Ransomware Advisory to the Legal Industry

Ransomware is a type of malware designed to encrypt files on a device until a ransom, typically in cryptocurrency, is paid to decrypt the files. Once encrypted, affected files will usually have a new file extension and be rendered inaccessible until the corresponding decryptor is used. Some ransomware variants will also try to spread to other devices on the network, and in many instances, victims' data might be exfiltrated. In Singapore, this remains a growing concern, with a 262% increase in reported ransomware cases in the last 5 years.

The Legal Industry, which plays a significant role in contributing to Singapore's position as an international financial and commercial centre, has not been spared and saw a 200% increase in reported cases in the last 5 years.

The purpose of this advisory is to (i) illustrate the potential impact of ransomware to your organisation; (ii) measures you can implement to protect your organisation; and (iii) how to respond and recover if your organisation has fallen victim to a ransomware attack.

It comprises the following sections:

This advisory does not in any way detract from a law practice's or solicitor's professional and ethical obligations, including those under the Legal Profession (Professional Conduct) Rules 2015, nor is it intended to create additional ethical obligations for a law practice or solicitor.

Impact of Ransomware

Ransomware attacks can lead to serious consequences to the victim organisation, including:

- Temporary or permanent loss of files or data
    - After a ransomware attack, recovery of encrypted files is usually difficult as each ransomware variant requires a unique decryptor, which may not be available for newer ransomware variants. Organisations could lose access to critical data, including any sensitive or proprietary information if there was no proper backup of data.

- Exfiltration of sensitive data
    - In a ransomware attack, confidential information may be exfiltrated and published in the public domain if a ransom is not paid. The exfiltration of personal data and client confidential information could result in reputational damage or regulatory penalties.

- Disruption to operations
    - When files or data tied to business-critical computer systems/networks are encrypted, services to clients may be disrupted.

- Due to the sensitivity of the information handled by the legal industry, threat actors have been observed to threaten to publish/auction exfiltrated data online or to notify the victim's stakeholders and media about the data breach to coerce victims into paying the ransom.

With the disruptions brought about by a ransomware attack, organisations may feel compelled to give in to the threat actor's demands and pay the ransom. However, SingCERT strongly discourages paying the ransom. Further elaboration on why you should not pay the ransom is available here:

https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/singcert-advisory-protect-your-systems-and-data-from-ransomware-attacks.pdf

https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022

Prepare Incident Response and Business Continuity Plans

It is vital for an organisation to be well prepared to recover quickly from a ransomware attack to minimise disruption to operations. This is especially so for the legal industry due to the various deadlines woven into legal frameworks for compliance purposes or to facilitate orderly processes. Having a robust incident response plan and business continuity plan will help organisations recover much faster. This section seeks to provide a guide for organisations to develop robust incident response and business continuity plans.

Develop an Incident Response Plan

An Incident Response Plan (IRP) is the organisation's immediate action plan against cyberattacks or data breaches. It is a structured guide that ensures a swift and coordinated response when a security incident occurs. It outlines the steps that the organisation's IT teams need to take to detect, contain and remove the threat, with the aim of minimising the impact of the incident and reducing any downtime. The plan should be regularly exercised, such as via cyber drills, to help relevant personnel know what actions to take. Organisations may wish to refer to the following Incident Response Checklist when developing such a plan:

https://www.csa.gov.sg/Tips-Resource/Resources/singcert/incident-response-checklist

Develop a Business Continuity Plan

A Business Continuity Plan (BCP) is the organisation's lifeline during any disruption, whether it's a natural disaster, pandemic or cyberattack. It is a comprehensive plan that outlines how to maintain essential operations and services during a crisis. It identifies critical business functions, assesses potential risks and develop strategies to mitigate those risks. BCP drills also should be conducted with operational departments and key decision-makers so that all relevant stakeholders are familiar with the plan. In addition, the BCP should also be reviewed regularly and updated whenever there are important changes in assets or stakeholders.

How do I Protect my Organisation?

Prevention is key to avoid falling victim to ransomware. To formulate an effective defence against a ransomware attack, everyone has a part to play, with measures being implemented at both the individual and organisational level. It is also critical to have a sound strategy for the backup and recovery of critical data. This section outlines key measures law firms should implement and good cyber hygiene practices employees should adopt to secure the organisation's network and data.

What can Law Firms do to Protect their Network?

Set out below are some measures that law firms can undertake to protect their network. In assessing and implementing the measures below, law firms should carefully consider the nature and size of their practices and the availability of internal resources to determine the most suitable approach. It is important to recognise that external support or outsourcing may be necessary to effectively implement some of these measures.

