Ransomware Readiness

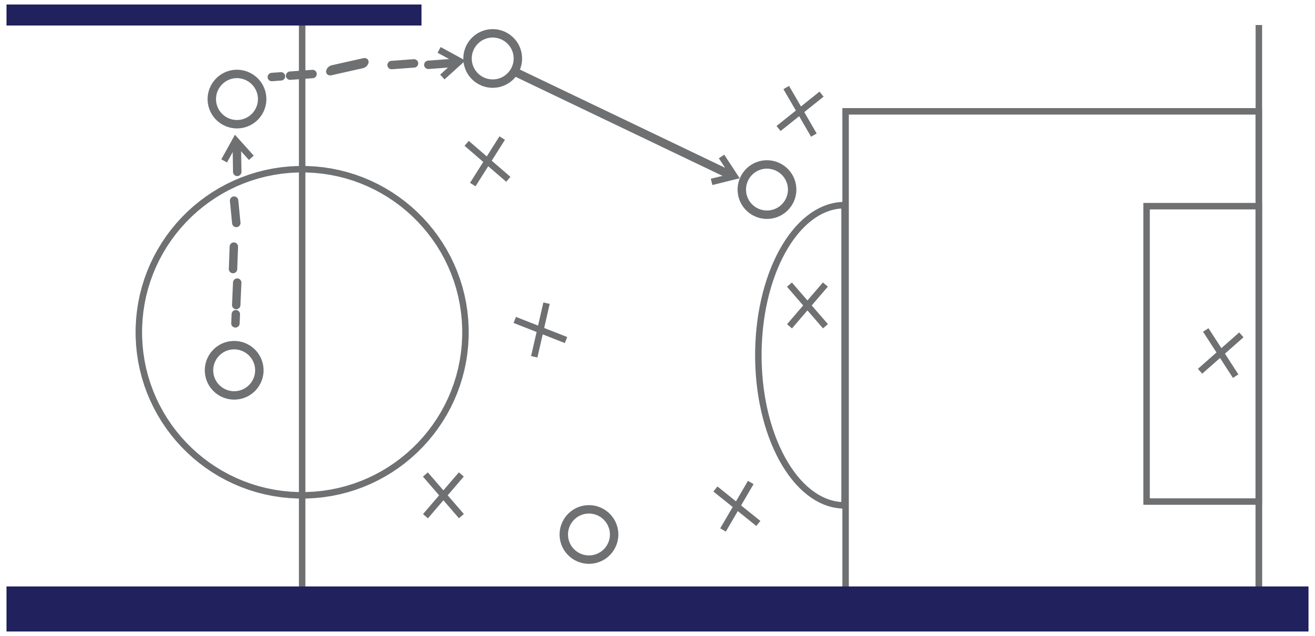
THE PLAYBOOK

How to Get Defence Ready

risk crew

Shelter from the Storm

CONTENTS



The Threat Landscape

THE PLAYING FIELD

We are all playing in the digital era that comes with cyber threats. There's no avoiding the game, but if you have a good understanding of the threat landscape, you can up your game significantly. To understand exactly what you are up against, you must know your opponents, their tools and the plays they run.

Ransomware is a form of malware (malicious software) used by threat actors (cybercriminals) designed to encrypt data on the system it infects by rendering it inaccessible to its users. It's that simple. Cybercriminals then demand a payment (ransom) in exchange for a decryption key to unlock the data. Delivered through unprotected attack vectors (paths to the target systems) this malware can have significant effects on a business as the average downtime associated with an attack is around three weeks.

A ransomware infection can severely impact business processes simply by denying it access to the data needed to operate and deliver mission-critical services. Additionally, most cybercriminals have started to include threatening to publicly "name and shame" the business if they refuse to pay the ransom demanded as a secondary form of extortion. Consequently, ransomware can pose both a financial and reputational threat to the business.

