2019
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

A Lifeline: Patient Safety & Cybersecurity

2019 Public-Private Analytic Exchange Program

Vulnerabilities of

Healthcare Information

Technology Systems

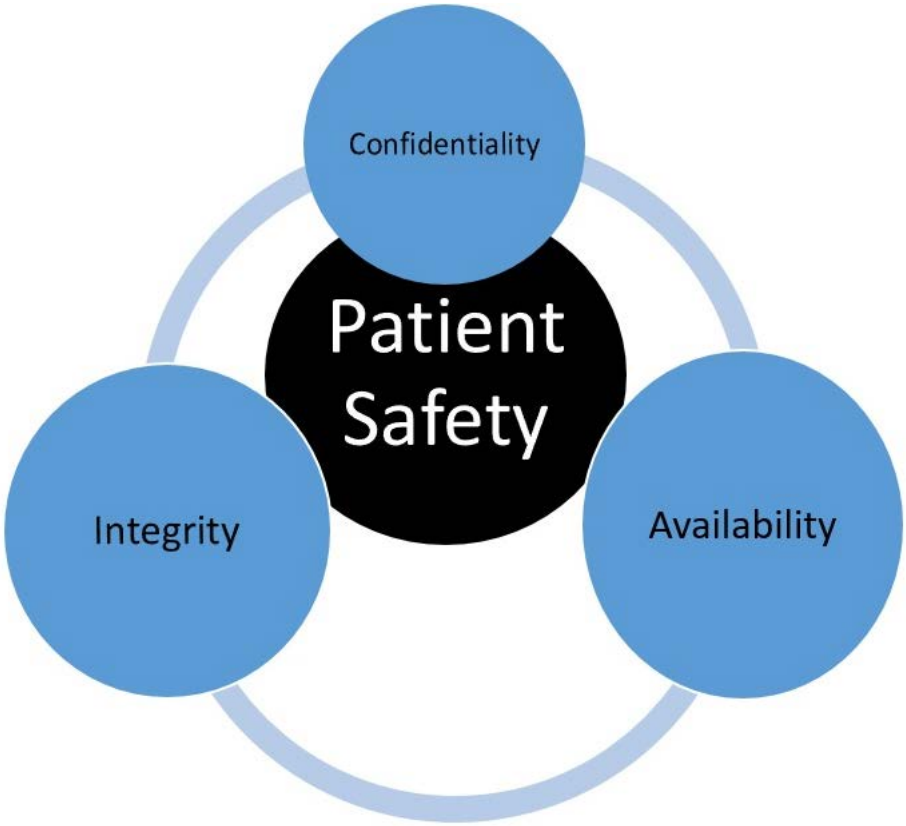

Table of Contents

Acknowledgement

We acknowledge and thank the federal government agencies and companies that supported the development of this paper. We also thank the Office of the Director of National Intelligence (ODNI) and the U.S. Department of Homeland Security (DHS) for the opportunity to have participated in the 2019 Public-Private Analytic Exchange Program (AEP).

2019 AEP Public-Private Team Members – Vulnerabilities of Healthcare Information Technology Systems

- William Pachucki, CISSP, U.S. Department of Health and Human Services
- Michele Krajewski, Deputy Director, Health Care Security Requirements (HCSR), Veterans Health Administration
- Bruce de'Medici, Grey Oar
- Chris Letterman, Wostmann & Associates
- Hany Wassef, Meritor
- Jenifer Clark, Costco Wholesale
- Kevin Littlefield, MITRE Corporation
- Lee Kim, JD, CISSP, CIPP/US, Healthcare Information and Management Systems Society

People and Organizations Consulted

We are grateful to the following individuals that provided information and expertise for this report:

- Al Roeder, Branch Chief Advanced Cyber Defense (ACD), U.S. Department of Health and Human Services
- Axel Wirth, CPHIMS, CISSP, HCISPP, AAMIF, FHIMSS, Chief Security Strategist, MedCrypt
- Bayardo Alvarez, IT Director, Boston PainCare
- Bob Bastani, Critical Infrastructure Protection Division, Assistant Secretary for Preparedness and Readiness, U.S. Department of Health and Human Services
- Greg Singleton, Director Health Sector Cybersecurity Coordination Center (HC3), U.S. Department of Health and Human Services
- James Antonucci, Director Security Operations Division, U.S. Department of Health and Human Services
- Janet Vogel, Chief Information Security Officer, U.S. Department of Health and Human Services
- Jay Angus, Industrial Control Systems Vulnerability Management and Coordination (ICS-VMC), National Cybersecurity and Communications Integration Center (NCCIC), Cybersecurity and Infrastructure Security Agency (CISA), US Department of Homeland Security (DHS)
- John Rasmussen, MA, MBA, CISSP
- Julie Chua, Chief Risk Management Branch, U.S. Department of Health and Human Services
- Nick Heesters, Office for Civil Rights, U.S. Department of Health and Human Services
- Richard Staynings, Cybersecurity Evangelist and Chief Security Strategist, Cylera
- Seth Carmody, CDRH/OST/DARSS, U.S. Food and Drug Administration
- Suzanne Schwartz, Deputy Director Office of Strategic Partnerships & Technology Innovation, Center for Devices and Radiological Health, Office of Strategic Partnerships and Technology Innovation, Division Director (Acting) All hazards Response, Science and Strategic Partnerships, U.S. Food and Drug Administration
- Verne Rinker, Office for Civil Rights, U.S. Department of Health and Human Services

