WHA WISCONSIN HOSPITAL ASSOCIATION
ADVOCATE. ADVANCE. LEAD.
The Valued Voice

Vol. 67, Issue 51 Thursday, December 21, 2023

GUEST COLUMN: Ransomware: What to Know to Create an Incident Response Plan

By Derek Laczniak, M3 Insurance, WHA's Premier Partner

10 Steps to Mitigate the Impact of a Ransomware Attack

Derek Laczniak

- ## You need to know who is on your incident response team

Discovery of a data breach happens in an instant. Critical 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 (including major stakeholders of the organization) is critical.

- ## Have multiple forms of communication available for your teams to communicate

Many ransomware attacks target critical infrastructure to induce fear and panic. Even when significant operations like email are not infected, it may be in the best interest of the organization to take uninfected systems offline to avoid the spread of attacks. Be prepared by having cell phone numbers saved in a group text string, and, even more importantly, having personal or standalone email addresses already created for use in the event of an attack.

- ## Be prepared to make decisions about voluntarily taking systems offline

Ransomware has the ability to spread from one device to another when devices come online. This could affect individual user endpoints, but it also could affect more critical server infrastructures. Prioritize a list of critical systems and your willingness to take them offline ahead of time. Lastly, make sure the incident response team includes the individual who has the network authority and ability to do so on a moment's notice.

- ## Be prepared with an internal communication plan

If you decide to control spread of an attack by limiting end points from logging into the network, be prepared by knowing how and what you will communicate with your employees. Will you share all the details? What might they share to your customers or other outside sources? How will you communicate with your employees, especially if your email system is down? These topics need to be thought about ahead of any attack.

- ## Do not allow any employees to reach out to the ransomware threat actor themselves

It may feel intuitive for an IT team or managed service provider to jump in and manage the incident themselves. They may feel they have the expertise, or may wish to further investigate the issues. 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 by a significant amount. 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 – be prepared**

Two of the most critical parts of any incident response team are the breach coach (an attorney) and your incident response team. 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, and 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 of these 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 service, they will retain a specialized third party on your behalf to assist. In many cases, and depending on your insurance policy, you will be required to wire US 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 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 in the last few years, trying to achieve an “airgap” between their primary networks and the backups. The latest trend in ransomware, however, is that bad actors will not only encrypt information, but also steal it. They do so to increase the pressure on you to pay the ransom, not because they actually want it. If you have good backups, and choose to restore them in lieu of paying a ransom, know that you might not be out of the woods yet. 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**

While communication internally with employees might be forced based on the circumstances, communicating with outside groups, like boards and customers, is an organizational choice. Some boards of directors may have a higher priority of knowing about the incident than others, and some customers 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 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
- Call M3 to report the incident to the insurance carrier

Other Articles in this Issue

- Wisconsin Health News Hospital CEO Roundtable Discusses State of Health Care
- DHS and CMS Substantiate High Quality Care and Culture of Safety
- New CMS Hospital Price Transparency Rules Set to Begin January 1
- Wisconsin Hospitals State PAC & Conduit Exceeds $350,000, Aggressive 2023 Goal Met
- GUEST COLUMN: Ransomware: What to Know to Create an Incident Response Plan
- WHA Board Discusses 2023 Outcomes, Ongoing Priorities into The New Year