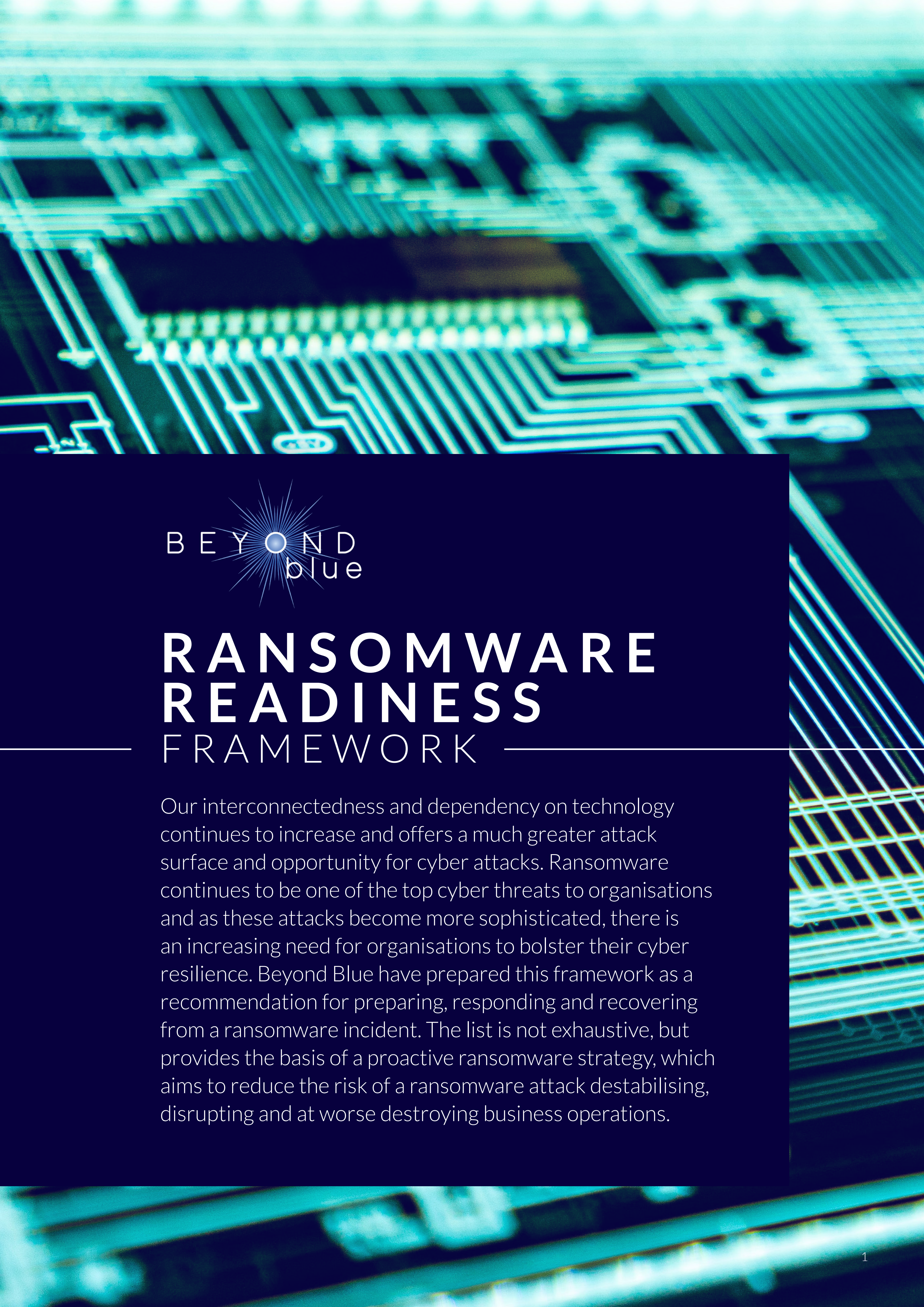
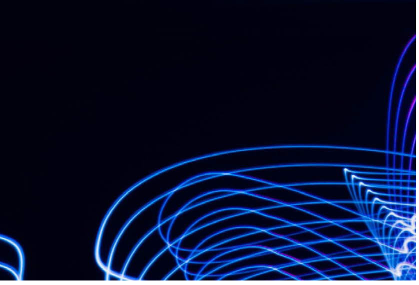


