CUNA MUTUAL GROUP

Ransomware

A Checklist of Things to Know

Ransomware Attacks Continue As The Predominant Cyber Issue

Ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data and internal company secrets would be publicly released. Unfortunately, **six and seven-figure demands** have become routine among ransomware attacks. Credit unions need to be looking out for ransomware techniques. These cyber attacks have no boundaries and are truly a global issue. Ransomware has grown in frequency and severity and extortion demands have risen significantly.

The fact that ransomware attackers can steal as well as encrypt data isn't a new phenomenon but the possibility that sensitive data might be revealed is potentially more damaging than any short-term disruption caused by the malware. Data could include member financial records, employee information, termination letters, salaries, and much more.

Pay-or-Get-Breached

An expected increase in targeted ransomware attacks that employ a "pay-or-get-breached" methodology, intensify the threats of data exposure, potential regulatory compliance issues, and disruption for victimized credit unions. As these affected organizations become more inclined to pay demands in order to bring their systems back online, they are also likely to incur scrutiny by government agencies over concerns that the funds will land in the hands of entities on U.S. sanctions lists.

While the most identified infection points remain phishing emails, corrupt attachments, and weak remote desktop protocols (RDP); unpatched systems, extensive reuse of passwords and a lack of multi-factor authentication has also contributed to the increase in successful entry.

Additionally, ransomware operators are placing more effort towards remaining undetected on a breached network - commonly referred to as dwell time. Increased dwell time provides threat actors with opportunities to escalate hijacked privileges while searching for data caches of sensitive information that can be exploited. The average dwell time is 43 days for ransomware according to Infocyte.

*There's no foolproof way of preventing ransomware attacks from occurring; however, there are a number of **things to know** to help you be prepared.* ***Check them out on the upcoming pages >>>***

Ransomware: A Checklist of Things to Know

Know who is on your incident response team.

Discovery of a data breach happens in an instant and critical and 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 of the organization 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, but it also could be 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.

If you decide to limit 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 details? What might they share with members or other outside sources? How will you communicate with your employees, especially if your email system is down? Consider these topics and make them a part of your internal communication plan prior to any attack.

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. 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.

> *"These cyber attacks have no boundaries and are truly a global issue. Ransomware has grown in frequency and severity and extortion demands have risen significantly. A ransomware incident is one of the most disruptive and costly attacks your organization can suffer."*

Derek Laczniak, CIC
Director Cyber Liability

M3 INSURANCE

Ransomware: A Checklist of Things to Know

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

Two of the most 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 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, you 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 that you obtain underwriting approval prior to paying a ransom. A representative with the insurance company (either working for the insurance company or a third-party firm) will be working 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 of these matters.

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 bad 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.

Immediate Steps to Take to Manage the 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

Related Resources

You can also access CUNA Mutual Group's Protection Resource Center (User ID / Password required) at cunamutual.com for exclusive resources and RISK Alerts to assist with your loss control efforts including:

- Cybersecurity Threat Outlook eBook
- Ransomware Risk Overview
- Ransomware Prevention & Response Checklist

Beazley cyber insurance policyholders can access additional resources at www.beazleybreachsolutions.com (User ID / Password required). BBR resources include interactive online training on phishing and social engineering.

If you'd like to discuss ransomware or cyber risks in more detail,
simply schedule a no-cost personalized discussion with a CUNA Mutual Group Risk Consultant
or contact us at riskconsultant@cunamutual.com or at ***800.637.2676****.*

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. CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Insurance products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company, members of the CUNA Mutual Group.