While ransomware has been around for quite some time, it has considerably evolved over the last several years becoming much more sophisticated — making it more difficult to identify and prevent. Additionally, malware has become commoditised and more accessible and easier to use by less-skilled threat actors.

While both of these factors are responsible for ransomware's dramatic rise on the cyber threat landscape, the plain fact is that it's a quick, effective, and extremely lucrative for cybercriminals today — and it's becoming more and more profitable.

The National Security Institute reported that the average ransom demanded for a decryption key rose from $5,000 in 2018 to $2,000,000 in 2021.

Moreover, ransomware infections have become both more destructive and impactful in nature and scope. Once inside the target systems, cybercriminals will move laterally across the systems to locate the most critical information assets for encryption or to ensure the ransomware propagates itself across entire networks for maximum effect. They will also attempt to delete system backups, that make restoration and recovery more difficult or infeasible for the business.

11 seconds

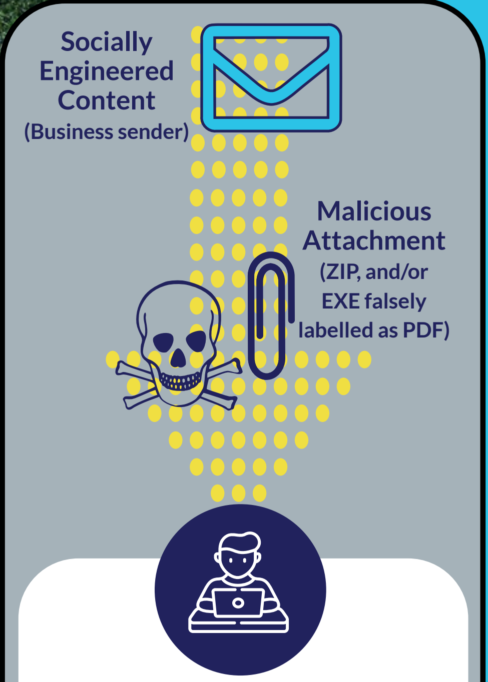
A RANSOMWARE ATTACK OCCURRED EVERY 11 SECONDS IN 2021.

The Attack Vectors

KNOW YOUR OPPONENTS

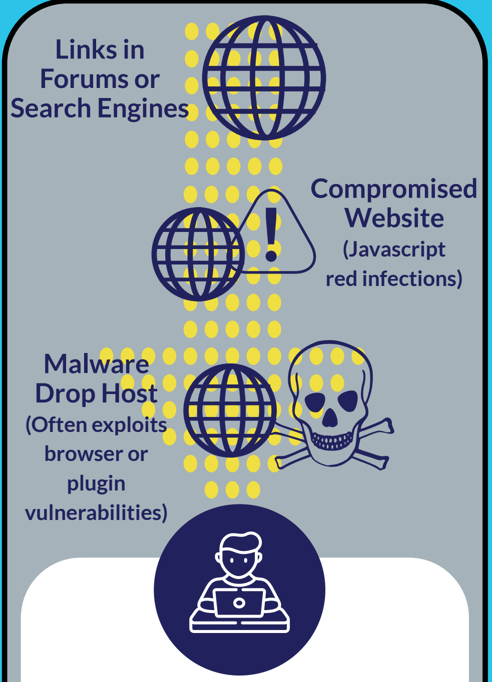
The first step in developing a survival and readiness strategy is to understand the attack vectors.

3 Common Attacks


Socially Engineered Content
(Business sender)
Malicious Attachment
(ZIP, and/or EXE falsely labelled as PDF)

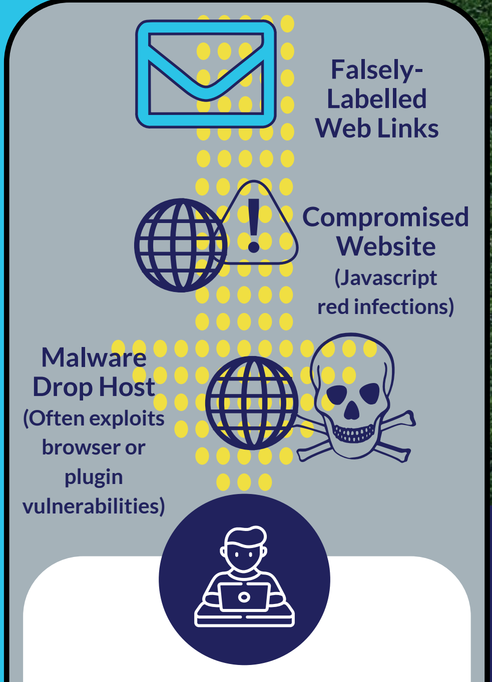
Email Only

Ransomware software is attached to an unsolicited email and sent to the users of the targeted systems through phishing or other social engineering methodology. Downloadable files then execute the malware which encrypts the host system.


Links in Forums or Search Engines
Compromised Website
(Javascript red infections)
Malware Drop Host
(Often exploits browser or plugin vulnerabilities)

Web Only

Redirect links are placed in established chat forums, social media platforms or search results that take end-users to bogus websites to infect systems through the user's browser or plugin vulnerabilities.


Falsely-Labelled Web Links
Compromised Website
(Javascript red infections)
Malware Drop Host
(Often exploits browser or plugin vulnerabilities)

Email to Web

The end-users receive unsolicited emails that contain malicious links to a compromised website to infect systems through user's browsers or plugin vulnerabilities.

While these are the 3 most commonly used attack vectors associated with users, ransomware can also infect target systems through video conference applications, instant messaging or removable USB drives — any activity that allows a user to download an executable file.

Following the initial infection, the ransomware may be programmed to try and spread itself across the network to shared drives, servers, attached computers and other accessible systems.

Additionally, cybercriminals can infect systems with ransomware through any "attack vector" that allows them to manually upload the ransomware software.

Internet-Facing Vulnerabilities or Misconfigurations

Cybercriminals will exploit security vulnerabilities in the external-facing hardware or software to gain access to business systems and execute the ransomware.

Third Parties or Managed Service Providers

Cybercriminals will also exploit security weaknesses associated with trusted third parties or service providers with connectivity to the target systems to execute the ransomware.

Once they obtain access through any of these vectors, cybercriminals will attempt to locate and encrypt backups maintained on the target systems to invalidate them for purposes of recovery. Alternatively, they may include building in periods of gestation or dormancy into the malware, so it gets backed up along with legitimate data — ensuring it cannot be used for recovery.

Ransomware is not an industry-specific problem. All businesses are at risk and should ensure they are adequately prepared. If you are not prepared, ransomware can and will significantly disrupt and damage your business.

The Anatomy of an Attack

OPPONENTS' STRATEGIES

Cybercriminals are getting increasingly sophisticated in how they identify and infect systems, avoid detection and thwart ransomware decryption efforts. When developing your ransomware prevention strategy consider the following trends.

Big Game Hunting

Spray and pray methods are starting to be replaced by big game hunting, where one big target, such as a centre hub or distribution central large is infected for a substantial ransom. Ransomware is starting to be custom-built for a specific target to insure the greatest impact and higher likelihood of success.

Blended Campaigns

Many organised cybercriminal organisations and Nation State threat actors are starting to blend cryptocurrency mining with ransomware campaigns to both generate revenue and create a distraction from other threat campaigns being launched.

Wiperware

Ransomware is increasingly being used as a distraction to cover up other more serious attacks. While the attack looks like ransomware the actual goal of the threat actor is to distract the organisation from other security events happening on the network and delete breadcrumbs of the ancillary attack. The hope of the attacker is that the organisation is so relieved to have recovered from ransomware that it doesn't investigate further.

