YOUR RANSOMWARE

SURVIVAL GUIDE

KALARA®

TABLE OF CONTENTS

What is Ransomware?

Ransomware is a type of malware, or malicious software, that hackers launch to disable or limit an organisation's access to its data until a ransom is paid. The hackers then instruct the organisation on how to pay the ransom in order to release the decryption key that will allow the company to decrypt the data and potentially gain access to its files, databases and applications.

Ransomware attacks are rapidly increasing, generating substantial revenue for cybercriminals and causing significant damage to businesses and government bodies. Attack groups are constantly adapting and evolving their tactics, devising new ways to extort ransom from victims. As long as these gangs can extort payment from businesses, ransomware attacks will continue to escalate.

To combat this, businesses like yours need to develop a solid cyber defence strategy to minimise the risk and mitigate the impact of ransomware so that they can recover quickly if their systems are compromised.

Attack methods used by cyber criminals

When you understand how ransomware attacks work, including the tactics used by cyber criminals, you can lower your chances of falling victim to them. Listed below are a few popular methods hackers use to launch ransomware:

Email phishing

Email phishing is a social engineering attack designed to entice targets into clicking on a link in an email that leads to a hacker gaining access to your network or sensitive information. In most cases, attackers are interested in stealing account credentials, personally identifiable information (PII) and company trade secrets.

Unsecured RDP ports

Hackers gain direct access to a server or computer by scanning the network and discovering open RDP ports that have not been adequately secured. Attackers aim to gain complete control over a system, obtain credentials or unleash malicious code on a target.

Software/patching vulnerabilities

Software vulnerability is a flaw or weakness in software that compromises the overall security of the system. A data breach or system attack can easily cost businesses millions of dollars in compromised files, operational challenges, system fixing and maintenance.

Malicious websites

Cybercriminals create malicious websites to steal sensitive data or plant malware, such as ransomware on victims' computers. These websites often spoof legitimate sites and lure visitors with phishing emails.

Pop-ups/ads

Pop-ups may appear in your browser due to adware that you might have accidentally downloaded, possibly by clicking a malicious advertisement. Another possibility is opening an attachment or clicking on a link in an email containing adware.

Ransomware trends

Ransomware gangs continuously rethink and upgrade their techniques as new technologies emerge and more businesses try to protect themselves against attacks. Here are a few of the latest techniques ransomware gangs and their affiliates use to target their victims.

Supply chain attacks
To maximise the attack radius and impact, threat actors target weak links in supply chains, threatening not only a single business but also an organisation's entire ecosystem.

Double extortion
Hackers not only encrypt the data, but also steal it and threaten the victim to release it unless a ransom is paid.

Ransomware-as-a-Service (RaaS)
Ransomware is big business and has adopted the same type of business models that existing in legitimate business markets. Affiliate cybercriminals secure access to a subscription-based platform that contains all the ransomware code and operating infrastructure needed to run ransomware attacks.

Increased attacks against small and midsize businesses
High-profile prosecutions of cybercriminals has seen a shift in criminal behaviour from high-profile hacking to targeting midsized businesses to evade public scrutiny. Enforcement agencies have seen a shift in criminal behaviour from targeting large corporates to midsized businesses. Mid-sized businesses will tend to have less protection and could be easier to secure a ransom from.

Impacts of an attack

The impact of a ransomware attack can be devastating for your business in multiple ways:

Extended downtime:

As you deal with an attack the downtime in your IT infrastructure could be very costly and impact your ability to execute critical projects. Dealing with a ransomware attack can take days initially but the distraction following that as you secure your infrastructure and deal with legacy issues also needs to be considered.

Damaged reputation and loss

A ransomware attack can significantly damage your company's reputation especially if it results in you leaking your clients data. A mid-size business is unlikely to hit broadsheet headlines, but you are duty bound to inform your clients and word of mouth is a powerful thing.

Regulatory fines

All data breaches in the UK need to be reported to the Information Commissioners Office (ICO). You could be subject to regulatory fines and not reporting any incidents increases the severity of these fines. The maximum fine the ICO is legally allowed to levy is 4% of global turnover. This is only reserved for the most serious of cases but it illustrates the priority that data breaches are now given by the UK government. In October 2020, the ICO fined British Airways (BA) a record-breaking £20 million after it ruled the airline failed to protect customers' personal data.

