Henderson Brothers, Inc. White Paper

What should you expect in the wake of a cyber security incident, and how can you prepare your organization?

Your organization's cyber security should not be an afterthought. Your business likely has a fire evacuation plan, hopefully has a business interruption plan, and may even have an inclement weather plan. Have you given sufficient planning and consideration to your cyber security incident response plan? Many organizations do not, until it is too late.

The sophisticated malware of today will breach your network and potentially exfiltrate sensitive data or put your organization into paralysis before your team even becomes aware. The breach itself may appear innocuous. Socially-engineered phishing messages or brute force attacks with no immediate harm will provide the entry point. From there, the malware will learn your system, collect admin credentials, map out the path to create the most debilitating result, and potentially leave trapdoors to prevent future remediation, all before the malware is actually deployed and enacts its intended purpose (for example, let's assume the malware is ransomware that encrypts all of your servers and paralyzes all of your network devices, including likely your phone system). This result of encryption lockdown makes it critically important for your organization to prepare for this potential reality in advance.

So, what exactly is happening or will happen when that malware, which has been incubating in your network for weeks or months, finally "drops"? What is the fall-out of this incident?

1. **Early Infection**. Upon deployment, a typical ransomware strain will initiate its own nefarious security program to encrypt your organization's files. The ransomware likely already identified the most important files or servers and has been building its framework for weeks or months.

2. **Collateral Damage**. This encryption process is not the benevolent type, so your files, servers, network equipment, and/or end-user devices might be permanently damaged.

3. **Paralysis**. At this point, your business is definitely impacted. Your phones are likely inoperable. Your clients, vendors, suppliers, and business partners are probably observing symptoms of ransomware, and law enforcement may be involved (voluntarily or involuntarily).

4. **Recovery and Response**. After the encryption has reached a critical mass and the paralysis is suffocating, you will receive instructions from the bad actor regarding resolution of the ransomware. You will likely need a cache of Bitcoin or other virtual currency to pay the ransom and obtain the decryption key. You may also need additional equipment to run the decrypter. Finally, you need someone, a breach coach, to communicate/negotiate with the bad actor and retain the necessary forensic and network security professionals to work on your behalf.

5. **Validation**. Assuming you paid the ransom and obtained the decryption key, you need to orchestrate a test file exchange to check if the decryption key itself is workable. If the decryption is workable, you need an architect to design your new network (rebuilding your old network in its same form is probably not advisable), and a forensics team to survey the damage. You also need your breach coach to determine whether you have any required responsibility under a myriad of data breach notification laws and/or voluntary responsibility to communicate with your clients.

6. **Improvement and Future Protection**. As you work with your network and forensic team(s), it/they may advise you that you need new equipment and new security programs. They may also recommend a different policy for your back-up programs and logs.

7. **Administrative Action**. Formally or informally, your network and forensic team(s) will provide a report of their findings and remediation work. Your breach coach will digest this report and give you instructions regarding any breach notification items you may have to complete. You

How can you prepare your organization to prevent or mitigate the possible damages and lost time?

may consider retaining a public relations professional at this point.

8. **Final Resolution**. You will then continue to work with your team of partners and professionals to resolve any other items until you have restored your network, mended relationships with your business partners and clients, addressed all of the findings from forensics, and satisfied any notification requirements. This process could take a few days or several weeks.

9. **Funding.** And if you have not made arrangements in advance, after all of the above is finished, then you have to figure out how to pay for everything.

Given the situation above, how can you prepare your organization to prevent or mitigate the possible damages and lost time?

Several of the items below may come with financial constraints or the perception that "hindsight is 20/20." Nonetheless, the nine (9) general experiences of a common ransomware can be addressed as follows:

1. **Early Infection**. The migration of ransomware through your network is typically anomalous. You can invest in security software, namely lateral movement monitoring and log event management notifications, to proactively block or cure any suspected malicious behavior.

2. **Collateral Damage**. You have to assume that everything the ransomware touched may be irreparably damaged. Segmentation, even micro-segmentation, is a best practice way to separate and attempt to insulate parts of your network to keep the virus contained.

3. **Paralysis**. At the time of paralysis, you want to have an incident response plan to put into action. The given situation may produce the need for some audibles but drafting an incident response plan and retaining your professionals in advance will lessen the pain.

4. **Recovery and Response**. If assembling your network team, forensic team, breach coach, and other internal and external partners (your risk management consultant and insurance broker) was not part of your incident response plan, you need to engage those firms now. You will be relying heavily on these teams of professionals to help you respond to and resolve the cyber incident.

5. **Validation**. Testing and validation is not a step to be overlooked. Organizations who experience a breach once are often exposed to future breaches because of trapdoors left behind or other intel the bad actors collected about the organization's network.

6. **Improvement and Future Protection**. The number one "regret" for most organizations after a cyber incident is that the organization did not place a high

Many of the costs and responsibilities, even the hiring of the professionals and breach coach, can be covered under a cyber liability insurance policy.

enough importance on the length of maintaining and the amount of detail for its logs. Logging for your network is a careful balance of cost versus protection, but this is one of the best investments you can make to help prevent or shorten your incident experience.

7. **Administrative Action**. If you have any responsibilities, or you wish to take action on your own, regarding notifications, you should be working with a professional. The determination of whether a "breach" actually occurred is a legal conclusion, so be sure to consult with your counsel. Selecting experienced cyber security and data privacy counsel is an important part of formulating your incident response plan, hopefully in advance of a breach.

8. **Final Resolution**. Your final resolution may be an exercise in patience. You do not want to cut corners or be spendthrift when you are close to full recovery. See the process through to the end and continue to actively monitor for months after your incident.

9. **Funding**. Funding is perhaps the most important of any of these items. Many of the costs and responsibilities, even the hiring of the professionals and breach coach referenced above, can be covered under a cyber liability insurance policy. A cyber liability insurance policy will give you access to pre-incident resources, a breach response team, and a breach coach. You can and should also inquire whether your organization's own network, forensic, and legal professionals can be included as providers on the insurance carrier's pre- and post-breach teams. Aside from resources, a cyber liability insurance policy can also provide coverage for a variety of malware types for your organization's first party losses and for third-party losses. The funding decision is really as simple as you want to make it. The financial and risk management benefits significantly outweigh the negatives identified above, and the resources that a cyber liability insurance policy provides yields significant peace of mind for when you may have to respond to a cyber incident and you need to make that first call.