Public Exposure

Ransomware attacks have taken an unwelcome turn as attackers have started to leak the victim's files as a way to exert additional pressure to pay the ransom. With such an escalated attack, victims now need to be concerned both about recovering their encrypted files and what would happen if their stolen unencrypted files were leaked to the public.

Intelligence Gathering

Ransomware crime groups are starting to spend more time gathering intelligence on their targets. In addition to penetrating the network and performing reconnaissance, threat actors study SEC filings for an organisation's financial position and use the information to scale ransom demands.

Tactical Trend

Increased Impact

Attacks are evolving to both increase the impact and thwart recovery attempts by the victims by encrypting the hard drive and master boot record, or attacking shared network drives or files stored in Infrastructure as a Service (IaaS) applications or collaboration tools.

Tactical Trend

Increased Stealth

Cybercriminals are lengthening their attack cycles to make it more difficult to detect. They slow down the encryption process by spreading it out over a longer amount of time or randomising the process instead of encrypting in a linear fashion. They are also delaying attacks by lying dormant for a period of time before activating the malware, using polymorphic code that changes or deploying multi-threaded attacks that launch differing processes.

Tactical Trend

Managed Service Providers (MSPs)

Managed service providers are a growing target for ransomware attackers. An attack on an MSP has the potential to devastate virtually any business. By exploiting vulnerable security systems typically seen in resource-constrained service providers that manage multiple businesses and municipalities, attackers can get economies of scale and exert pressure for payment.

Trend Increase

Cloud Services Providers

Ransomware writers are now targeting cloud service providers with network file encryption attacks as a way to hold hostage the maximum number of customers possible. The fallout from ransomware attacks against cloud service providers is devastating as the business systems of every cloud-hosted customer are encrypted.

Trend Increase

The Players

WHO'S IN THE MATCH

The ransomware attacks you read about are not as simple as they seem. The process and players that comprise a typical attack have been distilled down to their simplest form by the media to ensure public consumption.

Ransomware attacks are extremely complex and can involve multitudes of different players on both sides of the attack. Here's an overview of the most significant players.

The Hackers

The first step in any ransomware attack is for the attacker to get access to the target network. This can be done through social engineering, exploiting vulnerable attack vectors or simply by purchasing stolen passwords from the dark web. It's important to understand that the attackers who initially breach the network are not always the ones who infect it. Upon penetrating a network, attackers sell their access to other cybercriminals specialising in ransomware infections.

The Suppliers

Ransomware is a cottage industry supported by a sub-economy of organised cybercriminal gangs that design and develop malware to infect and encrypt its target. While these cybercrime gangs will often execute the attacks themselves, they also sell the ransomware to independent actors as a means of producing an additional revenue stream. This "Ransomware as a Service" (RaaS) business model has exploded in the last several years accounting for more than half of the illegal revenue generated in the market.

The Infectors

Upon getting access from the original hackers who penetrated the network and obtaining the ransomware software, the infectors will enter and conduct reconnaissance of the target network. (Infectors can be the original Hackers, Suppliers or an entirely different threat actor.) Infectors can take anywhere from a few hours to a few months, to assess the network and identify the most lucrative target for encryption. Once identified, the Infectors will infect and encrypt it with malware and demand a ransom from the victim for the decryption keys.

The Muscle

If a business initially refuses to pay the ransom, attackers often hire a separate criminal group to intimidate them and get them to pay. This group is known as the Muscle whom works for a percentage of the ransom. Tactics used by Muscle groups include threatening public disclosure of the breach, sending emails to employees and clients, or even placing calls to the victim's partner and supplier connections — threatening to infect them.

The Responders

The first step for the business is to trigger its incident response plan and rally the team (Responders) to examine, contain, and attempt to remove the infection and identify root cause. This is often an outsourced supplier with the skills and tools required to assess the infection, recommend recovery options and remedial actions. In the event, that a decision to pay is made by the victim business, Responders may facilitate the payment and apply decryption key if received.

The Lawyers

A victim business' next reaction is usually to contact their legal team for advice on all of the legal issues associated with the breach. The business is usually overwhelmed with answers to questions they may never have considered such as the following. What compliance requirements were violated? What are the legal consequences of the breach? Who needs to be informed and when? Should payment be made? Would payment violate local law? What legal costs may be associated with recovery?

The Insurers

If the victim business decides to pay the ransom, Insurers may cover some or all of the costs depending on the coverage (assuming they have insurance). Some insurers will actually facilitate the ransom payments directly through established bitcoin accounts. Claim limitations, notification and filing procedures must be clearly understood. Often, large organisations will "stack" policies to ensure they are covered for large (multi-million pound) ransoms.

The Disinfectors

Once the ransom is paid, victims receive a digital key to decrypt the infected target and recover access. However, regaining access is a lot like coming home after being robbed. Files may be missing, incomplete, not where they were previously located, and software or services may not work as they should. As a result, victim businesses often turn to outsourced recovery professionals to ensure full decryption and reinstatement is achieved.

The Mixers

Ransom payments made by a victim business are usually transferred straight into a standard cryptocurrency wallet. Cybercriminals will then engage a "Mixer" to launder that cryptocurrency. A Mixer blends and mixes the victims payment with other digital currency coins to conceal/obscure the source and destination of the ransom payment to avoid detection and tracing by law enforcement. Mixers provide the service for a percentage of the ransom amount.

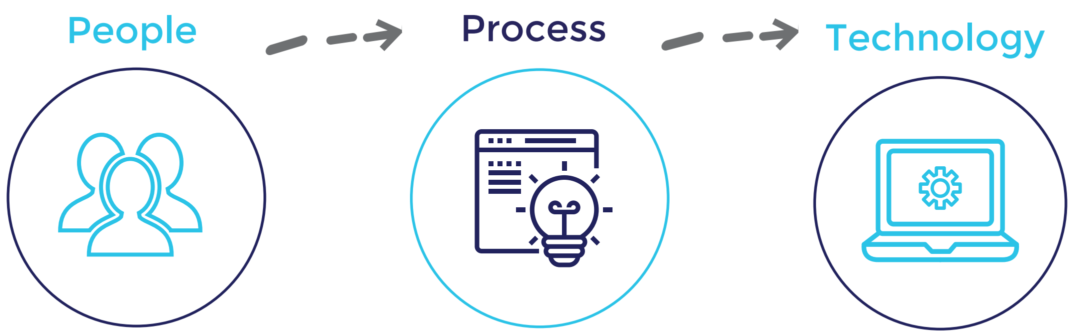
This is a simplified overview of the players typically involved in a ransomware attack. But ransomware attacks are never simple. Ransomware is a growth industry and has become extremely lucrative for cybercriminals. Therefore, your hostage prevention strategy should include this factor and expect that attacks will increasingly become more commoditised, sophisticated – and so more complex. Sadly, it will get worse before it gets better.

The Best Practices

STRENGTHENING YOUR DEFENCES

When it comes to ransomware, prevention is your best defence. Businesses that rigorously practice the fundamental principles of information security risk management, significantly reduced their risk of infection. They are called "fundamentals" for a reason — they work.

To reduce your risk of ransomware, we recommend implementing the following practices in your people, process and technology.



People

Process

Technology

People

Phishing is the most used ransomware attack. As discussed, threat actors use bogus links, attachments, or both to trick users into taking some sort of action that will download and enable the ransomware infection. **Consequently, people constitute your biggest risk of succumbing to ransomware.** Therefore, when it comes to mitigating this risk, knowledge truly is power. It is crucial to educate your users about the dangers of phishing emails so they can be your business's first line of defence.