BEYOND blue

RANSOMWARE READINESS FRAMEWORK

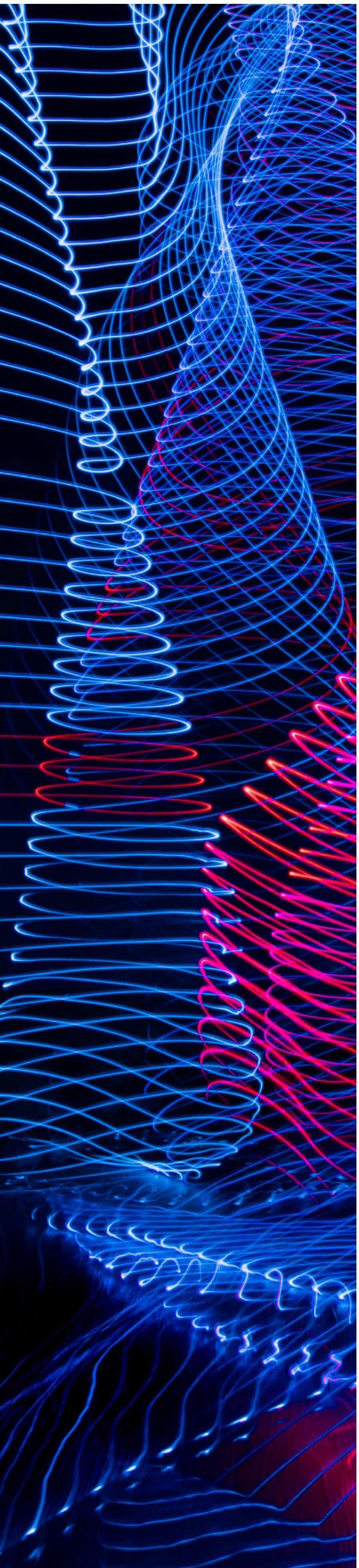
Our interconnectedness and dependency on technology continues to increase and offers a much greater attack surface and opportunity for cyber attacks. Ransomware continues to be one of the top cyber threats to organisations and as these attacks become more sophisticated, there is an increasing need for organisations to bolster their cyber resilience. Beyond Blue have prepared this framework as a recommendation for preparing, responding and recovering from a ransomware incident. The list is not exhaustive, but provides the basis of a proactive ransomware strategy, which aims to reduce the risk of a ransomware attack destabilising, disrupting and at worse destroying business operations.



PREPARE & PROTECT

WHAT TO DO BEFORE AN INCIDENT

OPERATIONAL CONSIDERATIONS



Understand the Threat: Leverage a mix of open-source tools and threat intelligence to align defence strategies to the continuously evolving ransomware methods and threats. Continuously monitor the threat landscape and undertake risk analysis to prioritise and benchmark the strength of existing security capabilities.

Create Policies: Develop and embed policies, procedures and agreements for incident response management and cyber security, including business continuity plans and disaster recovery. This will help build a secure culture and provide clear expectations to help your organisation run efficiently.

Build a Secure Culture: Engage and educate senior management and the Board on; cyber threats, the risk that poses to the organisation, roles in a ransomware incident, potential impacts, and methods like double extortion. Develop a mature education and awareness programme supported by tools and processes, to enhance end users' ability to spot and report anomalies. This should emphasise data classification and identifying phishing, and by extension ransomware incidents, to enable users to act as your first line of defence.

Resilience by Design: Define and embed principles within your Operating Model to help identify ways to design and build resilient systems and processes as they evolve.

Cyber Insurance: A cyber insurance policy could mitigate the impact of a ransomware incident and should be part of a layered approach to security, utilising your insurer's assessment process is a helpful opportunity to review and strengthen security controls. Organisations should not rely on cyber insurance to pay a ransom demand, but should expect that the insurer will cover the least expensive method of returning to BAU (which in some cases may go against your organisation's own ransom policy).

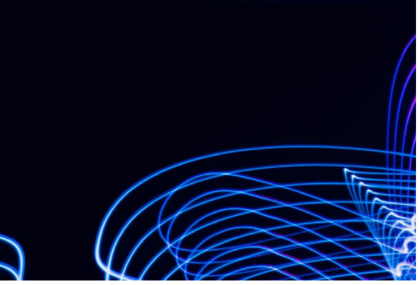
Create Plans & Playbooks: A crisis management plan will help develop a focussed response during an incident. Communications standards and guidelines will facilitate seamless communication during and after a crisis, including lines of internal and external communication. Consider your technical incident response teams to allow sufficient delegated authority, or direct communication lines to senior decision makers to make timely decisions to contain and mitigate overall impact.