Executive Summary

Healthcare information is unique and personal to us all. Indeed, the patient is at the center of healthcare, as it would not exist if the patient did not exist. Bits and bytes in today's digital world have real significance when it comes to patient care as patient lives are on the line. Any disruption, corruption, or leak of data may significantly alter the course of patient care for affected patients—with the potential for adverse consequences. As a result, patient safety is directly tied to cybersecurity in today's digital world.

Yet, many people within the healthcare sector have not made the connection between patient safety and cybersecurity. Relatively little is known about the impact on patient safety as a result of lax cybersecurity. Yet, the loss of even a single patient's life as a result of lax cybersecurity would be one person too many. Computers can be replaced, but people cannot.

Patient safety should be a paramount objective for any responsible steward. This includes those of us that are entrusted to safeguard patient data. Otherwise, patient lives may be at risk if we are not responsible stewards. We must mitigate the risk to patient safety by ensuring the confidentiality, integrity, and availability of patient data. We need to make certain that the right data is being accessed by the right person at the right time for the right patient. Otherwise, patient care may be impacted in some way, whether directly or indirectly.

Through a series of virtual and in person interviews, literature reviews, and other engagement, we examined the nexus between patient safety and cybersecurity from various facets. Based upon our research, we learned that in order to protect the patient, we must protect the patient's data as well.

An Introduction to Patient Safety and Cybersecurity

Patient safety is defined as the prevention of errors and adverse effects to patients. [1] Cybersecurity is defined as the ability to protect or defend the use of cyberspace from cyber attacks. [2] Three attributes that are critical for secure systems are confidentiality, integrity, and availability of data. [3] This is also known as the confidentiality, integrity, and availability (CIA) triad.

Confidentiality involves ensuring that access is appropriately restricted to sensitive data. [2] In healthcare, this includes information such as protected health information (PHI), which is governed by HIPAA and other applicable state and Federal laws, personally identifiable information (PII), and intellectual property (IP).

Integrity involves guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [2] Information must be trustworthy and reliable. The right data must be associated with the right patient.

Availability involves ensuring timely and reliable access to and use of information. [2] The data must be accessible and usable on demand. Availability helps to ensure that the patient data can be accessed or used at the right time (i.e., as requested or required).

Nonetheless, even though many hospitals prioritize securing patient data, it should not come at the expense of patient safety. Further, the devices, infrastructure, and specific medical information relating to a certain patient will be targeted when an attacker targets a patient's health. Thus, the cybersecurity practitioner's thinking of what needs to be addressed may shift, depending upon what the concern is. [4]

A leak or breach of personally identifiable information may be a different concern from a leak or breach of protected health information. Moreover, a leak or breach of intellectual property (IP) or proprietary information of an organization is quite a different endeavor as well. These are also quite distinct from a situation in which a patient's health may be targeted by an attacker. Thus, depending upon the motivation for the attack (i.e., PII, PHI, IP, or patient health), the defensive strategy may change accordingly. [4]

Level Setting: Nexus of Patient Safety and Cybersecurity

Healthcare technological advances seek to improve patient experience and outcome. Hospitals are complex environments, and many of the technologies deployed in a hospital infrastructure focus on the patient experience and are fundamental to patient treatment. Furthermore, healthcare delivery organizations operate complex infrastructures that include systems supporting clinical information systems, medical devices, clinical staff support systems, financial billing systems, physical security systems, and heating, ventilation and cooling systems, with central systems housed in a common physical plant, all using technologies that allow communications to vendor support networks, satellite facilities, academic networks, and the public Internet. Healthcare delivery organizations also integrate with third-parties providing clinical care, first responder services, medical coding and billing support, cloud hosted service providers, and sometimes even to the patient's home. Accordingly, securing the healthcare ecosystem can be quite complex.

Additionally, hospital information systems may include electronic health record (EHR) systems, radiology information systems, and scheduling systems, where the need for confidentiality and data integrity are vital. These are examples of systems that run on computers such as workstations, servers, and mobile devices—many of which are not directly patient-facing, but which nonetheless have some sort of impact on the patient, albeit indirectly.