Lost files, wages and equipment

If you don't have proper backup protected from attacks, this could cause further losses in terms of compensation, time and money spent rectifying and recovering lost data. Even basic remedial actions, such as having to wipe and rebuild laptops, desktops and servers, could cost a considerable amount.

Additional costs

If you need to employ external support to remedy any impact of the ransomware attack, businesses can incur considerable IT fees for labour and recovery services. It may also be necessary to replace some hardware to complete any restoration and secure your infrastructure.

Best practices to protect your business

The UKs National Cyber Security Centre recommends the following precautions to shield users against today's sophisticated ransomware threats:

Hackers can easily exploit vulnerabilities in outdated applications and operating systems because they have more areas of vulnerbility. Update your software and operating systems with the latest patches to stay ahead of threats.

- A standard tactic hackers use to launch ransomware attacks is sending phishing emails with malicious links or attachments. Never click on links or attachments in unsolicited emails.
- Keep your backups safe by taking them offline and ensure they are malware-free.
- To reduce the risks associated with online browsing and remote connections to your network, ensure your employees are aware of security best practices and maintain cyber hygiene.

More best practices include:

- **Anti-phishing and email security protocols and tools**
  Utilising the right tools to identify and protect against incoming emails should be your first step in preventing ransomware phishing emails.

- **Security awareness training**
  Provide ongoing cybersecurity awareness and training programs for your employees, partners and stakeholders so that they are updated with the latest threats and security best practices.

- **Vulnerability scanning**
  With automated internal and external vulnerability scanning, you can find vulnerabilities in your network and generate a detailed report for remediation before hackers find them.

- **Patch management**
  An automated patch management tool can keep your systems up to date with the latest security patches and bug fixes.

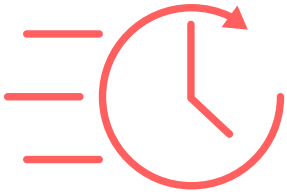
- **Endpoint detection and response**
  Endpoint detection and response (EDR) software detects and blocks ransomware before it infects endpoints, networks and cloud services.

- **Network monitoring**
  Use network monitoring tools to keep track of all your infrastructure components, performance metrics (CPU, memory, disk space, uptime), processes, services, event logs, and application and hardware changes.

- **Network segmentation**
  You can categorize your organisation's network into smaller, distinct sub-networks, allowing your network teams to compartmentalize the sub-networks and provide unique security controls and services to each.

- **Identity and access management**
  Identity and access management (IAM) secures your critical assets by ensuring that team members only have access to the tools they need to do their jobs.

- **Strong password policies/good password hygiene**
  Using multifactor authentication (MFA) and maintaining strong password policies prevents credentials from being compromised.



How to respond if an attack happens

As ransomware attacks increase in number and severity, you need to know how to respond in the event of a successful attack. Sadly whilst you can greatly minimise the likelihood of a successful attack the dynamic nature of technology means the risk cannot be completely eradicated.

Kalara are specialists at running mock "Table Top" exercises mimicking the after effects of a successful attack to help organisations prepare for real life and also spot any gaps in your defence.

The outcome of these Table Top exercises is to ensure you have:

- A process to identify which systems have been compromised through a variety of different ransomware tactics.
- A way to identify the infection status, network topology and virtual currency address provided for payment.
- Knowledge in terms of segregation and not turning off or shutting down any ransomware-affected systems.
- Best practice to isolate the infected device and compromised network area immediately.
- Checklist to change online account and network passwords right away and to gather all available log information.
- A procedure to recover data using your oldest backup.
- Agreed out-of-band communication techniques that you can utilise outside your existing network.
- A process to check if any files were dropped onto your system or if any memory captures were taken.

The chances of you falling victim to a ransomware attack are the same as those of any other company. If it happens to you, you need a plan to ensure you will be able to recover fully?

Kalara are experts in reducing the risk of ransomware attacks and providing support should it ever happen.

If you would like to talk to us about a Table Top exercise or any other topic contained in this report contact us on:

t: 01293265777

e: hello@kalara.co.uk