This of course, is best done by implementing a formal cyber security awareness programme, explaining the methodology and objectives of phishing attacks, and most importantly – how to identify and respond to one. Also, it is best practice to **conduct simulated phishing attacks against your staff routinely to verify their understanding of the threat.** You can also prevent phishing emails from reaching end-users by enabling strong spam filters.

Good cyber security awareness programmes not only reduce the risk of phishing but improve the business's overall security posture and can significantly enhance incident identification, reporting and response times, minimising impacts in the event of an infection.

It's critical to **provide training to the incident response team members or stakeholders — tasking them with responding to a ransomware attack to ensure they possess the knowledge, skills and tools required to address the infection.** Conduct simulated ransomware infections to test response teams capabilities and adequacy of your existing incident response plan.

> Education is as close gets to a 'silver bullet' for ransomware. Invest in your people for the greatest return.

Process

Ensure you maintain offline, encrypted backups of your business data and regularly test these backups to ensure their accuracy. Backup procedures should be conducted routinely and maintained offline as many ransomware attacks attempt to locate and delete or encrypt accessible backups. This practice is crucial and can make the difference between recovery and disaster.

Make sure your business implements and maintains good cyber incident response, business continuity and disaster recovery plans with clear and current communications plans. Your incident response plans should specifically include response and notification procedures for ransomware incidents. Business continuity and disaster recovery plans should specify how to operate if you lose access or control of critical business functions.

Identify and mitigate your internet-facing vulnerabilities and misconfigurations to the reduce risk of actors exploiting the attack surface. This is best accomplished through conducting routine security vulnerability scanning and exterior-facing security penetration testing of your exterior-facing systems.

Ensure your business' cyber insurance coverage addresses ransomware attacks and is fit for purpose given your defences.

Technology

Deploy Multi-factor Authentication (MFA) for all services possible, particularly for webmail, Virtual Private Networks (VPNs) and accounts that access critical systems.

Implement best security configuration practices for use of Remote Desktop Protocol (RDP) and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services to then later spread the ransomware. Begin by auditing your network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply MFA and log RDP login attempts. These simple configuration practices have profound results in preventing ransomware attacks.

Ensure you continually update software, including operating systems, applications and firmware as soon as updates are issued. Prioritise patching of critical security vulnerabilities on internet-facing servers and software processing internet data, such as web browsers, browser plugins and document readers. If you can't do this immediately, implement any vendor-provided temporary mitigations.

Ensure that all devices connected to the network are properly configured and all applicable security features are enabled. Disable any ports and protocols that are not being used for a business purpose. Less is more. It's a good practice to disable or block inbound and outbound Server Message Block (SMB) protocols and remove or disable outdated versions of SMB.

Practice good cyber hygiene by ensuring antivirus, anti-malware software and signatures are implemented on critical systems and kept up-to-date. It's good practice to implement application "allowlisting". Make sure that user and privileged accounts are limited through account use policies, user account control and privileged account management.

> Implementing and adhering to these fundamental practices is your best defence in managing your risk of ransomware.

The Readiness Checklist

PREPARING FOR THE GAME

Whether you are an SMB or enterprise-level organisation, and no matter what industry, it's vital that you are prepared for ransomware attacks. This readiness checklist includes basic practices for protecting against ransomware attacks. We do recommend consulting an expert if one is available to you.