However, there are many other types of computer-enabled technology that the patient may interact with or otherwise come into contact with at some level within the hospital environment. Examples of such technology include HVAC systems, physical access systems, and medical devices. These devices may have a direct or indirect impact on patient safety, depending upon the circumstance. Some examples of what could potentially occur are listed in the hypothetical scenario section of this paper below. Thus, strategies associated with patient safety and cybersecurity should align given the nexus between the two.

Current State of Patient Safety and Cybersecurity

Hospitals are well versed with dealing with patient safety issues when adverse events happen from a traditional people and process perspective. Errors, accidents, and close calls may be carefully reviewed, as well as lessons learned, but little attention is given to potential cybersecurity issues. For example, the root cause of a device malfunctioning may have been a cyber attack or compromise and this malfunction may have led to the serious injury of a patient or a patient's demise. However, because many in the healthcare sector have not yet made the connection between patient safety and cybersecurity, situations such as these are not recognized and are thus ignored. The number of serious adverse events or patient deaths are largely unknown as mechanisms generally do not exist to examine such problems within the context of cybersecurity concerns.

Despite the disconnection between the two worlds of patient safety and cybersecurity, those in the healthcare sector are significantly concerned about patient safety and cybersecurity—but mainly as separate topics. In terms of cybersecurity, however, those of us in the healthcare sector are now acutely aware that cyber attacks are rampant. Prior to nation state actors targeting a hospital system in 2014 [5], however, many of those in healthcare refused to believe that anyone would want to target a hospital given the noble purpose that we have—saving patient lives.

According to a recent industry survey, hospital leadership teams have indicated that their top priority is patient safety with privacy, security, and cybersecurity being the second priority. [6] Other industry surveys have indicated that the vast majority of hospital respondents indicate that their organizations have been victims of cyber-attacks and/or significant security incidents. [7, 8]

Why Patient Safety Must Evolve with Cybersecurity

We have seen the impact of patient safety as it relates to cybersecurity in recent times. Examples include WannaCry. Some of the England National Health Service (NHS) organizations were infected with WannaCry. The WannaCry ransomware attack affected at least 80 out of 236 trusts across England. These NHS organizations could not access important information and electronic systems, including patient records, and had to cancel appointments and operations. Some trusts had to divert patients to other accident and emergency departments. NHS did not report any cases of harm to patients or of data being compromised or stolen. [9] Nonetheless, there was some impact on patient care.

According to reports, NHS England's view was that WannaCry infected some parts of the NHS because such organizations failed to maintain good cybersecurity practices. [9] All NHS organizations infected by WannaCry, at the time, had unpatched or unsupported Windows operating systems. [9] Furthermore, auditors noted that taking action to manage Internet-facing firewalls would have guarded these organizations against the infection. [9] NHS has since focused on lessons learned from WannaCry, including adopting appropriate proactive measures.

By the same token, when the NotPetya cyber attack occurred, some surgeries had to be postponed due to this cyber attack. [10] Indeed, it is a critical time for the healthcare sector to make the connection between patient safety and cybersecurity. [11] Patient safety is a cybersecurity issue in today's digital health world. [11]

In light of these examples, patient safety and cybersecurity must evolve together to ensure that patient safety is either not impacted or mitigated to the greatest extent possible—if and when a significant security incident occurs.

Hypothetical Scenario: Patient Safety and Cybersecurity

Across the nation, every day, people from all walks of life place their trust and their own lives into the hands of healthcare providers. The healthcare and public health sector is unique in that it touches virtually everyone. At some point in our lives, we are all patients across a continuum of care. We expect that our patient data will be kept safe and secure. Yet, we know that this is not always the case. However, few of us realize how fragile the healthcare system is, especially when it concerns cybersecurity within the context of patient safety. Unless leadership within our institutions come to realize that patient safety is a cybersecurity issue, patient lives may unnecessarily be at risk.

To help illustrate the problem, the following is a hypothetical (i.e., fictional) situation:

On a bitterly cold day, the polar vortex hit the northeast and caused many power outages and disruptions. A community hospital experienced a significant power outage for a prolonged period of time. Fortunately, however, the community hospital has two fuel-based power generators. As luck would have it, though, only one fuel-based power generator was operational as the other generator was struck by lightning three months ago and is still out of operation. Only critical systems are plugged into red outlets. Many systems, however, run on regular power.

At this particular community hospital, the hospital's employee entrance uses a proximity card reader. To help deter unauthorized entry, the proximity card reader system is designed to fail secure in case there is a loss of power (i.e., the door is locked when power is lost). Employees must press a button to call for assistance from the hospital's security department. Since this hospital has lost power, a group of employees could not get into the building via the employee entrance and instead have to press the button to call for help from the hospital's security department or walk to the emergency room entrance (which is open to visitors with a security guard at the front entrance). In either case, valuable time is lost waiting for assistance in trying to gain access to the hospital. Meanwhile, patient lives are on the line and are potentially at risk because critical team members are deterred from entering the hospital—at least for awhile.

In this case, it takes more than 10 minutes for a security guard to get to the restricted employee entrance, due to the distance between the employee entrance and where the security guard is stationed. It is very cold outside and the group that has gathered is unwilling to wait anymore. The group then heads over to the emergency room entrance. Members of the group say wave or nod to the security guard and the security guard waves them on, by and large. There is one person, though, that he has not seen before, but who looked somewhat familiar nonetheless. He stops this individual and asks him if he is new. He says he is a contractor that needs to do important work on a workstation located in the emergency room. He shows his badge to the guard which seems authentic enough to the guard. The guard lets him pass. Unfortunately, what the security guard did not know is that the supposed contractor is not an authorized individual at all. Once in the emergency room, the "contractor" makes his way to the workstation and proceeds to log into an account using the information posted on the monitor (i.e., a sticky note with username and password). Nurses and doctors hurry past him, but no one quite seems to notice.

The "contractor" places a malware-laden USB drive (which happens to be a WannaCry ransomworm derivative) into the machine and, seemingly within moments, others in the hospital system are not able to access the EHR system and other mission critical systems. Many staff are perplexed and unsure what to do, especially since film and paper records are either not kept at all or are not necessarily up to date. Meanwhile, many patients are awaiting care, but patient care is, at least in some cases, stalled because the clinicians are fighting with technology—thus, taking valuable time away from the patients. Some patient monitor alarms are missed and response times are significantly delayed. Time is ticking and so is the potential adverse impact on patient safety.

But, these are not all of the complications that have arisen. The heating ventilation and air conditioning (HVAC) system has failed in some areas, likely due to only one power generator running as emergency power backup (or perhaps due to the rapidly spreading malware). Unfortunately, one of the critical areas in which the HVAC system has failed is the operating room in the hospital. Multiple surgeries are happening at the same time. In one instance, a patient starts to become hyperthermic and the surgical team takes proactive measures to cool down the patient's temperature. In another instance, a surgeon starts to profusely sweat and the operating room technician proceeds to wipe the sweat off of the surgeon's forehead so that the sweat does not contaminate the patient's surgical wounds.

Finally, some of the elevators within the hospital suddenly stop operating (in some cases, with patients and staff trapped in them). The hospital recently invested in smart elevators that replace traditional electromechanical systems with computer-enabled mechanisms. The origin of this odd behavior with the elevators is unknown (whether due to the hospital running on limited power or the rapidly spreading malware), but panic has ensued and parts of the hospital are indeed in chaos.

An incident, such as the one described, can result in a cascade of failures. A "domino effect" can occur when there are interdependences on other systems. Given the size and complexity of healthcare organizations, one incident may trigger another. While no one wants to experience the "domino effect", we must be prepared for the worst case scenario – ideally, with a plan that has been written, tested, validated, and regularly updated as situations occur.

Primary and Secondary Attack Surfaces and Examples of Patient Impacts

This paper focuses on both primary and secondary attack surfaces that may result in patient harm and/or risk patient safety. Primary attack surfaces include medical devices, medicine, surgeries, and non-invasive procedures. [4] For example, a medical device may be modified or tampered with to produce a denial of service condition (thus denying treatment) or to deliver a fatal bolus of medication to the patient (e.g., an insulin pump being modified by a remote attacker to administer a fatal dose of insulin).

In another example, the wrong medication may be delivered to the patient, potentially resulting in serious adverse consequences or even death. In yet another example, an anesthesia system with a ventilator may be manipulated to fail during a surgery. These are examples of "smart" equipment that may be tampered with by an attacker.

In terms of a secondary attack surface, these may include such things as electronic health records (EHR), medicine inventory systems, power, and test results. [4] Additional secondary attack surfaces may include HVAC systems (e.g., building HVAC and elevator HVAC systems), fire alarm systems, and physical security controls. By way of example, a patient's medication list or medication allergy list may be intentionally tampered within an EHR system. In another example, a power supply for a building may be tampered with so as to disrupt power in the operating room while surgeries are taking place. [4] In yet another example, elevators may fail to operate or service may be disrupted, if such systems are tampered with. In still another example, a radiology image may be manipulated so that it is flipped, showing the left side of the brain as the right side. A patient needing to have a tumor removed from the left side of the brain may instead be operated on the right side, notwithstanding a robust surgical pause protocol to confirm that the right patient is being operated on at the right site and that the correct procedure is being performed.

How to Proactively Address Patient Safety and Cybersecurity Issues

While many in the healthcare sector are still largely unaware of the nexus between patient safety and cybersecurity, some are very much aware of this connection. The knowledge and skill of being able to hack into a device and cause patient harm is there, according to some. [12] Yet others believe that hacking into a device to cause patient harm is still very difficult. [13] However, there have been many reports of devices being vulnerable to exploitation by threat actors exercising a relatively low level of skill. Unfortunately, this understanding is not common knowledge across the board in the healthcare sector and we need to not only raise awareness, but also take proactive steps to address patient safety within the context of cybersecurity. Indeed, industry analysts have recently reported that hackers exploiting remote access to systems to disrupt healthcare operations is the number one health technology hazard. [14]

Financial Planning and Procurement

Hospitals, whether small, medium, or large entities, are generally concerned about financial planning and procurement. This includes capital expenditures for IT and OT assets. Hundreds of thousands of dollars or even millions of dollars may be spent on infusion pumps, imaging modalities (such as CT and MRI equipment), and other types of equipment involved in patient care. Fortunately, however, the life expectancy of such equipment can be as many as five, seven, ten, or more years. [21]

An MRI machine, which can cost over a million dollars, may be in service for seven or more years. An infusion pump may be in service for five or more years. While infusion pumps are not quite as expensive, many hospitals have hundreds or thousands of them, depending upon size. Upgrading expensive equipment such as these can be a complex endeavor, resulting in a tension between functionality (i.e., "it works") versus cybersecurity (i.e., "it's vulnerable"). Frequently, the projected timeline for upgrading equipment because it is not secure (or no longer supported—i.e., a legacy device) may be quite different from the projected timeline for upgrading equipment because it no longer works (i.e., a failure to satisfy clinical requirements).

Thus, financial planning and procurement strategies of hospitals should ideally be revised in order to address both worlds—safety and security as well as functionality. This can be facilitated with the work of cross-disciplinary teams across clinicians, chief information security officers (CISOs), chief medical informatics officers (CMIOs), chief nursing informatics officers (CNIOs), procurement specialists, and others. The lack of cross-disciplinary financial planning and procurement team strategies (including selection and vetting of medical equipment) could potentially lead to less safe and secure equipment being purchased (e.g., supply chain problems or equipment being purchased from the lowest bidder). [15]

Medical equipment that has not been appropriately selected vetted can potentially result in significant impacts to the patient, especially in regard to life sustaining or life saving devices. Further, old medical equipment that has reached its end of life may prove to be problematic when use is continued in clinical settings. By the same token, when cross-disciplinary teams are looking at procuring certain medical equipment, such teams also need to (ideally) concurrently plan for when such equipment will need to be replaced.

The Convergence of IT and OT Assets and Personnel

Definitions of Operation Technology and Information Technology

Operational Technology (OT) is defined as hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. [2] OT includes building management/automation systems and HVAC systems. Building management/automation systems may include electrical systems that control an entity's HVAC system, lighting, fire safety and security systems, plumbing, and elevators. [16] Information Technology (IT) is defined as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an entity. [2] IT systems may include workstations, servers, network routers and switches, firewalls, and other types of IT assets. Accordingly, OT systems and IT systems are, at least by definition, distinctively different. Yet, some organizations have started to take proactive steps to converge OT and IT to help increase interoperability, refine processes, and develop collaborative ways to support common objectives. [16]

Historical Focus of Operational Technology

Historically, OT has focused on physical security concerns. Traditionally, OT systems have been electromechanical devices that have operated by way of manual or electronic controls. Such OT systems did not have the same types of risks that IT systems have had. Thus, most vulnerabilities have typically

required either physical access or physical proximity to the device in order to exploit the OT device. Typical controls to safeguard OT devices have included security guards, fences, and locks. But, as with many technologies, there have been advancements in the state of the art. More particularly, OT systems have evolved to become computer-enabled systems (i.e., smart/connected systems). This has, in turn, increased the attack surface of the OT device. Accordingly, manufacturers and operators of OT smart devices need to be concerned about cybersecurity risk (similar to concerns faced with traditional IT assets). [16]

Operational Technology and Information Technology as Traditionally Separate Departments

While IT and OT technologies have traditionally developed independent of each other and IT and OT departments within organizations (including in healthcare) have also operated typically separate from each other, the convergence between these two technologies (namely, OT devices becoming more IT-like with connectivity) has necessitated both manufacturers and the consumers of these devices to work together in a more collaboratively to ensure not just functionality, but also safety and security. This is easier said than done, as IT and OT have typically had separate paths, both from the manufacturer perspective and the consumer perspective. Within healthcare and other industries, the facilities department is typically in charge of physical assets and security. The IT department is typically in charge of IT assets and security (notwithstanding a specialized department for IT security). But, both IT and OT have the common objective of ultimately ensuring that these technologies are safe and secure.

OT and IT Teams Working Together on Smart/Connected OT Devices

It is important for personnel in the OT and IT fields to work together to blend their respective skills, trades, and strategies. This is especially relevant since OT technologies have started to converge with IT technologies. In other words, many OT technologies are becoming more IT-like as they are now connected devices or smart devices.

Additionally, as we are keenly aware, various malware variants have been used to specifically target emergency systems within the healthcare sector and across other critical infrastructure sectors. These emergency systems have been designed to protect both facilities and the people within them. [17] For example, the tampering of fire safety and security systems could essentially take away a significant line of defense. This, in turn, increases the risk to both people and facilities. In the face of these challenges, OT and IT teams must collaborate in order to ensure that safety and security is achieved.

Breaking Down Silos Between OT and IT Teams

Without a doubt, OT and IT teams will have barriers to break. Such barriers may include jargon, planning approaches, operating hours, interpersonal communications, and techniques. However, these barriers can be mitigated by sharing experiences, lessons learned, risks and hazards, challenges, and possible solutions. Above all, communication is key. Nonetheless, day-to-day work is challenging enough, but when significant incidents happen, the work can become much more complex.

Ensuring Reliable Emergency and Standby Power Systems

Ideally, hospitals will provide a high quality source of electrical power that is backed up with highly reliable emergency and standby power systems so that there is an uninterrupted flow of electricity to the entire facility, especially during crisis and natural disasters. However, power disruptions and

failures are fairly common occurrences. These may be caused by utility outages, equipment failures, testing, and maintenance. However, natural and man-made disasters may sometimes force a facility to rely solely on emergency and standby power systems for extended periods of time. [18]

The National Fire Protection Association (NFPA) code sets forth criteria for hospital emergency power requirements, including essential electrical systems (namely, backup power systems that are used in emergency and standby power situations). More specifically, EES includes a life safety branch which provides power to functions or warning systems that are required so that occupants of the building can safely leave in the event of an emergency (e.g., fire alarms, illuminated exit signs, etc.), a critical branch which is intended to serve a limited amount of loads that have an immediate impact on the well-being of patients or are essential to the clinical functionality of the healthcare facility (e.g., anesthesia system with a ventilator, life support equipment, etc.), and an equipment branch to serve mechanical loads that are required to support clinical activities (e.g., HVAC systems, elevators, etc.). [18]

Impacts of Power Failure or Disruption of Building Automation Systems

An example is the failure of a HVAC system in the event of a power failure or disruption. In accordance with NFPA code, EES systems will be operational to support HVAC systems. HVAC systems are not just simply for comfort of the patient, but HVAC systems are essential to patient safety as well. For example, as illustrated in the previous hypothetical scenario section, a variation in temperature due to a failure of an HVAC system (i.e., the building HVAC system) can potentially put a patient's life at risk while in the operating room.

In another example, an elevator machine room HVAC system (which is separate from the building HVAC system) may fail, thereby causing the elevators in a hospital to experience disruption or failure. [19] This can lead to individuals being trapped in an elevator or elevator doors failing to close. However, with the advent of smart elevators, these machines can, at certain times, alert facilities management teams when there is a need for elevator maintenance prior to a disruption or failure. This could potentially result in significantly less downtime for elevator systems which can be essential for patients, especially when time is critical. [20]

Role of Cybersecurity Education and Awareness in Clinical Settings

Cybersecurity, when properly engineered and implemented, should be an enabler of a hospital's mission (i.e., patient care) and its business operations. Confidentiality of patient data for hospitals is important. However, integrity and availability of patient data are essential elements, as we have seen with various well-publicized ransomware and distributed denial of service attacks. [22]

From a proactive perspective, cybersecurity professionals that are new to the hospital environment must quickly get up to speed in terms of how to balance appropriate cybersecurity measures with the need for authorized users to access patient data. To this end, education, awareness, and information sharing is key. For example, we know that HVAC systems have been used as a pivot point to gain access to corporate networks based upon well-publicized reports. [23] However, we also know that HVAC systems play critical roles in patient transport (e.g., elevators), operating rooms, and elsewhere within the hospital setting. Accordingly, the cybersecurity professional must learn how to manage

cybersecurity risk within the context of a clinical setting for the sake of patient safety. Above all, cybersecurity measures should not adversely impact the timeliness and quality of care to the patient.

By engaging in a meaningful dialogue and information exchange with Chief Medical Informatics Officers (CMIOs), Chief Nursing Informatics Officers (CNIOs), and others, cybersecurity professionals will gain a better understanding about how IT-related decisions may potentially impact patient care (e.g., taking a portion of the network offline, shutting off a device, closing a port, etc.). Informatics officers such as CMIOs and CNIOs bridge the gap between the clinical world and the IT world. But, by the same token, CMIOs, CNIOs, and others may also benefit from learning about cybersecurity from the cybersecurity professionals to better understand how cybersecurity affects their lines of business.

Reaching Across Externally

Mutual aid agreements and assistance agreements

Mutual aid agreements and assistance agreements are agreements between and among agencies, organizations, and jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective of such agreements is to facilitate rapid, short-term deployment of emergency support prior to, during, and after an incident. [24] For example, mutual aid agreements may be developed to assist with responding to incidents, diverting patients to a facility that is operational as needed in case the hospital has been adversely affected by a natural or manmade event, and/or providing loaner devices and equipment.