Identify and Protect Business-Critical Assets

Many organisations, including law firms, handle a wide array of sensitive data, including personally identifiable information (PII) of clients, trade secrets and financial records, making them prime targets for cyberattacks. Understanding the type of data held, their sensitivity, and data protection regulations will help law firms prioritise the protection of these core business-critical assets. Firms should strongly consider the implementation of network segregation that restricts connections between internet facing servers and internal networks to protect sensitive information stored in internal servers.

Install Antivirus Software on all Devices

Anti-virus/anti-malware software should be installed on all devices and regular scans performed to detect and remove any malware. This software should also be able to quarantine and prevent the execution of any malware that is deployed deliberately or inadvertently in the network.

Update Systems, Software and Applications Regularly

Update systems, applications and software to the latest version and apply the latest security patches promptly, especially for business-critical functions. If immediate patching is not possible or feasible, vendor-provided mitigations should be implemented.

Isolate Devices that use Legacy Operating Systems

Organisations are advised to upgrade their devices that use legacy operating systems to supported operating systems. If organisations are unable to upgrade their devices [or procure extended security support], they are advised to take precautionary measures to isolate these devices. Precautionary measures include the following (non-exhaustive):

- Set up Internet Protocol security (IPsec) rules
- Enforce login restrictions
- Isolate network/virtual local area network (VLAN)

Disable Excel Macros by Default

Given the unique demands of the legal industry, characterised by a high volume of document transfers, threat actors may attempt to deliver malicious payloads via Excel Macros. Upon execution, the macro may download and execute ransomware from external servers. Hence, organisations should disable macros by default and only enable them on a case-by-case basis.

Implement Strong Password Policies and MFA

Organisations should implement password policies requiring the use of strong passwords of at least 12 characters which include upper case, lower case, numbers and/or special characters, and implement MFA for all internet-facing services, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

Review Settings on Exposed Services and Open Ports

Some ransomware variants may take advantage of exposed services and open ports such as the RDP port 3389 and SMB port 445 to move laterally in the network. Organisations should disable unnecessary ports and if required, restrict connections only to trusted hosts.

Implement Principle of Least Privileges

Organisations may consider practising the principle of least privileges or any other applicable established framework when monitoring and validating privileges of users and devices, to reduce the chances of a threat actor gaining administrative privileges, organisations should:

- Control and limit privileged access to only authorised individuals who require full access to carry out their work.
- Give all other users the lowest user privileges necessary for work.
- Review and manage the use of all user accounts and disable inactive accounts.

Use an Email Security Gateway

Organisations may want to install an email security gateway to identify and block malicious emails before they reach employees' inboxes.

Implement Anti-Spoofing Controls

Enable the following email authentication protocols to prevent email spoofing where possible:

- Domain Keys Identified Mail (DKIM) to cryptographically sign the email you send to show it is from your domain.
- Sender Policy Framework (SPF) to publish IP addresses which should be trusted for your domain.
- Domain-based Message Authentication, Reporting and Conformance (DMARC) to set a policy for how receiving email servers should handle email which does not pass either SPF or DKIM checks. DMARC also generates reports, which can be used to understand how your email is being handled.

Encrypt Important or Sensitive Data

Organisations should encrypt important or sensitive data as this makes it more difficult for threat actors to read the data if it was exfiltrated. Encryption may also prevent some ransomware variants from detecting the files if they work by looking for commonly used file types such as images and documents.

Implement Application Control

Consider installing application control software that provides application and/or directory whitelisting. Whitelisting allows only approved programs to run, and can prevent unknown programs, such as malware, from running.

Implement Network Segmentation

Organisations can also consider implementing network segmentation to divide a larger network into smaller subnets with limited interconnectivity between them. This will control traffic flow between the sub-networks, prevent lateral movement and limit the spread of ransomware, should one subnet be compromised. Implementing network segmentation also generates logs for traffic flow between various subnets. Organisations should monitor these logs for any suspicious activities and carry out containment and response measures, where necessary.

Regularly Monitor all User Accounts

Regular monitoring should also be conducted on all accounts to detect any suspicious activities, such as multiple failed login attempts.

Conduct Regular Penetration Testing & Validate Defence Mechanisms

Conduct regular penetration testing on both external and internal facing networks to identify any vulnerabilities that may be exploited during an attack. This will allow organisations to make timely patches to existing vulnerabilities in networks or systems. Key defence mechanisms such as securing

access to sensitive data with robust authentication methods and checking of users' privileges should be validated against simulated actions typically performed by attackers such as data encryption.

