RANSOMWARE ATTACKS: MAKING YOUR ORGANIZATION'S "BEST DEFENSE A GOOD OFFENSE"

BY CHRISTINE MEADOR, CFE

Imagine, it is a normal day and you make your way into the office. You arrive at work and begin logging into your computer system. Things seem normal at first; however, you suddenly realize your system is not working properly. You then receive a notice that your information is inaccessible. Next, the notification on your screen indicates all of the organization's files are locked and encrypted. In order to unlock the system, you are instructed to follow a link and make a payment. What do you do? Who do you call? How do you proceed?

Many organizations have experienced these types of attacks known as *'ransomware.'* Ransomware, which is broadly defined as a "type of malware that blocks the user from accessing files," specifically locks the user out of the computer while setting demands for a ransom to be paid. As confirmed by multiple organizations, news reports and law enforcement, in 2019, ransomware attacks are rising.

To be prepared, organizations need to have a solid Response Plan in place. We have all heard the quote, "The best defense is a good offense." Does your organization have a good offensive plan in place to deal with these types of threats and how would you proceed in your defense of a ransomware attack?

RANSOMWARE ATTACKS IN OHIO AND ABROAD

Many reading this article may feel their organizations have cybersecurity covered, but the fact is, many victim companies felt they had this covered as well. In Ohio, the ransomware attacks came too close to home with incidents reported from Riverside fire and police, City of Akron and Cleveland Hopkins International Airport. Shortly after this, another ransomware attack was reported at the Louisville Regional Airport in Kentucky. Whether you are a basic user or a business, ransomware attacks do not differentiate between victims. This is revealed in the random reports from businesses, school districts, cities and hospitals in various states.

As reports of these attacks continue to surface across the country, we are learning ways in which law enforcement and victims have been dealing with these threats. Many victim companies have shared their stories. Some go public when the obvious cannot be hidden and other companies may pay the ransom and remain silent. For each organization, it is a choice; however, in theory and from actual cases, if a fraudster is not stopped, they will move on to strike again. Now, think in terms of a hacker who is untraceable and often sitting in another country. These hackers are sophisticated, funded and working with malware that is constantly changing. If these fraudsters are not caught, they will continue and possibly return as a future threat.

The City of Akron attack is an example of a municipality that came forward to give an account of the attack and recovery. Through Akron's transparency, the public has received a tremendous insight into the required plans for disaster and recovery.

WAYS YOUR ORGANIZATION CAN DEVELOP A "GOOD OFFENSE"

Response Plan – The best way to prepare in advance is to develop a good Response Plan. Response Plans, often referred to as a Disaster Recovery Plan, are not new; however, the layers of what is classed as 'disasters' is constantly evolving due to new threats. With Disaster Recovery Plans of the past, the term 'disasters' referred to events such as fire and weather, with light discussion of cyber controls such as passwords and viruses. Effective Disaster Recovery Plans now include a more extensive cybersecurity layer to support 'disasters' such as ransomware. When developing the cybersecurity layer, it is essential to secure the assistance of IT professionals versed in cybersecurity.

Insurance policies – In relation to insurance policies, it is critical to know your policy in advance and to understand where cyber threats fall under the insurance umbrella. Damages associated with cybersecurity breaches may be covered under a cyber liability and/or data breach insurance policy. Additionally, damages relating to business interruptions may also qualify depending on the disruption associated with the breach.

Educate your 'in-house' team – As with organizational trainings on topics such as ethics, it would be beneficial to offer trainings on cybersecurity threats. Engage your staff in luncheon trainings on cyber threats such as ransomware. These trainings should be offered to all members of the organization, from board & trustee members to employees and volunteers. Look to professionals with expertise in this area to secure training for your organization. Many professionals in the field, such as recovery management companies and forensic professional organizations, are equipped to perform these types of short trainings.

HOW ARE YOU SET TO RESPOND?

In the event of a ransomware attack, initiate your organizations Response Plan. The organization's plan should include securing the attack and assessing the damages for reimbursement.

Securing the ransomware threat should include identifying how the breach occurred in order to fix and prevent it from reoccurrence. Additionally, it is critical to properly retrieve data in a manner that will not corrupt the information as this could prevent finding the way in which the ransomware and threat occurred.

