Ransomware first response

You? The organization?

Dr. Betina Tagle
University of Maine at Augusta (UMA)

RANSOMWARE

A popup says your computer is locked until you pay!

It is your work laptop! What should you do? What will your organization do? Your heart races!

Image from CISCO Umbrella

What, How, Why

First, what is ransomware?
Malicious code (Malware) that can take over a computer. CSOOnline suggests that the most common is to encrypt files on the computer (1). In some cases the ransomware also can send out the files to the attacker. The biggest factor, the key to decrypt is only known by the attacker (1).

Second, how is it done?
Ransomware is performed through social engineering techniques, most commonly phishing emails (1). Some are targeted to specific leadership, while some are random.

Third, why is it done?
It makes money and its easy.
It creates an emotional response of the victim to want to act quickly.

Example:
Imagine if the organization was a medical facility that built a good reputation in the community. An attacker threatens to publicly post pornographic images (hospital personal pasted into image) if the ransom payment is not made, even if those images didn't exist.

STATISTICS

Ransomware is growing!

A NYTimes article says there has been a growth of 41% increase from 2018-2019 of organization's files being attacked by ransomware, with payments spiking to $84,116 (2).

In April 2020, Maze committed a ransomware attack on Cognizent, a Fortune 500 company (3). According to Infosecurity-Magazine, the Maze attack was performed when "…Maze purchased access to Cognizant's data from a hacker who was advertising the sale of access to a huge IT company's data for $200k" (4).

How did the hacker gain the data, where they an insider? Regardless, Maze took the opportunity.

No organization is safe against ransomware!

How to respond

Your option?
Report it to your supervisor immediately!
This is not a time to be worried about being the cause of it or not. The organization needs to take quick action to report to external agencies as required (5).

The organization's options?
1. Pay the ransom
2. Not pay the ransom

The organization's security policy should clearly state in "thou shall" language which option the organization can take.

In the meantime, the incident response team should be working on the case as soon as it is reported.

What is the ultimate knowledge taken from this slide?
The organization's responsibility is to review policy, review their cyber insurance, and then look at what backups are on standby.

What does Cyber insurance do?

Cybersecurity insurance can be categorized into different types. Some examples: Data Breach, Cyber liability, even Cleanup & Recovery.

Why?
Because there different type of attacks that my required different activates based on laws and the insurance requirements.

For example: In a data breach a company is required to notify customers based on state laws, thus, the insurance company includes this aspect into a policy purchased for data breach coverage. The insurance company may pay to provide to notifications, and services to manage the notifications.

Another example: if there was a network attack, it may be that the insurance company may require a third-party to make a determination of the legitimacy of the attack before paying for damages. In this case the company would need to clearly understand who pays for the third-party investigation.

Final example: the insurance company may provide for recovery and clean up from attacks, but as an addendum (additional cost).

What does Cyber insurance look like?

Looking at: **The Hartford** [https://www.thehartford.com/cyber-insurance]

The Hartford offers: **Data Breach & Cyber Liability Insurance**
They state: "Our data breach insurance and cyber liability insurance are two different policies." (10, para 6).

Data Breach policy helps >

- Notify affected customers, patients or employees
- Hire a public relations firm
- Offer credit monitoring services to data breach victims

Cyber Liability policy helps >

- Legal services to help you meet state and federal regulations
- Notification expenses to alert affected customers that their personal information was compromised
- Extortion paid to recover locked files in a ransomware attack
- Lost income from a network outage
- Lawsuits related to customer or employee privacy and security
- Regulatory fines from state and federal agencies

Additional items (Addendums)* > lost income from data breach, Prior Acts coverage (claims related occurring before policy effective date), Extortion Coverage. *extra cost

Key Take away

It is important to review annually the cyber insurance policy purchased.

This ensures that updates in the policy are captured in the security policy (remember, the “thou shall” or “shall not” document).

At UMA we have a Security Assessment Team (SAT) as a security resource for small businesses within the community. One of the activities we have done is review cybersecurity insurance policies with the company security policy to help in the alignment of requirements so cybersecurity insurance requirements are met.

Example: if the cyber insurance requires a third-party to determine the legitimacy of the attack, and the company must report the attack within a certain time frame to the insurance company, that must be a part of the security policy ***and*** incident response plan.

Again - to respond to a ransomware an organization needs to choose to pay or not pay, but the right support must be in place, like backups.

NIST GUIDANCE: BACKUPS

According to NIST, "A prevention solution involving backups, physical security, and employee education is often more effective" (8).

We discussed security policy (the 'thou shall" document) and cyber insurance. Let's look at backups.

NIST can help organizations have clean backups:

- identify the correct backup version (free of malicious code and data for data restoration)
- identify altered data as well as the date and time of alteration
- determine the identity/identities of those who alter data
- identify other events that coincide with data alteration
- determine any impact of the data alteration (9).

Backups should be performed regularly!

Important items to keep in mind

- Many organizations pay the ransom, although law enforcement doesn't encourage this since it is a positive reinforcement to the behavior of ransomware attacks (6).
- It is common knowledge that an organization may pay the ransom amount, but it does not guarantee the key given will restore all files (data/information).
- If the malware (ransomware) is removed, the attacker cannot restore your files even if you pay the ransom (6).
- Many ransomware attackers know the amount of cybersecurity insurance an organization has to pay out. Although encouraged to pay via cybersecurity insurance, premiums have increased greatly (7).
- Having adequate backups is a key to restoration after an attack, but if the backups are done through a network connection (like online journaling) it is possible that those backups fall victim to the ransom attack as well. The best is to do a backup, remove those backups from the network, and store separately off-site.

References

1. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
2. https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html (Popper, 2/9/20, para 5/6).
3. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/maze-ransomware-attacks-us-it-firm
4. https://www.infosecurity-magazine.com/news/maze-wage-ransomware-attack-on/ (Coble, n.d., para 12).
5. https://www.justice.gov/criminal-ccips/file/872766/download
6. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
7. https://www.cpomagazine.com/cyber-security/ransomware-attacks-are-causing-cyber-insurance-rates-to-go-through-the-roof-premiums-up-as-much-as-25-percent/
8. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-detect-respond-nist-sp1800-26-draft.pdf *NIST Draft (p23).
9. https://www.nccoe.nist.gov/publication/1800-11/ *NIST draft (online version), Volume B, 1. Summary, para 3.
10. https://www.thehartford.com/cyber-insurance

Thank you!

Dr. Betina Tagle, GSLC
Assistant Professor of Cybersecurity, UMA
UMA Security Assessment Team Advisor
betina.tagle@maine.edu
207-621-3032 (office)