Fighting COVID-19

Top eight areas overlooked while fighting COVID-19

March 2020

EY
Building a better working world

Top eight areas overlooked while fighting COVID-19

COVID-19 has already taken many lives across the world and has made its way to the US, where our health systems are already starting to see an influx of patients. As EY continues to meet with health systems throughout the US, we are recognizing a pattern of topics health systems' security teams are challenged by as they prepare diligently for the surge of patients. This is not a comprehensive guide how to prepare for COVID-19, but our observations of areas which are being commonly overlooked while dealing with the additional challenges presented by COVID-19.

1. How are you ensuring that you are protected against the increase in **cyber attacks** already seen by the Department of Health and Human Services (HHS) and local health systems?
2. Have you taken the appropriate steps to determine whether your **workforce** and infrastructure are set up to handle the significant increase in teleworking caused by government shelter-in-place directives?
3. Are your executives falling for targeted COVID-19 related **phishing** attacks?
4. Have you minimized the chance of **downtime** with your medical devices and infrastructure?
5. What else can you do to ensure that your network is able to withstand the surge of **traffic** caused by increased telework and a vast number of patients?
6. Are your **vendors** enabling you to get the medical devices needed and helping you fight COVID-19?
7. How prepared are you to make **critical decisions** in the absence of key employees sidelined by the virus?
8. Is your **communication** to your employees, clinicians and patients sufficient?

1) How are you ensuring that you are protected against the increase in cyber attacks already seen by the HHS and local health systems?

It is common that during a major event such as an election or pandemic there is an increase in attacks. On March 15, HHS was subject to a distributed denial-of-service (DDoS) attack by a foreign actor. It appears to have been targeted at shutting down the HHS to stifle the US' ability to respond to the coronavirus outbreak and to disseminate false information to cause public panic (on the web: Cyberattack against HHS meant to slow coronavirus response).

Just the week before, an Illinois health agency was hit by a ransomware attack that took the site down. Fortunately they had a robust disaster recovery strategy which allowed them to recover from the attack and minimize the impact (on the web: Illinois public health agency website taken down by hackers).

What you can do:

Monitor the rapidly evolving cybersecurity landscape (on the web: HIPAA Journal, US-CERT) **and take appropriate actions to mitigate the risks. Some of the new risks include:**

- **Understand the new risks**
  - Fraud schemes and cyber intrusion risks, such as criminals posing as medical and humanitarian groups to target organizations and victims (on the web: Cybercriminals impersonate World Health Organization and Cyber attacks in the health care sector
  - Phishing/business email compromise (BEC) – use of COVID-19 as a topic in phishing and spam emails to increase urgency in complying with requests, with the intent to spread malware (e.g., direct customers to fraudulent website, virus attachments), compromise systems, process illegitimate invoices quickly, etc. (on the web: Coronavirus-themed domains 50% more likely to be malicious)
  - Increased targeting of e-commerce platforms and patient portals – Stealing patients' personally identifiable and protected health information and using it to commit insurance fraud or fraud against the patient
  - Use of social media accounts to distribute malicious material or "fake news" – creation of similar but fraudulent accounts and topics to push misinformation and malicious activity across networks
- **Detect the attack by establishing new baseline** – as much of your nonclinical workforce is forced to telework and there have been significant changes to your clinical workforce, the everyday network traffic has changed. Monitor your network to establish a new "normal" baseline that can be used during this time of extended crisis. Recalibrate any monitoring settings (network, application, operating system) and alerts that need to be adjusted to accommodate this new baseline to assist with detecting cyber attacks. Validate whether any updates are needed to your current audit log settings
- **Be prepared to react quickly** – review your current incident management process and validate whether your escalation procedures are appropriate. During this time of crisis and increased cyber attacks, having the ability to react very quickly while still following security protocols is key. Confirm that backup approvers and decision-makers have been identified in the event that a key approver is not available
- **Tweak your risk-based approach to resilience** – confirm that your current recovery plans (including comprehensive backups) have been adjusted appropriately based on the many process and systems changes that have resulted from the major operating shift caused by COVID-19. Make adjustments to the process to incorporate things that are working well throughout the next few months as you operate in crisis mode. This will increase efficiencies and enable you to continue to operate effectively during the extended crisis period. If possible, keep operating documentation up to date so that an alternative person can take over in the event of illness

2) Have you taken the appropriate steps to determine whether your workforce and infrastructure are set up to handle the significant increase in teleworking?

With shelter-in-place and work-from-home directives by federal and local agencies, organizations are sending their workers home to keep them safe and help minimize the spread of COVID-19. Health systems might not be prepared for the shift from in-office to remote settings.

What you can do:

- **Centrally manage and promulgate robust secure teleworking solutions** – this should include the use of virtual private networks (VPNs) and multifactor authentication as your remote workforce will still be accessing sensitive and confidential data
- **Encourage the use of collaborative platforms** – remind your workforce of any collaborative platforms available to them and determine if other web based solutions can deployed quickly if needed. This may include video conferencing tools, secure portals for accessing sensitive data and protected shared drives to securely share information
- **Telework guidelines** (on the web: NIST Guide to Telework) – increase communication to your workforce regarding how they can be successful working from home. This includes reminders about security protocols (e.g., must use secure shared drives and not personal email address) and instructions on how to use the collaborative tools
- **Provide links to official pandemic resources** – during this time, it is critical that both your workforce and your patients have access to the information they need to keep themselves updated and safe. This includes providing links to the most recent COVID-19 updates, official government sites such as the Centers for Disease Control and Prevention (CDC), internal communications regarding the pandemic and all other resources that allow people to continue to prepare for COVID-19. These should support enabling them at work and preparing their families for what is to come
- **Increase your formal channels for organizational messaging to increase transparency** – communication is key during a pandemic to be able to continue to operate at the heightened level and minimize chaos, confusion, misinformation, and the fear and anxiety associated with fighting a global pandemic
- **Be vigilant of new risks evolving as the result of a surge in teleworking. These risks include:**
  - **Insecure practices favoring availability over security**
    - **Unmanaged software/assets** – users unhappy or unfamiliar with approved telework solutions may install or set up their own "shadow IT"
    - **Patch deferrals** – increased load on telework-enabling resources may limit allowable downtime for patching. Confirm that you have not overlooked deploying any critical patches as you may have already deferred non-critical patches during this time
    - **Network "flattening"** – ensure that connectivity between cross-enterprise resources do not circumvent segmentation
  - **Dispersal of previously in-person activities and processes**
    - **Change in network baseline** – remotely performed high-privilege actions could trigger alarms. Establish a new network baseline to accommodate the shift in telework and clinical schedules and workload to minimize false alerts
    - **Increased load on help desk and IT which may increase risk**
      - New teleworking users may flood the help desk, creating pressure to skip authentication/authorization steps
      - Fraud attempts to leverage help desk support for further malicious activity (e.g., password reset, adding/changing contact information, provisioning access to resources)

3) Are your executives falling for targeted COVID-19 related phishing attacks?

There has been an increase in using COVID-19 as a topic in phishing and spam emails targeting health care organizations, specifically corporate executives. These attacks use the coronavirus to demonstrate a false sense of urgency, requiring the executive to click on a link, download a file and/or respond with sensitive information, thus spreading malware.

What you can do:

- **Inform high-ranking personnel** – as we have noticed an increase in phishing attacks targeting executives, reach out to your corporate executives and inform them of these most recent phishing attacks. Provide them with tips that they can use to distinguish between a real email vs. a phishing email and where they can forward the suspicious email
- **Security awareness and communication**
  - Conduct a very brief phishing and security awareness refresh. This should include updating your entire workforce on the recent COVID-19-related phishing attempts and refresh them on various phishing techniques like URL redirects, embedded links and malicious email attachments. Employees should know what to do when they suspect a phishing email, the people they can contact with any questions or concerns, and what to do if they click on an attachment or link.
  - Increase organization-wide emails outlining different types of phishing attacks to watch for, what to do to avoid these schemes and how to respond once receiving and/or opening a phishing email. Include examples of the latest-known scams and phishing techniques, directing employees to websites like (on the web: FraudWatch International), which lists recently validated phishing accounts and can be useful for general awareness. Use various ways of communicating, including email, announcements, daily newsletters and management meetings. Consider conducting a mandatory conference call with all employees to inform them of recent phishing attacks. Provide tips that they can use to increase awareness
- **Inform patients** – just as you are being targeted as a health system, so are your patients. Develop broad communications to your patients informing them of known phishing attempts and how they can determine whether an email that they receive is legit. Remind them that you will never contact them via email to get personal and/or health-related information
- **Continue to respond to phishing attacks** – given the increase in cyber and phishing attacks, determine whether additional resources are needed to enable you to respond quickly. Identify the malicious email, see who has been targeted and immediately remove it from mail servers and employee mailboxes. Determine whether anyone in the company has fallen victim to it and clicked on fraudulent links, installed infected files, etc. Determine what has been compromised and take steps to investigate and minimize the impact done, following your emergency incident management processes and team. Increase communications to the health system as a whole regarding the specific attack that targeted your health system to help minimize the risk of others falling for the same attempts. If possible, increase training around phishing attacks for your employees to help minimize future incidents. Remember, if you suffer a security breach, having a well-planned response to stop the spread and minimize the impact is key

4) Have you minimized the chance of downtime with your medical devices and infrastructure?

As you prepare for an influx of patients, review your medical devices that have been in storage to determine whether they are operational and ready for immediate use for patient care. It is not uncommon for an organization to overlook recalls and vulnerabilities for their medical devices that have been in inventory and not recently used. It is critical that preparation is done to confirm that a device is safe and operational before it is needed. (on the web: Medical Device Cybersecurity)

What you can do:

- **Assess medical devices not in use to determine operability** – given the surge of patients, any medical devices available to treat COVID-19 patients will be needed. Devices that may have been in inventory or recently purchased may not have gotten the most recent patches and may not have been checked for recalls. Make sure your devices are up-to-date with recent security patches and that they are operational before they are needed in the very near future
- **Track your medical devices** – as you acquire new medical devices and start to use ones that have been in storage to assist with the influx of patients, make sure that your tracking and inventory of the devices is kept up to date. This includes knowing where medical devices are, your inventory of what exists and detailed information about the devices. Determine whether there have been any defects or recalls with the device and that the software managing the device is updated
- **Prioritize vulnerabilities requiring immediate attention** – prioritize and remediate vulnerabilities based on a combination of threat intelligence, exploit availability, vulnerability data and asset criticality. Devices with the highest risk to patient care, data privacy and operations must be prioritized for immediate attention before they are needed at hospitals. For devices in use, determine whether the vulnerability risk identified warrants the downtime needed to patch the device; https://nvd.nist.gov/vuln/full-listing (on the web: ICS Advisory, Most Dangerous Hacked Medical Devices, FDA issues warning, Heath industry cybersecurity practices, NIST vulnerability database)
- **Reach out to device manufacturers** – initiate communication with medical device manufacturers regarding any known vulnerabilities, misconfigurations and other weaknesses. The influx in vulnerabilities in medical devices can be attributed to the lack of data sharing that goes on between medical device manufacturers and health care organizations (on the web: Cybersecurity in Medical Devices, FDA medical devices, H-ISAC med devices, ICS-CERT advisories)
- **Update anti-malware software** – where applicable, ensure that all devices have up-to-date anti-malware software and appropriate security controls
- Manage passwords – change the default passwords of medical devices, as they can be more prone to being targeted in cyber attacks due to the common practice of not changing default passwords on internet-connected devices
- **Segment and segregate** – refrain from connecting devices with known vulnerabilities to the network. Keep end-of-life (EOL) devices off the network. If EOL devices are to be used due to the urgency of the situation and require network connectivity, connect devices to a segmented and segregated network
- **Update VPN critical vulnerabilities** – if applicable, apply a software patch to fix a remote code execution (RCE) vulnerability. Multiple vulnerabilities were discovered in the Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS) VPNs. This includes an authentication bypass vulnerability that can allow an unauthenticated user to perform remote arbitrary file access on the PCS gateway (on the web: FBI Security Alert: VPN)

5) What else can you do to ensure that your network is able to withstand the surge of traffic caused by increased telework and a vast number of patients?

Health systems are designed to support temporary surges of patients that they may get in the event of a disaster and/or outbreak such as a bad influenza season. In general, health systems are not prepared or designed to handle something as large as the COVID-19 pandemic, and it is unlikely that you will have the capacity, health practitioners and equipment to handle the surge. Taking immediate action to prepare for capacity increases is needed to be able to effectively manage the pandemic. (on the web: Protecting the Healthcare Digital Infrastructure)

What you can do:

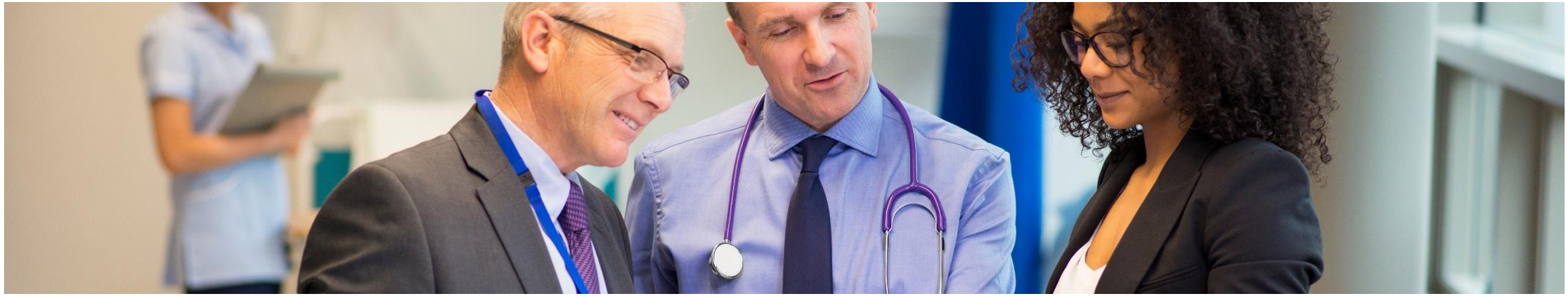
- **Confirm whether current infrastructure is properly supporting increased traffic** (on the web: Cyber Resilience Review) – review your infrastructure to determine whether it is set up to accommodate the increase in traffic and remote users. Consider the following:
  - What is the maximum number of remote users we can support, and do we need to implement additional network appliances to accommodate more?
  - Do we have enough bandwidth to support increased traffic and, if not, how quickly can we get it? This would include both employee networks and patient networks
  - Do we have enough licenses for the tools and software that are needed to accommodate the shift to employees working remotely?
- **Refocus resources and accelerate the onboarding and IAM access requests** – given the size of the potential influx of infected patients, health systems are asking retired nurses and other health care practitioners to assist with patient intake and treatment during the expected surge. These practitioners will need to be quickly onboarded and granted access to the systems that would allow them to do their jobs. There may also be practitioners who will be relocated from lightly hit areas to those impacted the most and will be included in the population of onboarding and access requests. Determine what an appropriate accelerated process would be for handling a large number of these requests within a short period
- **Surge of patient inquiries** – make any needed adjustment to assist with the influx of questions and confusion a pandemic brings. This may include setting up a help desk (or increasing resources) that is available to potential patients who are sick and require guidance on their next steps. Actions may include going to a testing center to confirm diagnosis, self-isolation, going to a local urgent care center, going to the nearest hospital or going to an alternative site designed to specifically quarantine coronavirus patients
- **Resource and equipment limitations** – inventory the equipment available that may assist in the treatment of coronavirus patients (e.g., personal protective equipment (PPE), ventilators), and work with local and state authorities to determine the estimated number of patients you may see over the next few weeks and months. Shortages should be communicated immediately and frequently. Requests to the state and federal governments for access to any available equipment stockpiles they have (e.g., PPE, ventilators) should be made quickly, as many health systems will soon be overwhelmed and looking to do the same. Revise your plan for how shortages are handled (e.g., reaching out to vendors for additional supplies)

6) Are your **vendors** enabling you to get the medical devices needed and helping you fight COVID-19?

Collaborating with your current vendors is critical during a time when there are increased cyber attacks, widespread illness in workforces, and shortages of critical medical devices and protective equipment.

What you can do:

- **Validate vendor services** – take proactive actions to validate that current vendors are able to provide uninterrupted supplies and/or services. Ensure that large vendors who supply and service many health systems have your organization as a priority. If not, determine what, if any, actions may be taken to move up their priority list
- **Collaborate with vendors** – determine how vendors are impacted by the coronavirus, how that may impact the service they can provide to you and how they can assist you with the various challenges you are currently facing (e.g., a system and organization controls (SOC) vendor adjusting its baseline to include the new "norm" of increased activities while working to identify threats) (on the web: COVID-19: How to protect your supply chain). Consider the following:
  - Review your current inventory levels to locate critical gaps in supply
  - Define actionable immediate activities with your vendors to support your business's day-to-day operations
  - Define short-term action plan items for the immediate future to ensure continuity of your health care business and services as this crisis persists
- **Find alternate vendors** – take proactive actions to pursue and align secondary vendors for supplies and services in the event that current providers are unable to meet the needs of your organization
  - Be cautious – Interpol warned that criminals are running financial scams by posing as medical distributors who claim to be selling masks and other supplies. In some cases, fraudsters posed as hospital officials in order to request payments for care given to relatives (on the web: Scammers Launch Coronavirus-Themed Attack)



7) How prepared are you to make critical decisions in the absence of key employees sidelined by the virus?

During a pandemic, there is a large shift in the standard operating procedures for health care systems. The shift into crisis management changes the overall strategy of how to treat patients and how to operate as an organization. It is not uncommon that key business leaders and clinicians may get sick themselves and not be available to make critical decisions. It is essential that these worse case scenarios are discussed and a plan is in place before key members of the workforce are not available to continue operations. (on the web: COVID-19 and pandemic planning: How companies should respond)

What you can do:

- **Critical business and clinical processes** – confirm which functions are essential during a crisis. These would be processes and operations that are needed to ensure patient safety, develop a treatment plan for a patient and treat the patient. This also would include the supporting infrastructure needed to assist those critical processes, such as payroll, procurement and IT (on the web: Reshape results and plan for COVID-19 recovery)
- **Essential personnel** – confirm which functions are essential during a crisis and who is responsible for executing and managing those key processes. For each of those critical team members, identify a secondary and tertiary person who will operate in that role if the person becomes ill or is not available to continue their responsibilities. Set up the secondary and tertiary resources with any information, documentation, tools, etc. they will need to successfully take over the role, and make sure they have adequate training and understanding of what their new duties are.
- **Inform personnel** – to reduce confusion, communication must be frequent. Inform personnel of any change in reporting structure, who has taken over making critical decisions in the area impacted by the unavailable personnel, and how they need to change their operations to accommodate for the reduced workforce and change in management during the pandemic. This is also true for when essential personnel recovers and re-enters the workforce after illness

8) Is your communication to your employees, clinicians and patients sufficient?

During a pandemic, anxiety and panic is at an all time high. People are worried about whether the hospitals can accommodate the surge of patients and whether you can provide quality care for their family if they get sick. Your employees, clinicians and patients want to know that you are there for them and making your best effort to support them in any way possible (medically, mentally, financially).

What you can do:

- **Communicate COVID-19 related resources to your workforce and patients** – misinformation, or lack of information, creates an environment of anxiety and panic. Provide your workforce and patients with reliable resources they can use to keep up to date on COVID-19 and how it may impact them and their family
- **Increase employee and patient support** – during a time of global crisis, everyone will need additional support. Consider the following:
  - Is our paid sick leave appropriate in this pandemic situation or does it need to be temporarily adjusted?
  - Do we have a mental health crisis hotline that our employees can call? Do our employees have access to mental health services through the health system's insurance program?
  - Should we consider offering or modifying our financial assistance available to our employees? This may include rewarding employees with a small bonus recognizing their dedication and increase in hours, which may be needed to cover their personal COVID-19 related expenses (e.g., increased doctor appointments, quarantine supplies, medications)
  - Are there other accommodations we can do to help our employees (e.g., employer loans, mental health assistance, paid sick leave)?
- **Communicate how you are supporting your workforce and patients** – it's not enough to tell your workforce and patients that you are there to support them. You must demonstrate how you are doing that and provide frequent updates as situations change very quickly. Communicate the following:
  - How you are keeping your clinicians safe during a time when COVID-19 is rampant. This may include your quarantine procedures, how you're addressing the PPE shortages, hospital intake procedures, any updates to how patients are prioritized and who gets equipment during shortages, etc.
  - How you are supporting your workforce. This includes both the regular employee assistance program and any additional assistance you are providing. Be clear on the medical, mental health and financial resources available to them as all may be needed during this time

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EYG no. 001482-20Gbl
ED None

ey.com