✓

- □ Staff have received information security awareness training explaining how to identify and respond to a phishing attack within the last 3 months.
- □ Staff have been instructed on how and where to report security incidents.
- □ Staff have been subjected to simulated phishing attacks within the last 3 months.
- □ Incident Response Team members have received ransomware response training.
- □ Set up a crypto wallet.
- □ Backups are routinely conducted, encrypted and maintained offline.
- □ Backup and backup procedures have been tested for accuracy.
- □ Incident Response Plans and procedures are in place and have been tested within the last 6 months.
- □ Business Continuity Plans and procedures are in place and have been tested within the last 6 months.
- □ Disaster Recovery Plans and procedures are in place and have been tested within the last 6 months.
- □ Internet-facing vulnerabilities & misconfigurations identified in routine vulnerability scanning & security penetration testing have been identified and mitigated within 5 days of discovery.
- □ Cyber insurance policy is reviewed for applicability, aligned to critical business assets & recovery objectives.
- □ Strong spam filters are deployed on mail services and end clients.
- □ Multi-factor Authentication (MFA) is deployed for access to all services (to the highest extent possible), particularly for webmail, Virtual Private Networks (VPNs) and accounts that access critical systems.
- □ Standard security builds are established and maintained for all devices connected to the network.
- □ Remote Desktop Protocol (RDP) and all other remote desktop services have been removed and are only allowed by approved sessions.
- □ Change Management procedures are established and implemented.
- □ Software, operating systems, applications and firmware are updated immediately following their release, prioritising the patching of critical security vulnerabilities on internet-facing servers and software processing internet data, such as web browsers, browser plugins and document readers.
- □ All network connected devices are properly configured & all applicable security features are enabled.
- □ Ports and protocols that are not being used for business purposes are disabled.
- □ Inbound and outbound Server Message Block (SMB) protocols have been removed, disabled or block if not required for a critical business function.
- □ Antivirus, anti-malware software & signatures are implemented on all critical systems & kept up to date.

The Response Checklist

REMEDIATION STRATEGY

In the event of a ransomware infection, you would of course immediately implement your existing cyber security incident response plans and procedures would typically include the following practices.

- □ Immediately secure system operations to stop additional data loss.
- □ Determine which systems were impacted and immediately isolate them. If several systems appear impacted, take the network offline at the switch level. If taking the network temporarily offline is not immediately possible, locate the network (e.g. Ethernet cable) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- □ If affected devices cannot be removed from the network or the network cannot be temporarily shut down, power infected devices down to avoid further spread of the ransomware infection. Note: this step should be carried out only if necessary because it may result in the loss of infection artefacts and potential evidence stored in volatile memory.
- □ Triage impacted systems for restoration and recovery. Prioritise based on criticality.
- □ Confer with your team to develop and document an initial understanding of what has occurred based on preliminary analysis.
- □ Engage your internal and external teams and stakeholders to inform them of how they can help you mitigate, respond to and recover from the incident. Strongly consider requesting assistance from a reputable third-party incident response provider with experience in data breaches.
- □ If no initial mitigation actions appear possible, take a system image and memory capture of a sample of affected devices.
- □ Collect any relevant logs as well as samples of any “precursor” malware binaries and associated observables or indicators of compromise.
- □ Do not destroy forensic evidence and take care to preserve evidence that is highly volatile in nature — or limited in retention — to prevent loss or tampering.
- □ Implement notification requirements as outlined in your cyber incident response plan.

THE ESSENTIAL RESOURCES

CISA.gov – Cyber Security Evaluation Tool (CSET®)
https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

National Cyber Security Centre (NCSC) – Security Information for Small and Medium Organisations
https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations

NCSC Early Warning Service
https://www.ncsc.gov.uk/information/early-warning-service

How and When to Report a Ransomware Incident to the ICO
https://ico.org.uk/media/for-organisations/documents/2614816/responding-to-a-cybersecurity-incident.pdf

Game On

READY TO PLAY?

Now you have the entire picture of what and how ransomware is and how it works, it’s time to start protecting your business.

It can be a daunting task of knowing where to begin but the Crew is here for you. Whether you have an information risk management programme in place or are just getting started.

Risk Crew provides a full portfolio of services to help you mature your cyber security programme.

Not sure where to begin? Give us a call. We are happy to chat with you to assess your needs.

Ransomware Readiness Audit

Information Risk Management Services

Information Security Policies

Staff Awareness Training

Cyber Essentials Certification

ISO 27001 Compliance

ABOUT RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

☎ +44 (0) 20 3653 1234
riskcrew.com
info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom