THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 14 NUMBER 6

MARCH 2015
HEALTH CARE SECTOR

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

This month, our authors discuss aspects of security and resilience within the **Health Care Sector**. After the recent information breach experienced by one of the nation's major health care organizations, this topic takes on an added relevance.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, Dr. Elivra Beracochea, President and Founder of Realizing Global Health, will discuss the need for health care critical infrastructure protection within the new 2030 development agenda being set by the United Nations General Assembly. Authors Justin Snair and Matt Deleon then provide an overview of cyber threats against the health care critical infrastructure and related vulnerabilities. Next, Amanda Joyce, Michael Thompson, Andrea LeStarge, and Dr. Nathaniel Evans of Argonne National Laboratory highlight one such vulnerability and present an article on improving cybersecurity response efforts to prevent medical identity theft.

Parham Eftekhari and Ryan Kalember, both fellows with the Institute for Critical Infrastructure Technology, describe the concept of "Defense in Depth" as it applies to health care organizations and their data. In the final article, Amanda Joyce, Michael Thompson, and Dr. Nathaniel Evans discuss mobile medical device usage in the operating room.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight. We hope you find this issue of The CIP Report useful and informative. We are thankful for your support and the rich dialogue that follows each topic.

Best Regards,

Director
Center for Infrastructure Protection and Homeland Security (CIP/HS)

Critical Infrastructure Protection in Global Health in the 2030 Agenda: What Has Happened Since 2013

by Dr. Elvira Beracochea*

In 2013, I wrote an article about the importance of protecting the health infrastructure in developing countries and proposed a roadmap to globally manage health infrastructure and address the impending risks. Sadly, not much has happened since 2013. Then, a visit to Northern Nigeria had raised my awareness of the lack of infrastructure standards and of maintenance of standard operating procedures (SOPs). At that time, the local governments did not know what needed to be done to maintain and even upgrade their facilities. Lack of mosquito screens on windows and nets on beds, lack of cleaning routines or ways to dispose of broken down equipment, all worsened by lack of functioning restrooms and electricity were the most visible signs of deficient infrastructure in a district health center that served several thousand people (photo 1).

The Labor room also did not meet infrastructure standards. In the photo you can see how in spite of having a sink, they had to use a bucket to wash hands. Also, the walls and floor had not been cleaned in a long time and the bed lacked linen and was not up to standards either (photo 2).

The intent of these photos is not to criticize. In fact, the staff were doing the best they could with what they knew. The problem was what they did not know about their infrastructure, about maintenance and SOPs that would have allowed them to deliver quality healthcare. We all get used to our surroundings and stop "seeing" the problems.

The recent Ebola epidemic brought to world attention the fragility of health systems and the inappropriateness of the health infrastructure in West Africa. On the other side of the Atlantic, we also saw how Ebola cases were rapidly detected, treated, and contained by trained staff in appropriate facilities. The main and most striking difference between the two scenarios on both sides of the Atlantic was

(Continued on Page 3)

(Continued from Page 2)

the infrastructure of both health systems.

Now it is 2015, a new development agenda is being developed for 2030 to be approved by the UN General Assembly in September. Among many other priorities, this agenda calls for ending preventable child and maternal deaths as well as effective treatment of malaria, HIV/AIDS, and TB. However, the agenda does not include the urgent need to upgrade the health facilities up to standard, at least 10% per year for the next 10 years. Without this, health systems in most developing countries are going to be inoperable by 2030.

What Is a Health System?

The health system of any country includes a number of healthcare delivery and healthcare management structures that are essential for its optimal performance, that is, protect the health of the people of that nation. In the US, the latter is represented by the Department of Health and Human Services (DHHS) and its federal and state agencies implementing policies such as the Affordable Care Act and many others, setting and ensuring quality standards, and implementing programs to address various health priorities. The former is the network of health facilities run by mostly the private sector providers such as HMOs and others, and a minority of health facilities run by the local health departments and by non-profit organizations. The private sector does a pretty good job keeping their facilities up to standards because they want to protect their investment.

In West Africa, the national and state Ministries of Health (MOH) is responsible for managing the health status of the country. Like DHHS, the National MOH is responsible for creating and implementing policies and the state MOH are responsible for implementing the national policies as well as local ones through various programs that address maternal and child health, disease prevention, etc. In contrast with the US, these MOH and their district offices are also in charge of managing a widespread network of public facilities that deliver healthcare to most of the population. Some facilities were built during colonial times and have been adapted to deliver healthcare, others were built recently but due to the weather and lack of maintenance they are in need of repair. The health center in the photo seemed to have been built 30 years ago but in fact, it had been built only five years earlier. In all, health staff are unaware of their responsibility of protecting the infrastructure and how to do it.

In addition to the lack of maintenance plans and infrastructure standards, my visit to Northern Nigeria showed that the floor plan in many facilities does not meet the needs of a busy health center. The patient areas and staff areas are not defined and separate from the public waiting areas and there is no infection control program in effect. Restrooms are out of order and patients, including mothers that had just delivered their babies, have to use the woods nearby. You may think that this is because it is a poor region, but no, that was not the reason. The main reason was that the authorities did not know what infrastructure standards have to be met to safely and effectively deliver quality healthcare. I asked if the health team could work with the local health committee to mobilize resources, fix the restrooms, and do other repairs, and they said they had not thought about it. They did not think that was a priority, but said it was possible to include that in the following year's budget.

This visit to this health center in Northern Nigeria taught me three lessons that the Ebola epidemic emphasized:

1. There is a need for an outsider to visit health facilities and point out those infrastructure deficits that have become invisible to those that work there every day. Standards need to be progressively met by every facility mobilizing all resources available in order to be able to deliver quality services as well as be ready to respond to epidemics just as well in West Africa as in the US. It will not happen overnight, but can be done in 10 years.

2. The Health Center is the center of the healthcare delivery of most programs. The infrastructure of these health centers must meet standards. Health centers like the one in the photo are where women get prenatal care, children are born, are immunized, treated for diarrhea, malaria or pneumonia and malnutrition, where all the adult population go for HIV/AIDS testing and counseling, and treatment of all other health problems. From the health center, community-based

(Continued on Page 4)

(Continued from Page 3)

programs and community health workers and volunteers are sent out to reach those who do not come to the health center and deliver basic preventive care and lifesaving misoprostol to prevent post-partum hemorrhage and chlorhexidine to prevent newborn infections and deaths.

3. We must not accept that things cannot change. There is always a way if you are committed and help people realize there is a problem. I believe the world can help upgrade the health infrastructure in West Africa. The 2030 development agenda must include not only targets for what must be done, such as reducing maternal mortality, but also how these targets must be achieved. We must have facilities that meet infrastructure standards to prevent maternal death. If we are really committed to ending these preventable deaths, facilities must be ready to provide emergency obstetric and newborn care, among other lifesaving services. No excuses.