Test Plans & Cyber Exercising: Regularly test your plans and incident response procedures, and personnel to practice your response in a safe environment and is a highly effective way to measure an organisations resilience. Consider a scenario based exercising program, which should also include critical suppliers to test and secure your supply chain.

Build Relationships: Build relationships internally and externally in areas you may require support during an incident e.g. system rebuilds, legal advice, forensics and case handling. Your cyber insurer should provide a list of trusted suppliers to proactively engage, including an approved ransom broker or negotiator to develop a ransomware negotiation strategy and to liaise with the attackers to achieve the best outcome for your business.

Supply Chain Management: Maintain oversight of your supply chain and managed service providers (MSPs). Document and regularly review contracts, policies and procedures to address security, integrity, resilience, and quality of your supply chain. Run proactive exercising with external support functions and consider reviewing relevant plans help identify, quantify and mitigate the risks involved in supply chains.

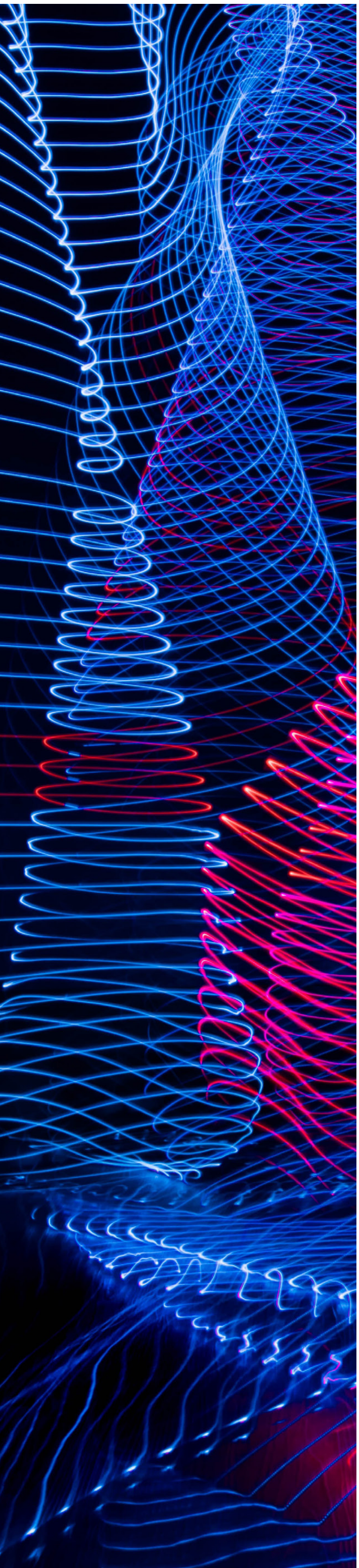
Recovery Order: Prepare a priority order of recovery to allow your critical systems and applications to be restored first after an incident. Consider any upstream / downstream dependencies between them that may need to be synchronised. Ensure to regularly test your ability to restore to confirm you could successfully recover.



PREPARE & PROTECT

WHAT TO DO BEFORE AN INCIDENT

TECHNICAL CONSIDERATIONS



Incorporate Threat Intelligence Feeds: Ensure accurate and relevant feeds from the analysis of strategic, tactical and operational threat intelligence reports are fed into triage, risk analysis, vulnerability management, and wider decision processes.

Assess Your Threat Detection Capability: Ensure your threat detection services and capabilities cover all your technical assets. You must also synchronise event feeds into a simple solution that allows analysts to efficiently detect and respond to threats.

Multi-Layered Defence: Take a multi-layered approach to better protecting your organisation. Consider segregating networks into separate subnets with appropriate protection around them to prevent lateral spread.

Data Classification and Encryption: Protect data using encryption at rest and in transit to prevent attackers being able to read sensitive data. Ensure the appropriate tagging and classification of your information and assets to protect and use them accordingly.

Asset & Configuration Management: Understand and inventory your organisation's IT assets, both logical (e.g., data, software) and physical (e.g., hardware) to manage patching and have fully documented configuration databases.

Backup: Develop an immutable backup strategy, ensuring you have encrypted backups offline and offsite to allow your data to be secure and rapidly available. Consider storing configuration databases in these secure locations in case of emergencies.

Environment Hardening: Improve the security baseline of your network and devices by utilising defence in depth and layering protection mechanisms. Consider deploying MFA, only allowing installation of authorised apps, secure RDP connections and following a zero-trust model to ensure user, device and application identities are verified before accessing the network.

Patch Management: Have an aggressive strategy to install patches to various device and application types as soon as possible, to protect against known vulnerabilities that ransomware could exploit.

Vulnerability Management: Zero-day vulnerabilities can be a difficult attack vector to monitor and so the approach must include correlating threat and vulnerability data from a variety of sources, identifying vulnerabilities that are actively being weaponised and ranking the most severe vulnerabilities for priority remediation.

DETECT & RESPOND

WHAT TO DO DURING AN INCIDENT

OPERATIONAL CONSIDERATIONS

Internal Communication: Assume the attackers still have access to the compromised network and could intercept communications. Establish secure means of communication with internal responders and response partners e.g. a secure platform, phone calls and secure messaging services that aren't connected to the network.

External Communication: Draw on your communications plan and deliver the necessary messaging to external parties, including customers and suppliers. Continuously assess the impact of the incident and notify as appropriate. Consider what content is delivered, when and by who to ensure a timely and appropriate delivery to mitigate impact to customers,

Reporting: Report to relevant competent authorities and consider any regulatory, legal and ethical responsibilities, including notification to authorities, regulators and customers of a data breach. You may wish to utilise authorities for additional support during the incident or assist with their investigations (e.g. cyber crime) by providing available evidence and updates, depending on the needs of your business. Where relevant, report to your insurance company to raise a claim and complete any Impact Assessments.

Ransomware Negotiation Strategy: Engage your Cyber Insurers to discuss available options and avoid contacting the attackers directly. If considering paying the ransom contact previously agreed external expert support (including incident response, negotiators/brokers, communications support and expert legal advice) who can assist with responding and negotiating on your behalf. Ensure evidence is presented by the attackers to prove their ability to decrypt the data if you decide that's the route you are taking

Disruption to Customers: Follow business continuity plans initiating manual workarounds or substitutions where possible to continue a minimal level of service to customers.

Crisis Management Structure: It's crucial the crisis management team follow assigned responsibilities to ensure minimal disruption to customers and business operations to return as quick as possible. For instance; bronze level to focus on operational issues including containment of the attack, silver level to focus on the tactical issues ensuring continuity of operations and gold level to focus on the strategic decision making to mitigate customer impact and forward planning to anticipate future risks.

Intel Sharing: Join and utilise external intelligence platforms e.g. CiSP to provide and extract information that could assist in investigative steps ahead of responding to a ransomware incident e.g. known recovery keys.

DETECT & RESPOND

WHAT TO DO DURING AN INCIDENT

TECHNICAL CONSIDERATIONS

Defensive Tooling: Combine and monitor defensive tooling solutions to get visibility of endpoints and network traffic to detect and identify indicators of ransomware allowing you to continuously detect and respond to attacks.

Monitor and Analyse logs: Utilise SIEM data for detecting anomalies in user behaviour or system activity on your network. Ensure you can collate activity logs from multiple devices into a simple solution that is efficient for analysts to detect and respond to threats

Containment and Isolation: Isolate infected networks or endpoints and where applicable switch-off to prevent a further attack from the same vector, or by deeper internal propagation of the infection.

Authentication Protection: Have an action plan to efficiently tackle forced mass credential resets or account disablement for customers and employees alike to allow any stolen credentials to be managed rapidly.

Incident Response / Blue Team: Rapidly deploy trained personnel to identify and triage what is infected, contain any lateral spread and isolate clean parts of the network where possible.

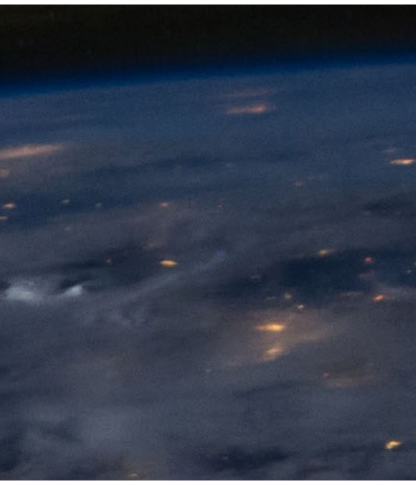
Check for Decryption Keys: As well as checking intelligence sources, utilise websites such as https://www.nomoreransom.org/ where certain known ransomware decryption keys are recorded.

Secure and Preserve Evidence: This will be required by the authorities to investigate cyber crimes, with an aim to identify suspects, bring offenders to justice and disrupt criminal activity.

RECOVER

WHAT TO DO AFTER AN INCIDENT

OPERATIONAL CONSIDERATIONS



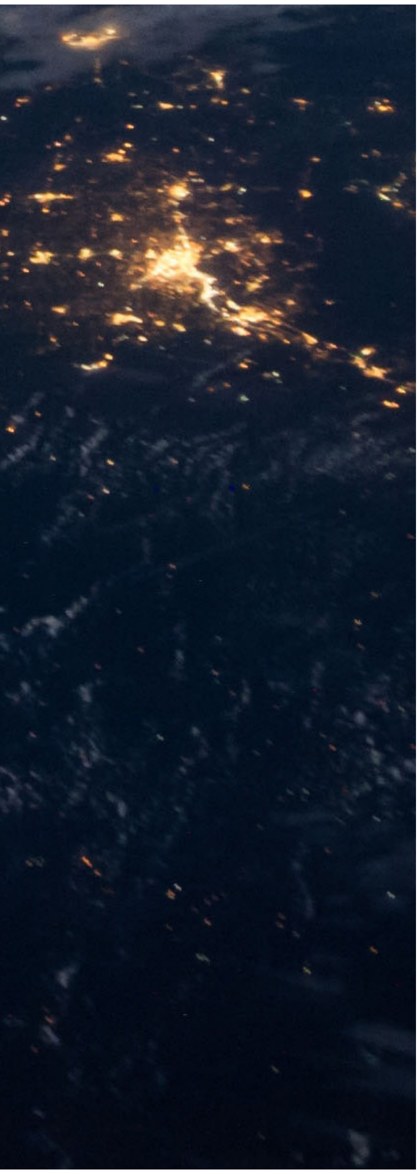
Investigations: Support any ongoing law enforcement and internal investigations. The evidence you present may identify offenders who could be brought to justice.

Lessons Identified: Complete a post incident review and learn from findings. Take further action to prepare and strengthen defences against future attacks.

Share Lessons: Share experience and lessons identified internally and across industry as appropriate to help prepare others.

Return to Business as Usual: Recover and process any backlog created during the incident and aim to return to full business operations. Consider actions required to indemnify any customers/stakeholders that have been impacted and repair any damage to reputation.
Take this opportunity during your recovery strategy to rebuild stronger to reduce the risk of another cyber attack e.g. fast-track any upcoming change programmes, digitisation projects and migrating from legacy infrastructure.

TECHNICAL CONSIDERATIONS



Forensic Analysis: Undertake relevant forensic activity to understand entry points, timelines and malware information building an end-to-end understanding of the incident.

Remain vigilant: Monitor for any signs of further re-infection such as malicious data loss, change or corruption (if not recovering from safe back-up).

Utilise Recovery Order: Follow plans to recover business applications and systems in priority order and consider the upstream/downstream dependencies to ensure correct synchronisation on restore.

Backup and Restore: Action your IT disaster recovery plan, where possible restore from a recent clean backup on clean operating systems.

Endpoint Rebuild: Utilise your playbooks to rebuild your endpoint estate on mass.

Lessons Identified: Complete a post incident review and learn from findings. Take further action to PREPARE and strengthen defences against future attacks.

GLOSSARY

Attack Vector – A method used by the attacker to gain unauthorised access to a network or system and can include phishing attacks, vulnerability exploits and compromised credentials.

Blacklisting – An access control mechanism to add certain elements e.g. email, websites (URLs), IP addresses etc, to a list to deny access to them

Business Continuity Plan - A documented procedures that guides an organisation to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

CiSP (Cyber Information Sharing Partnership) – A forum for exchange cyber threat information in real time, in a secure, confidential and dynamic environment. It is a joint industry and government initiative set up to increase situational awareness and reduce the impact on UK business from cyber crime.

Cyber Exercising - Cyber incident exercising helps organisations establish how resilient they are to a cyber incident and to practice their response in a safe environment. An exercise can be run using different methods such as a table-top, or live play.

Data at Rest – Typically covers data being stored on a computer, or in a stable destination that is not in use, or travelling.

Data in Transit – Typically covers data that is actively in motion between its source and intended destination on a computer network usually across the internet, within a private network, or from one device to another.

Disaster Recovery Plan (IT DR Plan) - A clearly defined and documented plan which recovers IT capabilities to an acceptable level within a predetermined period of time following a disruption.

Double Extortion – An evolving method of ransomware being used more frequently where the attackers exfiltrate sensitive data and then threaten, or actually do, publish the data online that they have gained access to, as well as encrypt it on the victim(s) computer systems.

Education & Awareness Programme – Cyber security awareness, training, and education provides the organisation and colleagues to understand, recognise, prevent, and respond to security incidents. This can be delivered in various formats including mandatory training, group sessions and presentations, one-to-one advice, gamification and leaflets.

Encryption – Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information.

Forensics - Identify, preserve and extract information as evidence for an incident (that involves electronic devices) that can be used to identify the point of entry and attackers. Analyse the data or system to gather detail to help better prepare to future incidents.

Immutable Backup – An immutable backup can't be encrypted, modified or deleted and aids successful recovery in a ransomware incident.

Integrity – "The quality of being honest and having strong moral principles that you refuse to change". Within cyber this refers to the accuracy and completeness of data, ensuring it is maintained through security controls and is not modified, misused or removed by unauthorised users.

Lateral Spread – The ransomware has been designed with the ability to move through the network and infect all computers

Least Privilege Model - Information security principle of least privilege asserts that users and applications should be granted access only to the data and operations they require to perform their jobs.

Managed Service Providers (MSPs) – An MSP is a third-party company that remotely manages a set of IT processes on behalf of its clients.

MFA (Multi-Factor Authentication) – A process of verifying who you are when signing into your online accounts. Traditionally authentication as achieved with a username and password, adding MFA (or 2FA) allows you to increase the security and add two or more pieces of information to verify (something you are – biometrics, something you know – security question, something you have – one-time passcode on your authenticator app or text message)

Open Source – Information that is publicly accessible.

Patch Management – A continuous process of notification, identification, deployment, installation, and verification of operating system and application software updates. A patch (update) is released to fix known vulnerabilities, errors or bugs and should be deployed as reasonably practicable.

Phishing - Phishing can be performed via a text message, social media, or phone, but the term 'phishing' is mainly used to describe attacks that arrive by email and is a method very commonly used to deploy ransomware. Attackers will impersonate someone, or an organisation in attempt to tricking you into doing the wrong thing, such as giving away personal information or opening a malicious like or file.

Ransomware – A type of malware (malicious software) delivered onto a victim(s) computer system by an attacker gaining access into the network. This software, or 'payload,' then makes the data unavailable through encryption or deletion. Ransomware is often designed to spread from device to device to maximise the number of files it can encrypt. A 'ransom' note is usually left by the attacker requesting payment (usually in cryptocurrency) in return for restoring the data with a decryption key that generally only the attacker can access.

Recovery Key – A unique identifier assigned to help regain access to your files or systems in a ransomware incident

RDP (Remote Desktop Protocol) – A secure network communication tool designed for remote management and access to virtual desktops, applications and servers.

Security Controls – Should be implemented across organisations to help protect data and infrastructure and can include physical controls (surveillance cameras), digital controls (MFA), cyber security controls (intrusion prevention systems) and cloud controls (measures for data protection).

SIEM (Security Information Event Management) – Can assist organisations in identifying potential threats and vulnerabilities before they have a chance to disrupt business operations

Subnets – A smaller section of a larger network

Threat Intelligence – Known information that can gathered to understand the threats an organisation has, or will face, this information can be used to strengthen defences.

Zero-Day Vulnerabilities – A flaw in the software or hardware that isn't yet known to the developer, supplier or those interested in the security, therefore does not have a patch available and has been exploited by an attacker.

Zero-Trust Approach – Build a strong Identity and Access Management (IAM) model whereby all users must be verified they can be trusted before gaining access to the network and being assigned any access rights.