Information sharing

Whether done with peers or as part of a formal group or initiative, information sharing with others is key to understanding what has happened, what is happening, and what may happen in the future. Information sharing helps to break down the silos. Peer-to-peer information sharing is quite common and often is done within one's local or regional geographic area. However, other groups exist to help broaden the scope of information sharing. An example of this is the Cyber Health Working Group (CHWG), which is currently managed and operated by the National Cyber-Forensics & Training Alliance (NCFTA) and the Executive Partnership for Integrated Collaboration (EPIC). [25]

In addition to sharing information with peers, we also need to keep in mind the need to share information within the walls of our own organizations. Frequently, the discovery and/or reporting of incidents may be significantly delayed due to lack of policies, processes, and/or a supportive culture to encourage such disclosures. Organizations must work from within to ensure that silos do not exist and that information shows appropriately in lateral, bottom up, and top down fashions. Otherwise, such communication failures may adversely impact hospitals and potentially their patients in the end.

Empowering Patients and Clinicians

There is typically a significant gap between the knowledge base of a cybersecurity professional versus that of a patient or a clinician. When a cybersecurity professional at a hospital notifies a clinician of a potentially significant problem with a medical device (e.g., a significant vulnerability that may result in a denial of service condition or a vulnerability that allows a remote attacker to execute commands of his or her choosing), there is the risk that the cybersecurity professional may not communicate the problem

with the device in terms that the clinician may understand well. This problem is not tied to the educational level, intelligence, or savvy of the clinician. Instead, the problem resides with using too much jargon and not breaking down the situation into terms that a layman (i.e., a non-cybersecurity professional) can understand.

As a result, even if a clinician is informed about a significant cybersecurity problem affecting a medical device, the clinician may not fully understand the problem and its potential consequences. Accordingly, the clinician may decide that the risk is too great to the patient and may perceive the cybersecurity problem to be a relatively small one—or at least one with a relatively low probability of occurring. This assumes, though, that patient harm will never (and perhaps has never) come about as a result of an attacker infiltrating a device. Thus, this assessment may need to be revisited in the future—especially if attackers proactively seek out to do harm to patients. [4]

Ideally, too, patients should be informed about what medical device is being implanted or used in (or in association with) their bodies. If there is a cybersecurity concern that may have an impact on the patient's well-being, patients should be informed about what the concern is and what, if any, can be done about it. In some cases, too, the patient may be responsible for the maintenance and integrity of their own device, depending upon the circumstance. (For example, some manufacturers deal directly with the patients as their customers, whereas others deal directly with hospitals as their customers.)

Conclusion and Recommendations

The healthcare sector must realize that patient safety is directly tied to cybersecurity in today's modern world. Innovation has led the way to many advancements that help save and sustain patient lives. The healthcare sector must keep up with the changing tide. Patient safety and cybersecurity—together—should be top priorities of hospitals and other healthcare organizations and such priorities need to be supported by leadership on the clinical side and on the administrative side. We can no longer afford to be anachronistic.

While hospitals and other healthcare organizations are advancing in terms of patient care, it is not without bumps on the road. It is largely unknown about the impact on patient safety as it relates to cybersecurity, but this does not mean that this issue should be ignored. On the contrary, doing so will needlessly put patient lives at risk. The healthcare sector needs to take steps to ensure that cybersecurity programs are aligned with robust and responsible patient care. For some, this is a new way of thinking. But, the health of individuals hangs in the balance and we need to be responsible stewards.

There are many ways in which patients may be impacted by cybersecurity events which may happen. Equilibrium must be achieved between the quest for robust patient safety and sound cybersecurity practices. With our digital world in healthcare, attack surfaces are ever present and expand daily. Never before have there been more opportunities and avenues to attack hospitals and their patients.

Hospitals are incredibly complex organizations. These institutions cannot afford anymore to operate in silos. Patient safety professionals need to work hand in hand with cybersecurity professionals, clinicians, administrators, and others. But, in addition to the day-to-day tasks and challenges that may come about, we also need to look ahead to the future and understand and proactively plan for what we

predict may happen. Otherwise, we will be woefully unprepared for what may come to be and our response would be haphazard at best. Proactive measures such as information sharing, mutual aid and assistance agreements, public-private partnerships, cross-disciplinary teams, and education and awareness will help us have a clearer understanding of the nexus between patient safety and cybersecurity and how to tackle the challenge.