Maintain an Updated Backup, and Keep a Copy Offline
Performing regular data backups facilitates data restoration in the event of a ransomware attack. It is important that a copy of the backup data is stored offline and not connected to your network, as some ransomware variants can propagate across the network. Organisations should also test backups periodically to ensure they can be restored successfully. Additionally, organisations may wish to implement immutable backups, which are backup copies of your organisation's data that cannot be altered, deleted, or changed except after specific time periods, providing additional robustness to your backups.

Maintain Regularly Updated "Golden Images" of Critical Systems
This entails maintaining image "templates" of virtual machines or servers. These images should include a preconfigured operating system (OS) and relevant software applications. If there is a need to rebuild the system, these images can then be quickly deployed.

Limit Data Stored and Properly Dispose Data That Is No Longer Needed
Organisations should only store information essential for business operations and ensure that data is properly disposed of when no longer required.

Stay Informed of the Latest Cyber Threats
Keep abreast of the latest developments in ransomware threats and mitigation strategies through security bulletins, news updates, and training sessions. CSA/SingCERT and SPF have collaborated to establish a ransomware portal to publish ransomware trends and advice for ransomware. The portal can be accessed here:

https://www.police.gov.sg/Advisories/Crime/Cybercrime/Ransomware

Raise Awareness & Conduct Employee Training
Securing your systems against ransomware requires an organisation-wide effort. Awareness and education are key to preventing ransomware attacks. Organisations should conduct regular training for employees at all levels of the organisation (including senior executives) to raise their awareness of cyber threats such as phishing which is one of the most common attack vectors used by threat actors. By having employees adopt good cyber hygiene practices and learning to identify potential cyber threats, cyber awareness within the organisation will be raised, minimising the chances of a successful attack. Organisations can refer to the cybersecurity toolkits under CSA's SG Cyber Safe Programme as a training resource here:

https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-toolkits

What can Employees do to Protect their Organisation?

Use Strong Passwords and Enable Multi-Factor Authentication (MFA)

- Use strong, unique passwords for all accounts, and update them regularly.
- Use MFA when available, as this presents an additional layer of protection.

Only Install Software from Legitimate Sources

- Check that you are only downloading software from official sources and that they comply with security requirements.

Backup Data Regularly

- Ensure regular backups of important files are done, stored securely and are not directly accessible from the network. One of the main goals for attackers to conduct ransomware attacks are to disrupt the organisation's processes and having good backup practices ensures business continuity at the individual level.

Be Cautious of Removable Devices

- Avoid using removable devices such as USB drives from unknown sources, as you might inadvertently introduce malware into the system.

Check the Authenticity of the Advertisements/Emails/Messages

- Always be wary of suspicious emails/messages and verify with the organisations through their official sources before clicking any links or downloading any attachments, especially if the email/message comes from an unfamiliar sender. Report the email/message to the service provider if you suspect it to be malicious.

Report Suspicious Activity

- Report any potential phishing emails, unsolicited phone calls/emails, suspicious links or activities to the IT or security team immediately.

What should I do after an Incident has Occurred?

Law firms and practitioners are reminded that in a data breach, they may have legal obligations to notify affected individuals (including clients) and/or regulatory authorities of the data breach. Therefore, law firms and practitioners are reminded to carefully consider their legal and professional obligations in responding to a data breach incident and to consider making notifications as appropriate within the relevant notification timelines.

Law firms who are the subject of a ransomware attack may wish to refer to CSA/SingCERT's Ransomware Response Checklist for information on the response and recovery steps. Organisations are recommended to review and familiarise with the steps in the checklist before an incident. Please refer to the following link for the checklist:

https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/ransomware-response-checklist.pdf

If a cybersecurity incident occurs and external assistance is required, victim organisations may wish to approach reputable cybersecurity vendors. Please refer to the following link for a list of CREST-accredited incident response vendors:

https://www.crestapproved.org/members/?filter_accredited_services_10717=Cyber%20Security%20Incident %20Response&filter_offices_10717=Singapore

To report ransomware incidents, please visit https://go.gov.sg/singcert-incident-reporting-form. CSA/SingCERT will help to provide any insights on the threat actors and their tactics, techniques, and procedures (TTPs). If a decryptor is publicly available for the identified ransomware variant, CSA/SingCERT can also assist to facilitate its provision.

Should I Pay the Ransom?

Please note that CSA/SingCERT strongly discourages paying the ransom. While it may appear to be a convenient way of recovering encrypted data, paying the ransom does not guarantee that locked data will be decrypted or stolen data disposed-off once ransom has been paid. Additionally, it not only encourages the threat actors to continue their criminal activities and target more victims, they may also see such organisations that pay the ransom as soft targets and strike again in the future.

More information is available here:
https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/singcert-advisory-protect-your-systems-and-data-from-ransomware-attacks.pdf

https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022

Jointly published by: