Information Technology Considerations for a Disease Outbreak

Prepared by the AEHIS Incident Response Committee

Committee Chair: Christopher Frenz
Vice Chair: Sonia Arista

Participating Members:
Florin Petrutiu
Dee Young
Tomislav Mustac

Introduction

With the recent outbreak of the Coronavirus (COVID-19), the prospect of a disease spreading exponentially is currently a high probability. As such, health systems need to be prepared to handle the potential impact on their operations. This guide is designed to highlight some of the information technology (IT) and information security (IS) issues that organizations should consider as part of their preparations for an epidemic outbreak. Some of the issues discussed are "worst case scenarios" but should be considered for planning purposes.

Supply Chain Shortages

With the bulk of the Coronavirus outbreak occurring in a region of the world responsible for the large-scale manufacturing of technology products, organizations need to be aware that there is the potential for certain technology resources becoming increasingly expensive or difficult to acquire. As many health systems are likely discussing the impact on supplies directly effecting patient care, considerations for technology supply also needs to be discussed.

It is recommended that organizations consider expanding their supply of in-house replacement parts and replacement systems in order to have a large enough supply to cover three to six months of component failures. Organizations need to consider this for both IT technologies as well as supplemental or ancillary technology used for supporting medical devices, Internet of Things devices (IoT), and core Operational Technology (OT) devices, such as but not limited to refrigeration units, physical campus security and lab technology.

Organizations may also want to consider delaying any noncritical system and application upgrades or technology refresh activities for a period of time when the critical status of the situation has passed. Organizations should also review their stock replenishment trigger points to allow for delays or disruptions in the supply line and consider backup sources for critical supplies.

Labor Shortages

If the Coronavirus contagion increases within the U.S., it is critical to remember that staffing may be at a heavily reduced level as employees may be calling in sick due to illness or fear of contracting illness. IT and biomed departments should ensure that staff are cross-trained to a sufficient extent so that an unplanned for or extended outage of one or more employees does not critically impact operations.

Likewise, the organization may have to consider that consultants or other third-party individuals may need to be brought in to cover any staff shortages in order to maintain an appropriate level of service. In the context of staffing, IT and biomed departments may want to vet some such services ahead of time. This will expedite third-party staff onboarding should normal IT personnel become unavailable in a large enough number that services are impacted, or if a surge in temporary workers requires an increased helpdesk footprint.

To address the potential increased use of third-party staff overall (i.e., from any department), and to accommodate any government or municipal agencies needing access to systems, IT departments should review their employee onboarding procedures, such as user account provisioning, credentialing of doctors, permissions assignment, etc., and look for ways any efficiencies could be added to the systems in order to help quickly onboard a potentially large number of temporary workers. In parallel, given that this will be a temporary workforce, account termination procedures and other exit procedures need to be reviewed as well to ensure the organization minimizes the risks of having a large number of accounts created. Auditing procedures for records access by the temporary workers should also be implemented to ensure that the changes in process do not inadvertently lead to a potential security incident.

Business Partner Considerations

The Coronavirus has rapidly developed into a global issue and hospital supply chains are dependent on business partners that have global facilities and subcontractors. If the outbreak continues to spread, there is the possibility that one or more business partners suffer staff shortages or other disruptive issues as a result of the outbreak. Organizations may want to ensure their critical business partners, those whose operations may have a direct impact on patient care or payment and billing processing, have taken appropriate measures to maintain adequate levels of trained staff and have adequate physical and information security controls in place to handle any potential unrest in their vicinity. It would be prudent to consider how a surge of potential cases would fold into operational workflows and create action plans for deployment in the event that the need is realized. Organizations may also want to plan for the possibility that some smaller sized business partners may become completely unavailable.

Telecommuting

If the outbreak affects the region that your organization operates in, the possibility exists for a larger portion of your work force to be seeking to or be asked to telecommute into work as an alternative to physically coming into work. It is advisable for organizations to check that their remote-access capacity is sufficient to meet their needs (bandwidth, server capacity, firewall throughput, etc.), and to revisit their remote access security controls to ensure that they are up to current industry standards. If systems are being made remotely accessible to help support remote workforces, organizations may want to ensure that all internet accessible systems are protected by Web Application Firewalls (WAF), ensure that VPN gateways are fully patched and properly configured, and that all remote workers credential through Multi-Factor Authentication (MFA) for systems access. Organizations may also want to increase their monitoring of their network to help detect and filter illegitimate access attempts to hospital resources.

For healthcare facilities that actively are receiving new potential cases, or those that are located inside confirmed community-spread locations, it would be prudent to consider asking a portion of the IT/IS departments to self-quarantine and work remotely. This action would limit exposure of critical employees while they can still provide highly skilled support from a remote location or be brought in as replacements for sick employees.

Physical Security

If an outbreak were to occur in your region it is highly likely that your hospital may have a much higher patient volume and overall higher throughput of people than normal. Physical security controls should be assessed to ensure that they are sufficient to prevent the theft of information assets, medical devices and other hospital resources. As with labor shortage suggestions above, physical security departments may want to vet some third-party services in advance that could serve as a source of additional staff in the event a labor shortage occurs or the higher patient volume demands an increased amount of security staff. Logical areas for supplemental resource planning would be the emergency department, primary care clinics, public spaces and the laboratory (for diagnostic testing). Organizations may want to consider creating plans surrounding which facilities and services could potentially be shut down to alleviate some staffing and resource constrains.

Test Business Continuity and Disaster Recovery Plans

While testing business continuity (BC) and disaster recovery (DR) plans should be a routine part of operations, with the potential surge of clinical operations pending it is especially prudent to assess BC and DR plans to ensure they can be effectively carried out. Given the potential for employee shortages, extra attention should be paid to ensure adequate cross-training or other contingency plans are in place. Organizations should also consider the possibility of multiple-risk scenarios occurring at the same time and the effects they would have on resourcing.

Mass Notification

Healthcare systems may want to ensure that they test their mass communications systems and procedures to ensure that they can get critical information into the hands of staff as quickly and efficiently as possible. They may also want to ensure that mass notification systems extend beyond using just hospital contact information as a means of alerting employees as it may be beneficial to reach employees en masse at home if closures of certain facilities are occurring or if staff shortages require off-duty employees to suddenly report in. Healthcare providers may want to consider a supplemental process to allow for employees to rapidly report or seek care if they are showing signs of infection, and subsequent processes should be outlined for investigation into impact on patients and staff.

Employee Education

With examples already appearing using fake Coronavirus alerts to spread malware and launch phishing attacks, it is highly beneficial to ensure that all employees are reminded of the risks of such attacks and the tactics commonly used by scammers. In particular, employees should be alerted to the risks of fraudulent emails pretending to be from the Centers for Disease Control and Prevention, other government agencies or healthcare organizations pretending to contain

Coronavirus information. It is advisable that organizations provide links to information resources to reduce the risk of clicking on malicious links or visiting malicious websites.

It is expected that other related scams will appear that may include the fake collection of donations for Coronavirus victims and theft of supplies; employees should be warned of these risks as well. If certain resources like face masks become scarce, then organizations may want to considering that phishing and other scams promising access to such resources will likely become commonplace.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule protects the privacy of patients' health information but it is balanced to ensure that appropriate uses and disclosure of such information may be made when it is used to treat the patient, protect public health and other critical purposes. The Office for Civil Rights of the U.S. Department of Health and Human Service released a bulletin titled: HIPAA Privacy and Novel Coronavirus that reminds providers of the do's and don'ts during an outbreak. This bulletin can be downloaded at: https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf. To ensure proper adherence to the HIPAA Privacy Rules and reduce potential inhibition of care, it is advised to circulate this bulletin or create similar guidance for health professionals to follow.

Education of employees for proper hand hygiene is a proven method to limit the spread of the disease. This is especially important for IT support personnel who interact with other-than-their-own devices and could be at a higher risk of exposure.

Electronics Disinfection

All departments should review their procedures for the disinfection of electronics and ensure that adequate supplies are available to disinfect a larger that normal number of systems that may result from surges in patient volume. This should include clinical departments as well as biomedical engineering. Particular attention is needed to address sanitation of mobile devices that are handed off by workers between shifts or handed from patient to patient. Frequently accessed doors and surfaces (like IT room access doors, shared keyboards in server rooms, etc.) should be cleaned and disinfected on regular basis.

Personal Protective Equipment (PPE)

Hospitals need to remember that biomedical and IT staff members are often sent onto patient floors to repair a computer and as such are also likely to come into contact with various infection vectors. Hospitals should ensure that all employees are versed in the hospital's infection control procedures and have access to the necessary PPE equipment to safely perform their job functions. It is advisable that organizations closely monitor their inventory levels to ensure that they are adequate to increased usage as well as additional users of these supplies.

It is further advised to limit IT staff members' access to patient areas (waiting rooms, treatment areas, patient rooms) in order to limit their exposure as well as limit the consumption of PPE and related supplies, unless necessary to actively respond to an outage.

Conclusion

Given the potential impact on normal operations and to the community in general, healthcare organizations have a responsibility to maintain current and trusted situational awareness of the impact of the contagion, and at least have initial conversations within the supply chain, information technology and security teams on some of the above recommended topics. Talking through various scenarios with your teams and thinking ahead about contingency planning for events specific to your organization are highly recommended.