Appendix A: Citations and Additional Resources

Citations

1. *See* World Health Organization Regional Office for Europe, Patient Safety, *available at* http://www.euro.who.int/en/health-topics/Health-systems/patient-safety/patient-safety.
2. *See* NIST, Computer Security Resource Center Glossary, *available at* https://csrc.nist.gov/glossary.
3. *See* EI-ISAC, Cybersecurity Spotlight – CIA Triad, *available at* https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/.
4. *See* ISE, Hacking Hospitals, *available at* https://www.securityevaluators.com/hospitalhack/.
5. *See* Forbes, Cyber Attack Nets 4.5 Million Records From Large Hospital System, *available at* https://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system.
6. *See* HIMSS, 2018 HIMSS U.S. Leadership and Workforce Survey, *available at* https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_US_LEADERSHIP_WORKFORCE_SURVEY_Final_Report.pdf.
7. *See* Accenture and AMA, Taking the Physician's Pulse, *available at* https://www.ama-assn.org/media/21666/download.
8. *See* HIMSS, 2019 HIMSS Cybersecurity Survey, *available at* https://www.himss.org/sites/himssorg/files/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf.
9. *See* National Audit Office, Investigation: WannaCry cyber attack and the NHS, *available at* https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.
10. *See* Pittsburgh Post-Gazette, Heritage Valley Health, drugmaker Merck hit by global ransomware cyberattack, *available at* https://www.post-gazette.com/business/tech-news/2017/06/27/Heritage-Valley-Health-Merck-targets-cyberattack-pennsylvania-ransomware/stories/201706270148.
11. *See* Healthcare IT News, How knowing the difference between Petya and NotPetya can help security pros block malware, *available at* https://www.healthcareitnews.com/news/how-knowing-difference-between-petya-and-notpetya-can-help-security-pros-block-malware.
12. *See* CSO, Hacking pacemakers, insulin pumps and patients' vital signs in real time, *available at* https://www.csoonline.com/article/3296633/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html. *See also* FDA, Cybersecurity, *available at* https://www.fda.gov/medical-devices/digital-health/cybersecurity.
13. *See* Asian Scientist, Murder by Medical Device?, *available at* https://www.asianscientist.com/2019/02/print/murder-by-medical-device/.
14. *See* ECRI Institute, 2019 Top 10 Health Technology Hazards Executive Brief, *available at* https://www.ecri.org/Resources/Whitepapers_and_reports/Haz_19.pdf.
15. *See* WBUR, Defending Hospitals Against Life-Threatening Cyberattacks, *available at* https://www.wbur.org/commonhealth/2018/04/26/hospital-cybersecurity.
16. *See* NexDefense, IT/OT Convergence: Bridging the Divide, *available at* https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.
17. *See* ZDNet, Triton hackers return with new, covert industrial attack, *available at* https://www.zdnet.com/article/triton-hackers-return-with-new-industrial-attack/.

18. *See* Consulting – Specifying Engineer, Emergency and standby power in hospitals, *available at* https://www.csemag.com/articles/emergency-and-standby-power-in-hospitals/.
19. *See* Consulting – Specifying Engineer, HVAC and Fire Safety for Elevator Systems, *available at* https://www.csemag.com/articles/hvac-and-fire-safety-for-elevator-systems/.
20. *See* Memoori, Cloud Connected Smart Elevators Enable Preemptive Maintenance Services, *available at* https://memoori.com/cloud-connected-smart-elevators-enable-preemptive-maintenance-services/.
21. *See* BEAG, Biomedical Engineering Advisory Group Guidance Paper: Life span of Biomedical Devices, *available at* http://cedglobal.org/download/Life%20Span%20of%20Biomedical%20Devices%20-%20Guidance%20Paper%20Final.pdf.
22. *See* Panda Security, Ransomware is Not the Only Ransom Attack, *available at* https://www.pandasecurity.com/mediacenter/security/ransomware-not-alone/.
23. *See* Trib Live, Sharpsburg vendor confirms link to Target data probe, *available at* https://archive.triblive.com/business/local-stories/sharpsburg-vendor-confirms-link-to-target-data-probe/. *See also* Trend Micro, New BlackPOS Malware Emerges in the Wild, Targets Retail Accounts, *available at* https://blog.trendmicro.com/trendlabs-security-intelligence/new-blackpos-malware-emerges-in-the-wild-targets-retail-accounts/.
24. *See* FEMA Emergency Management Institute, What Are Mutual Aid Agreements and Assistance Agreements?, *available at* https://emilms.fema.gov/IS703A/RES0102130text.htm.
25. *See* Executive Partnership for Integrated Collaboration, Healthcare Intelligence, *available at* https://www.intelligence.healthcare/.

Additional Resources

1. *See* Healthcare & Public Health Sector Coordination Councils Public Private Partnership, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, *available at* https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.
2. *See* AHRQ, Reporting Patient Safety Events, *available at* https://psnet.ahrq.gov/primers/primer/13/reporting-patient-safety-events%20on%20April%2016.
3. *See* AHRQ, Federally-Listed PSOs, *available at* https://www.pso.ahrq.gov/listed.
4. *See* Health Care Industry Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry, *available at* https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
5. *See* Imperial College London Institute of Global Health Innovation, Improving Cyber Security in the NHS, *available at* https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-Security-Ghafur.pdf.
6. *See* Archimedes Center for Medical Device Security, Publications and Research, *available at* https://www.secure-medicine.org/.