Recommendations

1. We must urge international development agencies and organizations to help the countries where they work to take a health infrastructure inventory and raise their awareness about the need to upgrade and improve their infrastructure. Information is power, the power to act. Below is a sample of what such an inventory may look like. At the minimum, every country should identify each and every facility and its condition, what immediate repairs are needed, and who will be responsible for working with the local authorities to help make these repairs happen.

2. USAID currently spends over $1 billion on infrastructure. The Department of Defense (DoD) has built hospitals in West Africa to respond to the Ebola epidemic. We must ask USAID and DoD to prioritize water and electricity to health facilities and assist countries to work with all donors to progressively cover all facilities in West Africa. The handover of the new infrastructure must be part of the country's overall CIP plan.

3. There is need of a Global Health Infrastructure Collaboration, Coordination, and Communication agreement among the hundreds of organizations, particularly the World Bank's global infrastructure facility, that work in West Africa to work with the West African governments to develop a plan to upgrade and or replace at least 10% of their health centers and hospitals per year in the next 10 years. The world's current infrastructure is insufficient and with population growth projections and another billion people in the planet in 10 years, it will be completely overwhelmed.

The roadmap I proposed in 2013 is still ahead and more valid and urgent than ever. It is the role of WHO and UN family, and a donor responsibility of every organization working in global health to point out where lack of infrastructure standards are not met and mobilize support to correct them. Do not tolerate lack of infrastructure standards any longer.

** Dr. Elvira Beracochea is the founder and president of "Realizing Global Health" formerly called MIDEGO, an international global health consulting company that assists donors, governments and global health organizations to develop self-reliant sustainable health systems that deliver quality healthcare to everyone everywhere every day. Dr. Beracochea has developed the "Health for All NOW" healthcare delivery model, and numerous solutions that improve the delivery of quality health services worldwide. She received her MD from the University of the Republic of Uruguay and her MPH from Hadassah Hebrew University in Israel.* ❖

Country	State or Province	Facility Name and #	Condition	Photo #	Impact on Quality	Impact on Safety	Impact on Staff	Decision: Fix or Replace	Cost	Responsible Organization

Cyber Threats Toward Critical Infrastructure on the Rise: Healthcare and Public Health Sector Increasingly Vulnerable

by Justin Snair* & Matt Deleon**

Threat of CyberAttack: A National Issue

In February 2015, Anthem, the nation's second largest health insurer, reported a sophisticated cyber-attack which exposed protected health information (PHI) and health plan membership information on 80 million individuals. Similarly, in August of 2014, Community Health Systems, one of the nation's largest hospital groups, was the victim of a cyber-attack from China, resulting in the theft of Social Security numbers and other PHI belonging to 4.5 million patients. In May 2014, the Montana Department of Public Health and Human Services[1] announced that a cyber-attack was detected on the health department's server, allowing a hacker to illegally access the PHI of 1.3 million individuals. These three attacks affected more people than the population of California, Texas, and New York combined.

These incidents are some of the largest cyber-attacks on the healthcare and public health (HPH) sector to date, costing more than $100 million in damage, and incurring even more loss in eroded trust. These examples, as well as other large attacks in the financial services and retail sectors, raise questions over how our nation should respond to the ongoing threat of cyber-attack. To answer these questions, it is necessary to understand the risk and evolving nature of cyber-attacks.

James Clapper, Director of National Intelligence

On February 26, 2015 James Clapper, Director of National Intelligence, delivered the 2015 Worldwide Threat Assessment of the U.S. Intelligence Community to the Senate Armed Services Committee, which can help illuminate the current status of this threat. In this annual statement, the Intelligence Communities' collective reflections and insights on global threats faced by the U.S. are shared. For the third year, cyber threats, which encompass cyber-attacks and cyber espionage, to U.S. national and economic security were presented first, before even terrorism, and viewed as one of the greatest threats to the security of the nation's critical infrastructure sectors.

These sectors—which include chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems—are so "vital to the nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[2] These sectors are diverse and complex assets, systems, and networks, both physical and virtual, and provide the means by which essential services are delivered to the American people. The sectors also provide the avenues that enable people, goods, capital, and information to move across the country, and the engine that underpins the nation's defense, manufacturing of goods,

(Continued on Page 6)

[1] Jeffrey Roman, "Montana Breach Victim Tally: 1.3 Million," *Data Breach Today* (June 25, 2014), available at http://www.databreachtoday.com/montana-breach-victim-tally-13-million-a-6992.

"What Is Critical Infrastructure?," *U.S. Department of Homeland Security Website*, Accessed February 24, 2015, http://www.dhs.gov/what-critical-infrastructure.

(Continued from Page 5)

production of energy, and our overall system of commerce. While a large, coordinated cyber-attack that incapacitates the entire national infrastructure is considered unlikely, the Intelligence Community envisions an on-going series of attacks by state and non-state actors against private-sector targets, imposing costs on the nation's economy and national security.

Our critical infrastructure is "increasingly connected '[via networked computer systems] and interdependent and enhancing its resilience is an economic and national security imperative."[3] Even with improving network defenses, the Intelligence Community finds that the cyber threat cannot be eliminated, only managed. Despite this ongoing risk, it is feared that many in the private sector fail to adequately account for cyber threats or the systemic interdependencies between different critical infrastructure sectors. The public discussion of cyber threats has focused largely on confidentiality and availability. The Intelligence Community anticipates that future cyber-attacks may look to manipulate electronic information, rather than to delete or steal it, in order to compromise reliability and impair decision-making by sector officials.

Moreover, Critical Infrastructure Control Systems, such as the programmable logic controllers (PLC) used for automatically regulating power and utility distribution, controlling heating and ventilation systems, managing traffic control systems, treating and disposing of wastewater, and activating emergency power generators, are vulnerable. The interruption of these systems by a cyber-attack could have catastrophic consequences for critical infrastructure sectors and communities throughout the nation.

Healthcare and Public Health Sector Faces Unique Risk and Consequences

While all sectors are vulnerable to cyber-attack, the threat and risk to the HPH sector is particularly concerning. The HPH sector serves or operates in every community throughout the nation, and protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. The sector includes public and private hospitals providing clinical care, medical education, and research services; emergency departments and outpatient facilities; blood banks; and public health laboratories. The HPH sector is a multi-trillion dollar industry employing over 13 million personnel, including approximately five million first-responders, three million registered nurses, and more than 800,000 physicians.[4] The sector has interdependent connections to other critical infrastructure sectors, such as supply chain, financial services, and energy, and operates at nearly 100 percent capacity on a daily basis."[5] The structure of the sector also introduces complications and risk. The HPH sector is an incredibly distributed network, jointly comprised of thousands of entities separately operating under private and public ownership throughout

(Continued on Page 7)

[3] Caitlin A. Durkovich, *Office of Infrastructure Protection Strategic Plan: 2012-2016* (Washington, DC: U.S. Department of Homeland Security, 2012): 1, available at https://www.dhs.gov/sites/default/files/publications/IP%20Strategic%20Plan%20FINAL.pdf.

[4] Nitin Natarajan, Todd Keil, Al Cook, David Morgan, and Erin Mullen, *Healthcare and Public Health Sector-Specific Plan* (Washington, DC: U.S. Department of Health and Human Services, 2010), available at http://www.phe.gov/Preparedness/planning/cip/Documents/2010-cip-ssp.pdf.

[5] David G. Henry and Justin Snair, "Risks of Cyber Attack on the Healthcare Sector Leave Public Health of Communities Vulnerable," *The CIP Report 12, no. 2* (Aug. 2013): 2-5. Available at http://cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_August2013_Health.pdf

(Continued from Page 6)

Centers for Disease Control and Prevention, Georgia

the nation, without a centralized control at the core. The distributed nature of the HPH sector likely prevents cascading failures from occurring across the entire sector from a cyber-attack, but does present other vulnerabilities.

Coordination and sharing of threat information becomes increasingly more difficult across a scattered network of separate entities. To share information, enhance efficiency, and improve patient flow and quality of care, the HPH sector has turned to networked computer technology. The reliance on this technology, however necessary, leaves the HPH sector vulnerable. As demonstrated by the recent cyber-attacks against HPH sector entities, private information and patient records are often the targets for cyber-attacks, as they both have incredible value on black markets. Stolen names, birth dates, policy numbers, diagnosis codes, and billing information are used to create fake IDs to buy medical equipment or drugs that can be resold. Or, they combine a patient number with a false provider number and file fabricated claims with insurers. Medical identity theft is not always caught quickly, giving criminals time to milk the value of stolen records. This stolen information is often valued at about 10 or 20 times more than stolen credit card information,[6] making the HPH sector a major target for cyber-attack. The HPH sector could see a loss in confidence from patients due to a perceived failure of health IT systems to protect their information and liability, and financial damages in the wake of information breaches.

Theft of private information and patient records is not the only consequence of cyber-attacks that should be concerning to the HPH sector. Public health operations can also be significantly impaired by an attack. The Centers for Disease Control and Prevention (CDC) have identified ten essential services that public health performs and all are susceptible to cyber-attack. For example, an essential service of public health is to diagnose and investigate health problems, which include epidemiological investigations of disease outbreaks and patterns of infectious and environmental hazards. Networked computer systems are often used to assist public health and medical officials in tracking potential outbreaks. A cyber-attack directed at these systems could prevent essential information from being shared during an outbreak or emergency, costing lives and degrading trust in governmental public health.

A cyber-attack could also impact health research performed by academic health institutions as well as research and development within the biotech sector. Academic hospitals could find research data altered or stolen rendering it unusable or questionable, severely hindering or reversing progress on research projects. Certain research centers work with data that could be used to make weaponized infectious agents if stolen and used by a malicious actor. Moreover, health research institutions are vulnerable to power outages caused by cyber-attacks, as infectious agents, cadavers, and a host of research animals are often housed in their laboratories and require a sensitive environment to remain intact and usable.

The intelligence report stated the motivation behind these types of attacks from state actors can often be to undermine the competitiveness of the United States and could be aimed at damaging the integrity of important drug development research and medical

(Continued on Page 8)

[6] Caroline Humer and Jim Finkle, "Your Medical Record Is Worth More to Hackers Than Your Credit Card," *Reuters* (Sep. 24, 2014), available at http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

(Continued from Page 7)

trial data. Just being a victim of a cyber-attack is enough for principal investigators, researchers, and executives to question the integrity of electronically stored research data. Similar to lost data and ruined research following natural disasters like hurricane Sandy or Katrina, this could potentially result in years of research lost or delayed and hundreds of thousands of dollars of cost to an affected research institution.

While cyber-attacks undermining the confidentiality, availability, accuracy and reliability of digital information is certainly a significant issue, the networked computer systems in use by critical infrastructure sectors do more than just store sensitive information and conduct essential healthcare and public health services. Like all sectors, the HPH sector relies on PLC, which as discussed previously, is used to regulate key infrastructure systems such as heating and ventilation, laboratory and blood bank temperature controls, security systems, and backup power generators. The interruption of the services these PLCs control could have catastrophic consequences for patient care, laboratory analysis, and ongoing operation of the affected institutions.

Given the HPH sector's reliance on this technology, strict regulatory requirements and penalties for breaches, and a demonstrated and growing risk of costly cyber-attacks should be enough to motivate sector members and the government to adequately prepare to prevent and withstand these attacks. However, the HPH sector is still severely underprepared and vulnerable. Cyber threat information sharing practices across the HPH sector are also less than optimal. As with many critical infrastructure sectors, information sharing is often provided by Information Sharing and Analysis Centers (ISAC). The HPH sector is served by the National Health ISAC (NH-ISAC), which provides threat information to those healthcare and public health entities that pay for membership. In an era of budgetary restraints, healthcare and public health entities frequently prioritize more traditional programs and operational considerations over network security[7] and may choose not to pay the NH-ISAC for access to this information, thus cutting themselves off from information critical to protecting their computer networks and technology. The utility of the NH-ISAC as a provider of timely and credible information sharing to governmental public health entities in the nation is questionable, as very few public health entities pay for the service. The Association of State and Territorial Health Officials (ASTHO) and the National Association of County and City Health Officials (NACCHO), the national representatives of our nation's state and local governmental public health are not members of the NH-ISAC either. This all entreats concerns over just how public health entities are learning and sharing information about cyber-attacks across the sector and the utility of the NH-ISAC in provide this service to public health departments.

What can be done to mitigate cyber risk to the HPH Sector?

Information sharing within and across sectors and the government is critical to battle cyber-attacks. Amid ongoing concern and the growing cost of attacks, in February 2015 President Obama signed an executive order urging government and the private sector to jointly step up the nation's defenses against cyber security threats. In a large part, this means backing the federal government's Cyber Security Framework (CSF), which was developed by the National Institute of Standards and Technology and released last year. It focuses on cyber risk management and is cited as having the potential to help transform cyber security on a global level.[8] The executive order also, among other things, pushes for the development of "Information Sharing and Analysis Organizations," that will serve as the central point for collaboration between private and federal entities, streamlining the access private companies have to classified cyber-threat information, and ensuring that information sharing

(Continued on Page 9)

[7] National Cybersecurity and Communications Integration Center (NCCIC), *Attack Surface: Healthcare and Public Health Sector* [Bulletin 201205040900] (Washington, DC: U.S. Department of Homeland Security, 2012), available at http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.

[8] Reena Flores and Arden Farhi, "Obama Recruits Tech Giants for New Cybersecurity Efforts," *CBS News* (Feb. 12, 2015), available at http://www.cbsnews.com/news/obama-recruits-tech-giants-apple-intel-reveals-new-cybersecurity-information-sharing-proposals/.

(Continued from Page 8)

will include strong protections for privacy and civil liberties. The White House also announced the creation of the Cyber Threat Intelligence Integration Center, which will combine cyber threat intelligence from multiple departments. Some large private corporations, such as Intel, have supported this effort. However, other large private sector entities, such as Facebook, are not in full support and instead launched their own threat information sharing clearinghouse—ThreatExchange—in February to help private companies collectively battle cyber threats.

These additions to the government and the private sector cyber security arsenal are vital and timely. But what can the HPH sector do to reduce their own vulnerability to cyber-attacks? As with most sectors, cyber security in the HPH sector begins at an individual and organizational level. HPH sector organizations should employ standardized security frameworks, such as the CSF, and procedures regarding requirements for managing the safety, effectiveness, and security of IT systems, including rules for password protection, data management, and employee training to promote good digital hygiene. At a minimum, any cyber security plan should include identification, authentication and access procedures, a fully enforced patch management system, and an annual cyber-risk assessment.

Similarly, leadership within HPH sector entities should have conversations with their chief information officers and IT staff to ensure that a cybersecurity policy is in place, and that the organizations emergency operations plan considers the effects of a cyber-attack. HPH entities, particularly those storing PHI, should consider cyber-attack liability insurance, to help defray the cost of damages should an attack occur.

In addition to efforts at the organization level, support from the national level must be provided. Key federal agencies must compel a nationally coordinated effort to improve the security of the HPH sector. Both the Department of Homeland Security (DHS), the agency charged with promoting and working towards the unified security and resilience of the nation's critical infrastructure, and the HPH Sector Critical Infrastructure Protection (CIP) Program in the HHS Office of the Assistant Secretary for Preparedness and Response, need to dedicate funding to improve the cyber security of the HPH sector. Funding should be directed towards national organizations representing HPH sector entities to conduct national assessments of healthcare and public health entities' awareness of cyber threats, as well as their cyber security activities. This would provide situational awareness on how the HPH sector is approaching cyber threats and help develop a nationwide agenda for improving upon vulnerabilities in the sector. After this nationwide assessment is conducted, tools and resources that help HPH sector entities to create cyber security policies and procedures, information governance and risk management life cycle tools, as well as guidance on conducting risk assessments should be developed. Threat information sharing practices and capacity with the HPH sector should also be assessed, with particular attention given to the utility of NH-ISAC and the dissemination of information to public health entities throughout the nation.

Cyber-attacks will increase and be directed towards targets that are poorly prepared and have something worth stealing, disrupting, or destroying. The HPH sector is critical to the continued welfare of our nation and national economy, possesses sensitive information and systems, and, as demonstrated by recent breaches, is vulnerable to cyber-attack. Continued attacks undermine the sector and will have both costly and life threatening consequences. More concrete and articulated steps, such as some of those mentioned previously, must be taken to improve the security of the sector.

**Justin Snair, MPA. is the Manager of Special Projects for the Association of Academic Health Centers. Justin is also a co-founder of HATCH, Inc., a startup nonprofit which seeks to improve how government, nonprofits, social institutions, industries, and communities share ideas and engage one another to jointly solve challenges our society faces. Justin holds a Master of Public Administration from Northeastern University and a Bachelor of Science in Health Science from Worcester State University. The opinions expressed in this article do not necessarily represent those of Justin's employers.*

(Continued on Page 10)

(Continued from Page 9)

***Matthew DeLeon, MSPPM is a Program Analyst at the National Association of County and City Health Officials (NACCHO). Matthew works on NACCHO's Public Health Informatics team, which aims to develop local health departments' ability to exchange, receive and use electronic health data to improve public health outcomes. Matthew holds his Master of Science (M.S.) in Public Policy and Management from Carnegie Mellon University's H. John Heinz III College, and holds a Bachelors of Arts (B.A.) in Government and International Politics from George Mason University. The opinions expressed in this article do not necessarily represent those of NACCHO.* ❖

CIP/HS is involved with a three year research study for the Department of Homeland Security looking at Improving the Effectiveness of Cybersecurity Incident Response Teams (CSIRTs). If you are a member of a CSIRT team or if you are involved in your organization's cybersecurity management or operations, we would like you to consider taking the attached survey. A link to the survey can be found here: https://www.surveymonkey.com/s/MHVXQTQ.

The survey should take 10 to 15 minutes to complete. The data collected in this study will be confidential and no individual or organization can be identified. A summary of the research results will be presented at future cybersecurity conferences and published in a future edition of the CIP Report.

Any questions on this survey or the DHS research study should be directed to me 703-993-4720 or via email at mtroutma@gmu.edu

Medical Identity Theft: Improving Cybersecurity Response Efforts

by Amanda Joyce, Michael Thompson, Andrea LeStarge, & Dr. Nathaniel Evans*

Background

On February 4, 2015, Anthem, Inc., the nation's second-largest health insurer, reported hackers broke into and stole a database containing the personal information of approximately 80 million customers and employees.[1] Although industry watchers do not believe that this incident resulted in the loss of personal health information, it prompted the following questions:

- What is being done to provide a best practice regarding the safeguarding of medical and personal health information?

- Is the health care and public safety sector sharing information to disseminate potential indicators and warning signs in order to implement protective measures against future theft?

Medical identity theft has become a "booming business," according to a *New York Times* article.[2] Medical information includes not only the typical personal identifiable information (PII) (e.g., social security number, date of birth, etc.), but also an individual's personal health information (PHI) (e.g., physician reports, orders/progress notes, diagnostic studies, etc.).[3] Electronic medical records introduce a variety of security and privacy concerns that have not been adequately addressed to date by the healthcare and information security professions.

> Why is medical information so enticing? Medical information includes not only the typical personal identifiable information (PII) (i.e., social security number, date of birth, etc.) but also one's medical history (i.e., physician reports, orders/progress notes, diagnostic studies, etc.).[3]

Problem Statement

Security experts warn that medical identity theft is not an unusual event; in one study approximately 90 percent of health care organizations reported they have had at least one data breach during the last two years.[4] Furthermore, security experts believe medical identity theft is on the rise because it pays.[5] Currently within the black market, complete medical records cost more than credit card numbers; in one instance, a patient's medical record sold for $251.00, whereas U.S. credit card records were selling for 33-cents.[6] Part of the discrepancy in prices is attributed to the amount of time that the record is valid for use, as once a credit card company is notified of the theft, the victim can freeze his/her credit and cancel the card/account, overall ending the viability of that credit card. On the other hand, medical records include information that cannot be easily changed, such as social security numbers, dates of birth, and physical characteristics (e.g., height, weight), making it impossible or nearly impossible to "cancel" the

(Continued on Page 12)

[1] National Health Information Sharing and Analysis Center(NH-ISAC), "NH-ISAC Alert – Anthem Cyber Attack" (Feb. 4, 2015), accessed Feb. 13, 2015, http://www.nhisac.org/blog/cyber-breach-news-data-breach-at-health-insurer-anthem-could-impact-millions.
[2] Reed Abelson and Julie Creswell, "Data Breach at Anthem May Forecast a Trend," *The New York Times* (Feb. 6, 2015), accessed Feb. 12, 2015, http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html?_r=1.
[3] Doctors Hospital at Renaissance, *Health Information Management (HIM)/Medical Records – FAQ*, accessed Feb. 12, 2015, http://www.dhr-rgv.com/Documents/HIMFAQ01.aspx; See also NH-ISAC, 2015, NH-ISAC Alert – Anthem Cyber Attack, Feb. 4, accessed Feb. 13, 2015, http://www.nhisac.org/blog/cyber-breach-news-data-breach-at-health-insurer-anthem-could-impact-millions, which states the following: "Investigators are still working to determine the scope of the [Anthem, Inc.] attack….The data breach resulted in exposing millions of names, birthdays, addresses and Social Security numbers, but medical personal health information does not appear to be breached."
[4] Ponemon Institute, *2013 Survey on Medical Identity Theft* (Traverse City, MI; Ponemon Institute, Sept. 2013), accessed Feb. 12, 2015, https://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-Identity-Theft-Report-FINAL.pdf.
[5] *Health Information Management (HIM)/Medical Records – FAQ*.
[6] Abelson and Creswell, "Data Breach at Anthem."

(Continued from Page 11)

record. As a result, the perpetrator gains useful information that is viable for a much longer period, and can be more widely used in everything from fraud schemes to passport forgeries.

Implications

Although credit card companies scan or analyze for inconsistent spending habits as potential indicators or warning signs of financial information theft, applying the same techniques to highlight misuse of medical identity information is much more difficult. As a result, victims of medical identity theft may find out about their victimization only through happenstance, as in the case of one individual who, when trying to donate blood 12 years ago, was denied without explanation. Perplexed, she called the agency to which she was trying to donate, only to learn that she was turned away because her social security number had been used to receive treatment at a free AIDS clinic in a different state, rendering her ineligible.[7]

The Federal Trade Commission warns:

> *A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. Once the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.*[8]

A Ponemon Institute study on medical identity theft concluded that an estimated 1.84 million adult Americans became victims of medical identity theft in 2013.[9] Furthermore, roughly 50 percent of the total estimated victims were not aware that medical identity theft could create inaccuracies within permanent records.

Mitigation Steps

The ultimate goal in risk mitigation is to protect a valued asset; in this instance, the valued asset is the medical identity and/or PHI. Health care providers need to adopt stringent best practices regarding protecting the security of medical identity information.[10] Specifically, providers should consider encrypting data-at-rest (i.e., their patients' medical identities and/or PHI stored in a database or digital medium) to reduce potential data leakage; they should also implement strong authentication and access control procedures. Implementing these steps can present challenges to smaller providers that lack dedicated staff to support information technology and security operations. Nevertheless, the highest priority must be placed on safeguarding patient information.

Another tool to aid in achieving risk mitigation is the sharing of information amongst trusted partners on the warning signs and indicators of potential threats and vulnerabilities. On February 12, 2015, President Obama signed an Executive Order to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government. The order encourages the development of central clearinghouses—Information Sharing and Analysis Organizations (ISAOs)—to share pertinent indicators and warning signs, vulnerabilities, and response plans to help curb or eliminate the impacts of cyber-attacks and facilitate information sharing in regional or sector-specific communities.[11]

The ISAOs, including the existing Information Sharing and Analysis

(Continued on Page 13)

---

[7] Laura Shin, "Medical Identity Theft: How the Health Care Industry is Failing Us," *Fortune* (Aug. 31, 2014), accessed Feb. 13, 2015, http://fortune.com/2014/08/31/medical-identity-theft-how-the-health-care-industry-is-failing-us.

[8] Federal Trade Commission, *Consumer Information: Medical Identity Theft* (Washington, D.C.; FTC, 2012), accessed Feb. 13, 2015, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

[9] Ponemon Institute, *2013 Survey on Medical Identity Theft*.

[10] Some best practices are outlined within the National Institute of Standards and Technology (NIST) Cybersecurity Framework, particularly the NIST 800-53 Publication on Security and Privacy Controls, and the Critical Controls for Effective Cyber Defense:

[11] The White House, *FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing*, Office of the Press Secretary (Feb. 12, 2015), accessed Feb. 13, 2015, http://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform; Katie Zezima, "Obama Signs Executive Order on Sharing Cybersecurity Threat Information," *The Washington Post* (Feb. 12, 2015), accessed Feb. 13, 2015, http://www.washingtonpost.com/blogs/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats.

(Continued from Page 12)

Centers (ISACs), will serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government.[12]

Specifically, one of those pre-existing ISACs is the National Health-ISAC (NH-ISAC), which provides "[a] collaborative partnership with the healthcare and public health sector, academia, standards, trade and certification organizations, …[and] is leading a national initiative to define and implement a National Health IT Cybersecurity Governance Model and a National Health IT Information Security Workforce Development Model."[13] The National Health IT Cybersecurity Governance Model is a nationwide partnership led by the National Healthcare and Public Health Cybersecurity Council, the Health Sector Coordinating Council (SCC), and NH-ISAC to unite the nation's health sector, cross-sector national critical infrastructure assets and government to enable health sector cybersecurity resilience through implementation and sustainability.

In addition, as known warning signs and indicators of attacks on systems are identified, sharing these elements amongst trusted partners within the private and government sectors can be crucial in stopping future exploitation of this data regardless of which critical sector was originally affected. Current efforts of the ISACs are helpful in information dissemination but will be greatly assisted by the adoption of machine-to-machine information sharing frameworks such as Facebook's ThreatExchange or Argonne National Laboratory's Cyber Fed Model. Near real-time sharing of threat information will ensure that organizations can protect themselves against new and persistent attacks as quickly as possible.

Argonne National Laboratory, the Center for Internet Security (CIS)/ Multi-State Information Sharing and Analysis Center (MS-ISAC), and various other ISACs — such as the NH-ISAC — are working in tandem to share, contribute, and collaborate regarding the actionable information and intelligence that are needed within government and the private and public sectors to detect, identify, and mitigate risks. To highlight, the MS-ISAC has partnered with the Medical Device Innovation, Safety and Security Consortium (MDISS) and a number of public and private sector partners to help with clearly articulating the value of applying well-defined security configuration baselines, thereby helping to further strengthen defenses against cyber-attacks. Through these partnerships, we enhance security intelligence, situational awareness, and knowledge centered on the risk elements of threat, vulnerability, and consequence.

Acknowledgment

The work presented in this paper was supported by Argonne National Laboratory under US Department of Energy contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne. Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

**Amanda Joyce, Michael Thompson, Andrea LeStarge, and Dr. Nathaniel Evans are with the Risk and Infrastructure Science Center (RISC)in the Global Security Sciences (GSS) Division of Argonne National Laboratory.* ❖

[12] White House, FACT SHEET.
[13] NH-ISAC, Membership Services, accessed Feb. 16, 2015, http://www.nhisac.org/membershipservices/.
[14] Center for Internet Security (CIS), "CIS and MDISS Launch Security Benchmark Mapping Guidance," Medical Device Security Benchmarks Initiative (2014), accessed Feb 17, 2015, http://benchmarks.cisecurity.org/about/MedicalDeviceOverview.cfm.

Defense in Depth: A Requirement for Every Healthcare Organization

by Parham Eftekhari & Ryan Kalember*

As the black market for healthcare data becomes larger, more sophisticated, and increasingly lucrative, healthcare stakeholders—which we define for the purposes of this essay as anyone who owns or transacts healthcare data—are now top targets for cyber criminals. To find proof of this one must look no further than the 138 percent increase in HIPAA data breaches since 2012,[1] a figure industry experts estimate will continue to soar. To respond to this threat, the healthcare industry is expected to increase spending on security products and services to $10B by 2020,[2] which would account for 10% of all critical infrastructure security spending.

As the healthcare industry scrambles to outpace the threats posed in the new digital health-ecosystem, we see it making the mistakes made by many of its peers: developing reactionary habits rather than establishing long-term, proactive security strategies. However, as the digitization of the healthcare industry is still relatively new, the community as a whole has a unique opportunity to implement security best practices based on advanced risk management strategies. We believe that begins with a Defense in Depth program.

Defense in Depth for Healthcare

One of the NSA's definitions for Defense in Depth is "a 'best practices' strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations."[3] This definition is important for a healthcare security executive to study and understand because it shows that a strong security strategy is not merely about implementing a set of technologies to protect the perimeter of your organization and keep "bad guys" out, but requires a combination of technical and non-technical elements to mitigate risk as effectively as possible.

To be certain, a strong defensive strategy does mean applying controls to different layers of your IT infrastructure including network, PCs, other devices, applications, and data,[4] which we will discuss later in this essay. However, the "depth" of your defense means that an executive must look at other aspects such as where your technology is being sourced from, leveraging non-security investments to bring visibility over your network and identify vulnerabilities, and working with partners and competitors to share information to protect yourself and the industry as a whole.

Key Aspects of Defense in Depth Strategy

Technology

While technology is not the only part of a security strategy, it is without a doubt crucial, especially proactive, analytical technologies that focus on prevention, detection, and response. Every healthcare organization must utilize SIEM (Security Integration and Event Management) technology to integrate their SEM (Security Event Management) and SIM (Security Information Management) functions into one system. The visibility afforded by a SIEM strategy was once considered

(Continued on Page 15)

[1] "Breach Report 2014 — Protected Health Information" *Redspin* (2014), available at https://www.redspin.com/resources/whitepapers-datasheets/Request-2014-Breach-Report-Protected-Health-Information-PHI-Redspin.php.
[2] "Healthcare Cybersecurity a Massive Concern as Spending Set to Reach Only US$10 Billion by 2020," *ABI Research* (Feb. 25, 2015), available at https://www.abiresearch.com/press/healthcare-cybersecurity-a-massive-concern-as-spen/.
[3] National Security *Agency, Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments*, (Fort Meade, MD: National Security Agency, undated), available at https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.
[4] "Better Security through Defense in Depth" *MC GlobalTech* (2014), http://mcglobaltech.com/component/k2/item/122-better-security-through-defense-in-depth.

(Continued from Page 14)

cutting edge, but should now be considered a standard requirement for any healthcare organization serious about its security.

Data encryption is another technology which exists and is infuriatingly underused, much to the delight of cybercriminals. Because health information is highly portable, often moving between devices, practitioners, administrators, and even different payer and provider organizations, implementing encryption and key management can often pose a challenge. Thankfully, solutions have emerged to keep health information encrypted or otherwise protected. File sharing and collaboration tools have now adapted to include information rights management (IRM) to secure information like test results and medical records that are in file format, while technologies like data masking have proven adept at securing health information stored in databases, even when it must be accessed by many different applications.

Identity and access management technology is a third technology which can dramatically impact an organization's security posture and an area where security leaders have an opportunity to think outside of the box and blend physical and virtual security to truly create sophisticated proactive security programs for their organizations. For example, if an employee is regularly accessing the building using his FOB key after hours or over the weekend, is there a program in place to check with his/her boss to see if the workload merits this level of extra hours? Access management technologies like dual-factor authentication and strong password programs are imperative, but innovation in this area is critical in Defense in Depth organizations.

Supply Chain Security

Supply chain security is especially important in the health arena due to medical devices which are used by doctors and patients to deliver care-critical medicine and data. An advanced supply chain strategy will not only look at who is making the equipment and how the product is getting from point A to point B, but the stability of the provider company itself. At the U.S. Department of Energy, the Office of the CIO has stated that part of its vendor evaluation program includes looking at the financial health of an organization to understand if the company providing the technologies or services is expected to be operating in the next several years, a viable question when making a multi-million dollar investment.

Information Sharing

Information Sharing comes in all different flavors, but it is critical that your organization establishes a culture that is inclusive of security information sharing with its peers. As Chris Schumacher, ICIT Fellow and Sr. Technology Consultant at New Light Technologies noted as part of a recent ICIT brief on upcoming cyber information sharing legislation, there are numerous public and private sector threat sharing portals that exist today. More importantly, thanks to technologies like encryption and IRM even truly sensitive information about breaches and internal security practices can now be shared without fear of disclosure.

The National Health Information Sharing and Analysis Center (NH-ISAC) is tasked with helping the nation's healthcare sector share threat information in a secure, safe environment and was instrumental, through the data sharing efforts of its members, to quickly ascertain that the Anthem hack attack was an isolated incident, not a broad attack on the healthcare industry or other critical infrastructure sectors. These types of insights are only possible when industry stakeholders are willing to share sensitive data and must continue in order for critical infrastructure sectors to remain resilient in the face of the enemy.

IT Asset Management

Historically, IT Asset Management (ITAM) has been used by CIOs with one goal in mind—saving money. While this is an obvious use of an ITAM platform, another innovative application of this strategy is as a means of fully understanding your IT footprint to identify potential vulnerabilities so you can then address them. In large organizations with hundreds (and sometimes thousands) of systems, it is not uncommon for licenses to expire and systems to remain on, but unpatched, for years without anyone knowing about them. These are a CIOs nightmare and a hackers dream, one that can be addressed using an ITAM strategy.

(Continued on Page 16

(Continued from Page 15)

Insider Threats

Today when people think of Insider Threats, they often think of Edward Snowden and CIA-type scenarios. While it may be argued that highly-classified environments have the most to worry about, the healthcare community is also at risk from insider threats, and a Defense in Depth strategy should include an insider threat component. Oftentimes in the civilian world, the risk comes not from a rogue nation but from an average "joe" who is down on his or her luck. To address these internal dangers, employers should use technology to their advantage to identify risk factors before they turn into a threat. What if an employee is preforming a high volume of searches on topics such as depression, divorce, or bankruptcy? Are these signs that he/she could be at higher risk of committing fraud against the company? Keep in mind this doesn't mean one should report this person to the comptroller or CFO; perhaps they just need to speak with H.R. However, a good Defense in Depth program is aware of the potential for risk to develop and is proactive in mitigating that risk before it happens.

Conclusion

In conclusion, the current state of information security in healthcare is best interpreted as an opportunity. While healthcare in general has been slow to adopt technologies and architectures like mobile devices and cloud computing, the silver lining of that slowness is that security technologies and practices have emerged in the meantime that can be leveraged to protect data that is traveling to more devices and across different infrastructures than before. This dynamic means that healthcare executives have a unique opportunity to develop risk management programs around these advanced security principles, and thus, the opportunity to provide patients the levels of privacy that they expect and rightfully deserve.