BRINGING IN THE EXPERTS

The recovery team along with law enforcement will be the best source to move the organization into recovery mode. As well as utilizing key employees of the victim company to assist in recovery, it is essential to bring in a team of professionals with firsthand expertise. Key professionals could include law enforcement, a recovery team, the insurance provider, outside legal and the necessary outside experts.

WHY BRING IN LAW ENFORCEMENT?

An essential line of defense in your plan should include engaging law enforcement professionals to offer critical guidance on how to proceed. The FBI has been instrumental in assisting many victims of ransomware attacks. Through a recent inquiry to the FBI, I had the opportunity to obtain the following FBI recommendations:

> *"The FBI encourages ransomware victims to contact their local FBI field office as they may have additional information on ransomware events which can help organizations navigate their specific ransomware incidents. When engaging the FBI, this allows them to capture intelligence and evidence related to these incidents, which is critical to the FBI's success in mitigating this threat. Additionally, organizations can also report ransomware events to the Internet Crime Complaint Center at* IC3.gov. *This is a valuable resource of information used by a variety of law enforcement agencies to investigate and disrupt organizations perpetuating ransomware attacks.*
>
> *The FBI stated beyond traditional Internet security for addressing common methods of attacks such as malicious email and remote access, it is extremely important to have a comprehensive back-up strategy that includes versioned off-network and/or off-site backups with periodic recovery testing. The FBI also recommends participating in a ransomware tabletop exercise with those involved in recovering from a ransomware event.*
>
> ### COMMON RANSOMWARE MISTAKES AS SEEN BY THE FBI
>
> *The first mistake to point out is premature remediation. While the FBI does not support paying ransoms, prematurely wiping infected systems eliminates a potential recovery avenue. Infected systems should be removed from the network and preserved to provide critical information related to the event and a potential recovery mechanism. Additionally, it is important to verify data has been restored and is accessible before wiping and re-imaging infected systems.*
>
> *Another mistake found is organizations storing critical recovery information solely on-network, such as the keys or passwords required to access off-network backups (e.g., cloud backups), contacts of internal and external incident response team members.*
>
> *One more common mistake is not utilizing role-based access controls (RBAC). These are system restrictions on an employee's access to network resources, which could limit the impact of ransomware events.*
>
> *Finally, another mistake is organizations having a limited understanding of the nature of the impacted data, incident events and timelines, and related security breach obligations."*

ASSESSING DAMAGES AND PREPARING THE PROOF OF LOSS

A Proof of Loss is an insurance claim from the insured company to the insurer. Victim organizations will need to work towards assessing damages required to support the Proof of Loss. Damages may include lost profits associated with not being able to operate a business due to computer systems not functioning as well as "extra costs" incurred by the organization in order to operate its business, such as hiring additional IT professionals to mitigate damages.

> Whether you are a basic user or a business, ransomware attacks do not differentiate between victims.

In preparing the claim, it is critical to know what your policy offers in advance, such as hiring of experts and filing deadlines (e.g., 60 days from date of incident). In addition to utilizing employees to assist in preparing the report, consideration should also be given to engaging outside legal counsel and experts to support a substantiated insurance recovery claim. The victim company should notify the affected parties in a data breach if required (e.g., "The presence of ransomware on a covered entity's computer or business associate's computer is a security incident under the HIPAA Security Rule." https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf).

In the event an organization is not satisfied with results, such as the insurance company's financial calculation of lost profits, the wise move would be to get a second opinion. Furthermore, if the company is not receiving the proper assistance, there is always the option to file in the courts to recover losses.

As reports of ransomware attacks continue to grow, victim companies, experts and law enforcement agencies urge organizations to prepare and take notice. To be prepared, organizations should take proactive measures in planning a good offensive strategy and having a solid Response Plan in place.

Christine M. Meador is a forensic accountant at Medica, LLC. She has extensive experience in accounting, budget development, grant work, financial reporting, internal controls, financial analysis and litigation support. Christine focuses on assisting nonprofits and other organizations with fraud prevention, detection and forensic investigations. Christine has been a CMBA member since 2017. She can be reached at cmeador@medicacpa.com.

A special thanks to the FBI Cleveland Field Office for contributions with FBI recommendations and to Dennis Medica with Proof of Loss and insurance policy recommendations.