TruStage™

Ransomware

Risk overview

The fact that ransomware attackers can steal as well as encrypt data isn't a new phenomenon. However, the possibility that sensitive data – including member financial records, employee information, salaries, etc. - might be revealed is potentially more damaging than any short-term disruption caused by the malware. Unfortunately, six and seven-figure ransomware demands have become routine.

Ransomware has grown in loss frequency and severity, in addition extortion demands have risen significantly. A ransomware incident is one of the most disruptive and costly attacks your organization can suffer.

Unfortunately, it's getting easier to deploy ransomware and malware, and that gives threat actors more access than ever before. Tools – such as do it yourself Ransomware-as-a-Service (RaaS) kits - are cheap to obtain and competition between ransomware providers has driven entry costs down. In addition, some tools are publicly available and anyone with minimal coding skills can re-use them.

There is also evidence that threat actors do not always honor their word to destroy exfiltrated data if the ransom is paid. Even if the original threat actor has been paid, it remains nearly impossible to ensure that the information is not accidentally or intentionally shared with other threat actors. This is one reason why fewer victims are paying a ransom.

Threat actors are also moving slightly up the market with the median size organization having 275 employees. They are also indifferent to which type of organization pays them as long as they are getting paid. This is being done to try and justify larger initial demands in the hopes that they result in large ransom payments.

$409K

Average ransom payment paid by ransomware impacted companies

24 days

Average downtime

Source: Quarterly Report, Coveware, January 2023

Typical ransomware scenarios

Initial compromise of your environment

Remote Access Security

- Microsoft RDP and Remote Desktop Gateway (RDG) can be used to provide remote access to computers and networks.

Phishing/Spear Phishing

- Fraudster or threat actor targets an individual within your organization with a phishing campaign.
- Spear phishing targets a select group with something in common – e.g., work or bank at the same organization.
- Malware is successfully delivered to one of your unsuspecting users via a malicious attachment or web link in an email.

Malware is installed

- The user opens the attachment and malware is unknowingly installed on the user's PC. The threat actor now has a foothold in your environment.
- The hackers undetectably explore your network looking for vulnerable systems and sensitive data. This includes other users' PCs but also servers supporting critical applications and file stores.

Ransomware is deployed

- With access achieved, ransomware is spread throughout the network.
- Attackers have now encrypted and disrupted a material portion of your business. Some parts of your business are completely disrupted while other parts are partially disrupted.

Extortion is demanded

The attackers demand ransom in exchange for the decryption key.

Most identified infection points

- Phishing emails
- Corrupt attachments
- Weak remote desktop protocols (RDP)
- Unpatched systems
- Extensive reuse of passwords
- Lack of multi-factor authentication

Proactive prevention tips

- Keep all systems including hardware, mobile devices, operating systems, software, cloud locations, and content management systems, patched and up-to-date.
- Activate two-factor / multi-factor authentication on all systems including managed service provider software platforms, administrator systems, and end-user systems wherever possible.
- Backup and test data regularly and verify the integrity – ensure backups are not connected to the computer or networks that are being backed up.
- Apply the principles of least privilege and network segmentation where an end user only has the privileges necessary to complete tasks related to their role.
- Vet and monitor third parties that have remote access to your network and other third-party connections. Ensure they are diligent with cybersecurity best practices.
- Gain familiarity with FinCEN's Red Flag Indicators s to assist in detecting, preventing, and reporting suspicious transactions.
- Provide regular social engineering and phishing training with employees.

Ransomware-related data breaches have doubled in each of the past two years. At the current growth rate, ransomware attacks will pass phishing as the number one root cause of data compromises in 2022.

Source: 2022 ITRC Annual Data Breach Report, IDTheftCenter.org

Checklist of things to know to help you prepare

Know who is on your incident response team.

Discovery of a data breach happens in an instant and critical, defining decisions that affect the outcome and the operation of your organization need to be made on short timelines. Understanding who is part of the incident response team and having the appropriate individuals from major stakeholders of the organization is critical.

Have multiple forms of communication available.

Many ransomware attacks target critical infrastructure of the organization to induce fear and panic. Even when critical operations like email are not infected; it can be in the best interest to take uninfected systems offline to avoid the spread of attacks. Be prepared by having contact information - cell phone numbers, personal email addresses, or standalone email addresses already created in the event of an attack. A best practice is saving this contact info in a group text string.

Be prepared to make decisions about voluntarily taking systems offline.

Ransomware can spread from one device to another when devices come online. This could be individual user endpoints or more critical server infrastructures. Often a decision needs to be made to take systems offline. Understand ahead of time your willingness to do so and prioritize a list of critical systems and your willingness to take them offline. Make sure the incident response team includes the individual who has the network authority and ability to act in a moment's notice.

Be prepared with an internal communication plan prior to any attack.

If you decide to limit the spread of an attack by limiting end points from logging into the network, be prepared on how and what you will communicate with your employees.

- Will you share all the incident details?
- What might they share with members or other outside sources?
- How will you communicate with employees, especially if your email system is down?

Do not allow employees to reach out to the threat actor themselves.

It may feel intuitive for an IT team or Managed Service Provider to jump in and manage the incident themselves as they may feel they have the expertise or wish to investigate the issue. However, there are other steps these teams can take to help manage the incident on their own.

Negotiations with criminals require special expertise and can change the dynamic of the negotiation quickly – often decreasing the ransom demand significantly. Allow the ransomware experts to intervene and utilize your resources to help contain the issue.

You will be asked to sign two agreement letters within the first 24 hours.

Two critical parts of any incident response team are the breach coach (attorney) and your incident response team. These make up the core group investigating any incident.

Following the initial call within hours after discovering a data security incident, your breach coach and the forensics team will provide your organization with two documents. The breach coach will ask for an engagement letter formally engaging your firm with theirs; the forensic team will provide a statement of work that includes both your firm and the breach coach outlining the scope of the work that the forensics team will conduct.

Both documents will outline hourly rates and a general budget. Typically, they will not require a retainer or a down payment as your insurance policy will act as collateral. Be prepared to review these quickly and have the appropriate individual sign them.

You do not need to have your own cryptocurrency on hand.

If you elect to pay a ransom, your organization will work with your breach coach and forensics team to facilitate the ransomware payment.

Some forensics providers offer ransom negotiation and payment as a service, while others do not. If they do not provide that negotiation service, they will retain a specialized third party on your behalf to assist.

In many cases, depending on your insurance policy, you will be required to wire U.S. Dollars in the equivalent of the ransom payment to the third party and they will use cryptocurrency on hand to pay the ransom on your behalf. This will become part of your insurance claim for reimbursement from the carrier.

You need underwriting approval to pay a ransom.

Most cyber liability insurance policies will require underwriting approval prior to paying a ransom. An insurance company representative (either working for the insurance company or a third-party firm) will work with your breach coach in the background.

While they must sign off on a ransom payment, they cannot unreasonably refuse. While this approval is required, it is typically handled swiftly given the time restraints.

Know your backups and understand that they are not always the answer.

Many organizations have strengthened their backups trying to achieve an "airgap" between primary networks and the backups. This does provide an alternative option when dealing with ransomware.

The latest trend in ransomware however is that threat actors will not only encrypt information but also steal it. This increases the pressure on you to pay the ransom.

If you have good backups and choose to restore from them in lieu of paying a ransom, know that risks may still exist. The information that was stolen still presents a data breach and will likely result in corresponding notification and other legal guidelines.

Think about who the organization needs to tell and when.

Communicating with outside groups such as boards, members, and the community, is an organizational choice. Some boards of directors may have a higher priority of knowing about the incident than others and some members have contracts that require notice of an incident in a certain period. Understanding these items will save time during the initial stages of an attack.

In general, more effort is being placed by threat actors towards remaining undetected on a breached network - commonly referred to as dwell time or the time that exists between the first execution of malware and its discovery inside the network.

Increased dwell time provides threat actors with opportunities to escalate hijacked privileges while searching for data caches of sensitive information that can be exploited.

If you suspect a ransomware attack, be sure your organization is ready to respond.

Immediate steps to take to manage a ransomware incident

- Do not restore data until images can be collected by the digital forensics team.
- Do a global password reset.
- Disconnect from back-ups.
- Disconnect from the internet.
- Check to see if there are any malicious inbox rules.
- Obtain the ransom demand to share with the legal and forensics vendors.
- Contact your insurance carrier immediately to report an incident.

Looking for additional insights?

- Access the **Business Protection Resource Center** (User ID & password required) for exclusive risk and compliance resources to assist with your loss control efforts.
- Go to **Emerging Risks Outlook** for critical questions, answers, and resources to help build additional awareness and drive organizational action.
- If you'd like to discuss this risk in more detail, simply schedule a no-cost 1:1 discussion with a TruStage™ Risk Consultant by contacting us at **riskconsultant@trustage.com** or at **800.637.2676**.

There's no foolproof way of preventing ransomware attacks from occurring. Data exfiltration resulting from ransomware, along with increased ransom demands, continues to become more common and has resulted in significant ransom payments even where ransomware recovery from backups was possible.

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. TruStageTM is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions,

TruStage™