A Tabletop Exercise for Assessing the Impacts of Remote Workers on Healthcare Incident Response

Prepared by the AEHIS Incident Response Committee

Committee Chair: Christopher Frenz

Contributing Members:
Dee Young
Florin Petrutiu
Andy B. Price

The current COVID-19 crisis has resulted in many changes within healthcare delivery organizations and it is important to consider, not only how these changes may impact the security of organizations but how they may impact our organizational incident response processes as well. The last few months have seen the rapid rollouts of telehealth and remote access technologies within healthcare, hospitals having to rapidly bring resources on line to ramp up capacity, and surges in not just patients, but also in temporary workforces in order to accommodate these increased patient loads. While many of these rapid changes were necessary for dealing with emergent patient care issues, few organizations have examined how these changes will have impacted their cybersecurity incident response processes. With an increasingly, remote workforce for example, do any changes to incident notification procedures need to occur or if remote access technologies are impacted by the incident, how will an acceptable incident response time be maintained? These and numerous other questions should be addresses prior to an incident impacting your organization in order to ensure that damage to the organization is minimized.

While providing patient care is clearly the priority within any healthcare organization, it is critical that healthcare organizations take the time to remember that in a modern hospital, good cybersecurity practices are essential for maintaining patient safety. It is also critical to remember that attackers have been taking advantage of the COVID-19 pandemic and have been using it as a basis to increase attacks on healthcare organizations. COVID themed malware and phishing campaigns are on the rise in recent months and healthcare organizations have been demonstrated to be especially common targets of these campaigns. A successful cyberattack occurring at a time when a hospital is already strained with surging COVID cases would have potentially disastrous consequences to patient safety. As a means of mitigating the impacts that a cyberattack could have on your organization, now is the time to reevaluate your organizations incident response processes to ensure that it is still effective when paired with the current changes to working environments that all healthcare organizations have undergone.

To help organizations evaluate their preparedness level in light of these changes, the AEHIS Incident Response Committee is making the following table top exercise available to healthcare organizations.

Start of the Scenario:

As part of reducing the exposure of employees to COVID and better complying with stay at home orders, many healthcare workers involved in backend office functions or in primary care roles were setup with remote access technologies and allowed to work from home. Telehealth technologies were also rolled out to primary care providers in order to allow them to continue to serve the community during the COVID crisis. Several primary care doctors were previously issued hospital laptops in order to securely facilitate the connectivity to allow working from home and had this type of access since before the onset of COVID. One such doctor had been issued a laptop for remote work many months ago. When he initially received the laptop he took it home connected it to his home's Wi-Fi network and tested to make sure he could establish a remote connection to the hospital. He then promptly powered the laptop off and forgot about it until COVID forced the need to work from home upon him. Unbeknownst to this doctor, his home network was infected with malware and when he pulled his hospital laptop out of the closest and powered it on, the laptop immediately connected to his home Wi-Fi network. The laptop, due to being powered off, was out of date with patches and AV signature updates and was soon compromised by the malware resident on his home network.

Questions to Consider:

1) Does your organization's remote access solution provide adequate isolation between the endpoints used to access the organization and the internal systems that are accessed? Was this ever tested and verified?
2) How are endpoints used to remotely access the organization protected?
3) How are endpoints used for remote access kept up to date with patches and other critical security updates?
4) Are there any controls that are not based on signatures present on these devices to limit compromise by malware in the absence of a signature for the threat (e.g. Software Restriction Policies, application whitelisting, DNS sinkholing, etc.).
5) If personal devices are allowed to establish remote access, what measures are taken to ensure they meet organizational security standards?
6) Is a Mobile Device Management (MDM) solution used to enforce any controls on personal or mobile devices used for remote access?
7) Is a compliance checker run, before allowing for a remote connection to be established?
8) What mechanisms are in place to detect a potentially compromised device that could be used for remote access?
9) If personal devices are used, are policies in place for the permission to obtain personal devices that may have been compromised to derive forensics? Are they part of the employment agreement or other "acceptable use" policy?

Inject 1:

The doctor takes his now compromised remote access laptop and uses it to establish a remote connection to the hospital. The remote access for the doctor and all primary care physicians had been expanded to include a larger number of systems in order to meet the increased work from home needs of the primary care workforce. As part of this rushed access expansion a slight misconfiguration was made and the doctor was granted network level access to more systems than intended, including access to legacy server that is used to collect telemetry data from a variety of bedside monitors throughout the hospital (This system

can be replaced with another system as appropriate for your organization). The legacy nature of the server combined with the remote access allowed the malware to spread from the doctor's laptop to the telemetry server.

1) Are there any controls in place to detect, prevent, and/or mitigate the spread of malware from a remote access endpoint to an internal system?
2) How are legacy and/or higher risk systems protected within your environment.
3) Would any of these controls likely be sufficient to detect such an attack? Have these controls ever been tested to ensure efficacy?
4) What kind of logging occurs for remote access traffic? Are logs audited with sufficient frequency?
5) Are these logs sent to and analyzed by a SIEM? Are there rules in place within the SIEM to detect traffic such as this? Have these rules ever been tested?
6) How segmented is your internal network? Are there other systems that this telemetry system could potentially communicate with that may become infected?
7) Is internal network traffic logged (e.g. Netflow data)? Is this Netflow data sent to a SIEM and does the SIEM have rules in place to detect anomalous traffic between systems (e.g. the telemetry server communicating with security camera system)? Have these rules ever been tested?

Inject 2:

The helpdesk receives a call from the doctor complaining that his laptop is slow and it's causing issues for him. Nursing is reporting that the telemetry system is running with delays and that results from the monitors are taking a few minutes to update on the server.

Questions to Consider:

1) Would these two events be correlated as having the same root cause at this point in time?
2) Would security even be involved in the conversation at this point?
3) Would IT be involved in troubleshooting both issues or would one issue be reported and looked into by IT and the other be initially handled by Biomed?
4) Would any one person be aware of both issues?
5) Would the performance issues be treated as isolated incidents or would the possibility of the issues spreading to other systems be considered?
6) At what point would this issue be considered an incident? Would this qualify as an incident at this point in time?
7) If any of your IT department or Biomed department is working remotely, how would this impact the time required to assess the issue?
8) How would remote work impact collaboration between the Biomed and IT teams in terms of troubleshooting?

Inject 3:

More legacy systems and systems that are not fully up to date on patches are starting to be reported as running slow. Patient care is beginning to be impacted.

1) Would the connection be made that these events are all likely related now?
2) Does the issue now meet the criteria for an incident?
3) Assuming an incident is now declared, what is the procedure for notifying all key stakeholders? Does your communication plan require any modification to accommodate a remote workforce?

4) Does your incident command structure need be reassessed depending upon what leadership is onsite vs. remote?
5) Are all key emergency numbers that ring to an onsite phone forwarded to the proper offsite party if no one is onsite to answer?
6) Is contact information current for the entire remote workforce?
7) Are emergency notification and other key incident handling systems reachable remotely? If they are cloud based, are the links known to staff responsible for accessing them in the absence of the bookmarks they have on their office PC?
8) Do you have a way to identify all systems that are missing patches?
9) How does having a remote staff impact the incident response process? Can investigation and containment activities be done remotely?
10) If remote access is one of the systems to go down, is there a contingency plan? Does IT and/or infosec have a secondary remote access method for redundancy?
11) Is there a plan for dealing with a potentially compromised system that cannot be accessed remotely?

Inject 4:

After investigation, it was determined that cryptomining malware had been spread through the organization and the CPU cycles spent mining cryptocurrencies were contributing to the slowness of hospital systems that become infected.

Questions to consider:

1) What is your organizational process for cleaning up malware infections? Can it be done remotely?
2) For cases where cleanup is not an option – What is your organizational process for backup and recovery? Are these systems reachable remotely?
3) Can desktops be reimaged remotely?
4) How does a remote workforce impact your communication strategy with regards to recovery efforts?
5) Can your organization recover with the same speed with a remote workforce?