**Parham Eftekhari serves as Co-Founder and Senior Fellow at the Institute for Critical Infrastructure Technology (www.icitech.org). Mr. Eftekhari holds a B.B.A. in Marketing & International Business and a minor in French from the University of Wisconsin - Madison and the Ecole Superieure de Commerce de Paris (ESCP-EAP) in Paris, France.*

Ryan Kalember is the Chief Marketing Officer with WatchDox and a Fellow with the Institute for Critical Infrastructure Technology (www.icitech.org). Mr. Kalember earned his B.A. at Stanford University. ❖

Mobile Device Usage in the Operating Room

by Amanda Joyce, Michael Thompson, & Dr. Nathaniel Evans*

The Emergency Care Research Institute (ECRI) predicts that 2015 will bring an increase in cyberattacks, making cyber one of the major areas of concern for the health care industry in 2015.[1] Many modern medical devices contain the same software and hardware as normal home computers, making them vulnerable to many of the same flaws. A modern anesthesia machine includes the following components: connections for oxygen, medical air, and nitrous oxide; reserve gas cylinders; high-flow oxygen flush; pressure gauges; flow meters; vaporizers; integrated ventilator; manual ventilation bag; breathing circuits; systems for monitoring gases, heart rate, electrocardiogram (ECG), blood pressure and oxygen saturation; and safety features in case of mishaps.[2]What many may not know is that anesthesia machines have universal serial bus (USB) slots and Ethernet connections.

Anesthesia machines have been under scrutiny for a bug found when plugging a device into the USB ports. Spacelabs Healthcare is recalling the ARKON Anesthesia System[3] with software version 2.0 due to a software defect that has led the FDA to issue a Class I advisory recall.[4] The software defect could cause the system to stop working when the USB ports are used for charging. This isn't the first recall that ARKON has had. Last year a recall was made due to the ease of obtaining personal data of patients.

Medical professionals have stated that the USB ports are meant to export information such as monitoring data and information regarding drug dosages and ventilation. This information is exported for medical records, audits, and research purposes. With that said, they agree that the USB port should be better secured to only allow for extraction of necessary information and not used for recreational purposes.

This is not the only vulnerability reported in these types of machines. Anesthesia machines and vital sign monitors are among devices subject to hard-coded password vulnerabilities. These types of vulnerabilities leave devices open to potential targeted attacks. One potential scenario outlines an anesthesia machine compromised in such a way that it doses anesthesia contrary to what the anesthesiologist enters. Then couple that with a vital sign monitor that says the patient's heart is beating at a healthy seventy beats per minute, when in reality the patient's heart is beating at a dangerous five beats per minute—a potentially lethal combination. Especially with mobile device proliferation and the relative lack of security protocols and protections on personal mobile devices, these types of personal devices act as perfect entry or "pivot" points for targeted attacks.[5]

Human factors or errors are the leading contributors to equipment-related problems. More training on the equipment and work-related uses may be needed. An analysis report from 1961-1994 showed that 72 of 3,791 claims (2%) were related to the machine/delivery. The most common adverse outcome was death (47%) and brain damage (29%). In 78% of the cases, better monitoring would have prevented adverse outcomes. When possible, design of equipment should be such

(Continued on Page 18)

[1] Rachel Bloodgood, "Data Security, HIPAA Audits Top Health Care Concerns for 2015," *Lockpath Blog* (Jan. 5, 2015), accessed Feb. 13, 2015, http://lockpath.com/blog/data-security-hipaa-audits-top-health-care-concerns-for-2015/.

[2] Michael Dosch, *The Anesthesia Gas Machine* (Detroit: University of Detroit Mercy Graduate Program in Nurse Anesthesiology, 2012), accessed May 9, 2014, http://www.udmercy.edu/crna/agm/02.htm.

[3] Spacelabs Healthcare, *ARKON* (2013), accessed May 9, 2014, http://www.spacelabshealthcare.com/anesthesia-delivery-ventilation/anesthesia-system/arkon/#.U2z77PldXtc.

[4] Phi Tran, "Anesthesia Devices Can Fail When Connected to Cell Phones," *Social Times* (Apr. 23, 2014), accessed May 9, 2014, http://www.adweek.com/socialtimes/anesthesia-devices-can-fail-when-connected-to-cell-phones/198550.

[5] Zuk Avraham, "The Biggest Threat to Enterprises Comes on the Smallest Screen," *Wired Innovation Insights* (Nov. 25, 2014), accessed Feb. 13, 2015, http://insights.wired.com/profiles/blogs/the-biggest-threat-to-enterprises-comes-on-the-smallest-screen#axzz3RdrsheSW.

[6] Bettina Dixon, Patient Safety and the Anesthesia Gas Machine (Pittsburgh: University of Pittsburgh, 2006), accessed May 9, 2014, http://c.ymcdn.com/sites/www.pana.org/resource/resmgr/docs/pana_fall06_agm_safety_prese.pdf.

(Continued from Page 17)

that human error cannot occur.[6]

The American Association of Nurse Anesthetists (AANA) Scope and Standards for Nurse Anesthesia Practice emphasize continuous clinical observation and vigilance as the basis of safe anesthesia care. Certified Registered Nurse Anesthetists (CRNAs) have an ethical responsibility to provide sage patient care by avoiding non-essential distractions: smart phones, tablets, personal digital assistants (PDAs). The AANA supports the use of mobile devices as established by institutional policy for patient-related communication among members of a patient care team to enhance care, but staff should avoid unnecessary use of these tools when delivering anesthesia care services. Few organizations have cell phone policies specific to the operation room (OR), an informal information gathering found. It has become a common sense issue and customer service concern that each OR personnel must consider.

Additional concerns related to mobile device use in the OR are bacterial contamination, interference with medical equipment, and interruptions/distractions. A study showed that after 40 anesthetists used hand sanitizer then were asked to make a short personal phone call, 95% had bacterial contamination on their hands again.[7] The benefit of using mobile phones in the OR should be weighed against the risk of unperceived contamination. A 2003 survey of 4,018 anesthesiologist respondents showed that approximately 2.5% of respondents saw some interference with medical equipment.[8] Although only a small percentage saw interference with equipment, this small interference can lead to bigger problems. Additionally, the use of mobile devices within the OR has led to a larger number of interruptions. Approximately 68 interruptions and distractions per hour occur for CRNAs.[9] Most are from OR personnel, noise, and communication, but mobile device usage was also considered.

Mobile technology has the potential to have a positive impact on healthcare. As such AANA encourages CRNAs and anesthesiologists to participate in the development of institutional policies regarding the usage of mobile devices and social media.[10] In addition, device manufacturers should closely evaluate the security processes in the design of their products, including identifying and addressing the cybersecurity risks of the devices they manufacture and documenting the steps the manufacturer has taken to implement appropriate risk-mitigation measures.[11]

In October of 2014, the U.S. Food and Drug Administration (FDA) released guidance for medical device manufacturers. The guidance suggests that medical devices should have ways to limit access to trusted users, including complex passwords that can be changed rather than hard-coded. It also includes the use of biometric and token authentication whenever applicable. Devices should be tested during development to assure that it's possible for them to be used safely even when their security has been compromised. The report issues a number of other important security suggestions for both medical device manufacturers and users that should be integrated into policy for health care institutions and industry.[12]

Implications

Mobile device usage within the OR can lead to distractions within the room and lead to serious events such as mistakes, wrong procedures, or even death. For the first time in

(Continued on Page 19)

[7] Jeske HC, Tiefenthaler W, Hohlrieder M, Hinterberger G, and Benzer A, "Bacterial Contamination of Anaesthetists' Hands by Personal Mobile Phone and Fixed Phone Use in the Operating Theatre," *Anaesthesia 62*, no. 9 (Sep. 2007):904-906.

[8] Soto RG, Chu LF, Goldman JM, Rampil IJ, and Ruskin KJ, "Communication in Critical Care Environments: Mobile Telephones Improve Patient Care," *Anesthesia & Analgesia* 102, no. 2 (Feb. 2006):535-541.

[9] Pape TM and Dingman SK, "Interruptions and Distractions During Anesthesia Induction: A Pilot Study," *Plastic Surgical Nursing* 31, no. 2 (Apr.-Jun. 2011): 49-56.

[10] American Association of Nurse Anesthetists, *Mobile Device Use* (Park Ridge, IL: AANA, 2013), accessed May 9, 2014, http://www.aana.com/resources2/professionalpractice/Documents/PPM%20PS%202.18%20Mobile%20Device%20Use.pdf.

[11] Philip Desjardins, "FDA Scrutinizes Networked Medical Device Security," *Information Week* (Dec. 1, 2014), accessed Feb. 12, 2015, http://www.informationweek.com/healthcare/security-and-privacy/fda-scrutinizes-networked-medical-device-security/a/d-id/1317758.

[12] Office of Device Evaluation & Office of Communication, Outreach, and Development, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Washington, DC: Department of Health & Human Services, 2014), accessed Feb. 12, 2015, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

(Continued from Page 18)

2013, mobile devices were in the top 10 health technology hazards list completed by the ECRI Institute.[13] According to the Pennsylvania Patient Safety Advisory, analysis on the events reported between January 2010 and May 2013 revealed 304 reports of events that occurred in the OR due to distraction. Approximately 73.7% (224) reported that the distraction caused errors related to procedures, treatments, or tests. Of those 224 that reported distraction, 75.4% of those were during surgery or an invasive procedure, followed by laboratory test problems (19.2%).[14]

Regardless of frequency of events, all OR distractions should warrant additional attention. Some serious events that have been reported due to distraction are:

- Wrong-side surgery,
- Wrong-site surgery,
- Transfusion of wrong blood, and
- Injection using an unlabeled syringe.

While smartphones offer benefits for health care providers in terms of improved communication and ready access to guidelines, they also carry a number of risks. Mobile devices carry bacteria and viruses that pose infection risk, especially within the OR. The most dangerous threat to patients is the lack of attention and focus from the doctors.

When these serious events occur and a claim for malpractice is pursued, the lawyer's first step is collecting records of everybody's cellphone usage in the room. A case in Dallas in which a woman died during surgery to correct her heartbeat caused a large malpractice suit. The surgeon accused the anesthesiologist of looking at their mobile device and failing to notice the patient's low blood-oxygen levels for over 15 minutes.[15]

Additionally, mobile device usage can interfere with some of the medical equipment. Although the overall power usage of mobile devices has been significantly reduced from the beginning days of cell phones to today's versions, there is still older equipment in use that may not work properly with cell phones. For example, older ICU ventilators utilized an antenna that would receive cell phone signals. Susceptibility to mobile device interference is no longer acceptable for medical personnel and medical equipment manufacturers, and thus all new medical equipment must be unaffected when a mobile device is used.[16]

Mitigations

Clear policies need to be in place governing the usage of mobile devices in operating rooms. Those policies must govern the appropriate use of personal devices and organization-owned devices. Policies must include policing and enforcement to ensure compliance. The use of mobile devices to assess a patient's history, update information, and look at their recent procedures may be acceptable, but must be done with organization secured mobile devices, ideally with central control from a mobile device management (MDM) software solution. These devices have a number of benefits, including providing a quicker update channel for doctors' and nurses' notes and getting instant access to records. The utility of these devices should not be ignored, but the potential dangers must be compensated for in appropriate policies and governance.

Conclusion

Mobile device usage within the medical field has provided both additional benefits but also has led to an increase in distractions. Health care professionals should look into creating policies within their organizations that put into place the usage of a personal or work mobile device during major procedures. Additionally, health care professionals should understand the consequences of mobile device usage when treating a patient. Finally, training on the potential work hazards should also

(Continued on Page 20)

[13] ECRI Institute, "Top 10 Health Technology Hazards for 2013," *Health Devices* 41, no. 11 (Nov. 2012):342-65, available at, file:///C:/Users/dpitman/Desktop/2013_Health_Devices_Top_10_Hazards.pdf.

[14] Michelle Feil, "Distractions in the Operating Room," *Pennsylvania Patient Safety Advisory* 11, no. 2 (June 2014): 45-52. available at http://patientsafetyauthority.org/ADVISORIES/AdvisoryLibrary/2014/jun;11(2)/Pages/45.aspx.

[15] Markian Hawryluk, "Is Your Surgeon Focused on You or His Smartphone?," *The Bulletin* (Feb. 2, 2015), accessed Feb. 13, 2015, http://www.bendbulletin.com/newsroomstafflist/2834727-151/cellphones-in-operating-room-pose-patient-safety-risks.

[16] Michael Dreyfuss, "Another Look at Cell Phone Use in the Operating Room," *Anesthesiology News* (July 2004), accessed Feb. 13, 2015, http://www.anesthesiologynews.com/ViewArticle.aspx?d_id=8&a_id=2661.

(Continued from Page 19)

be provided to health care organizations.

Acknowledgment

The work presented in this paper was supported by Argonne National Laboratory under US Department of Energy contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne. Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

**Amanda Joyce, Michael Thompson, and Dr. Nathaniel Evans are with the Risk and Infrastructure Science Center (RISC) in the Global Security Sciences (GSS) Division at Argonne National Laboratory.*

Mason-IBM-NSF Cybersecurity Leadership and Smart Grid Conference
April 30, 2015
Hyatt Fair Lakes in Fairfax, Virginia
Registration information for that conference is:
http://goo.gl/v4zq97

In October's CIP Report, we provided an early overview of the Mason - IBM - NSF Cybersecurity Research Workshop that took place on July 11, 2014. We are pleased to report that the workshop report "Cybersecurity and Smart Grid Leadership" from that very informative event is now available. You can access and download the conference report at this link: http://goo.gl/xuMmYb; Findings from all aspects of the projects will be unveiled and vetted at the Mason-IBM-NSF Cybersecurity Leadership and Smart Grid Conference. Registration information is below.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1