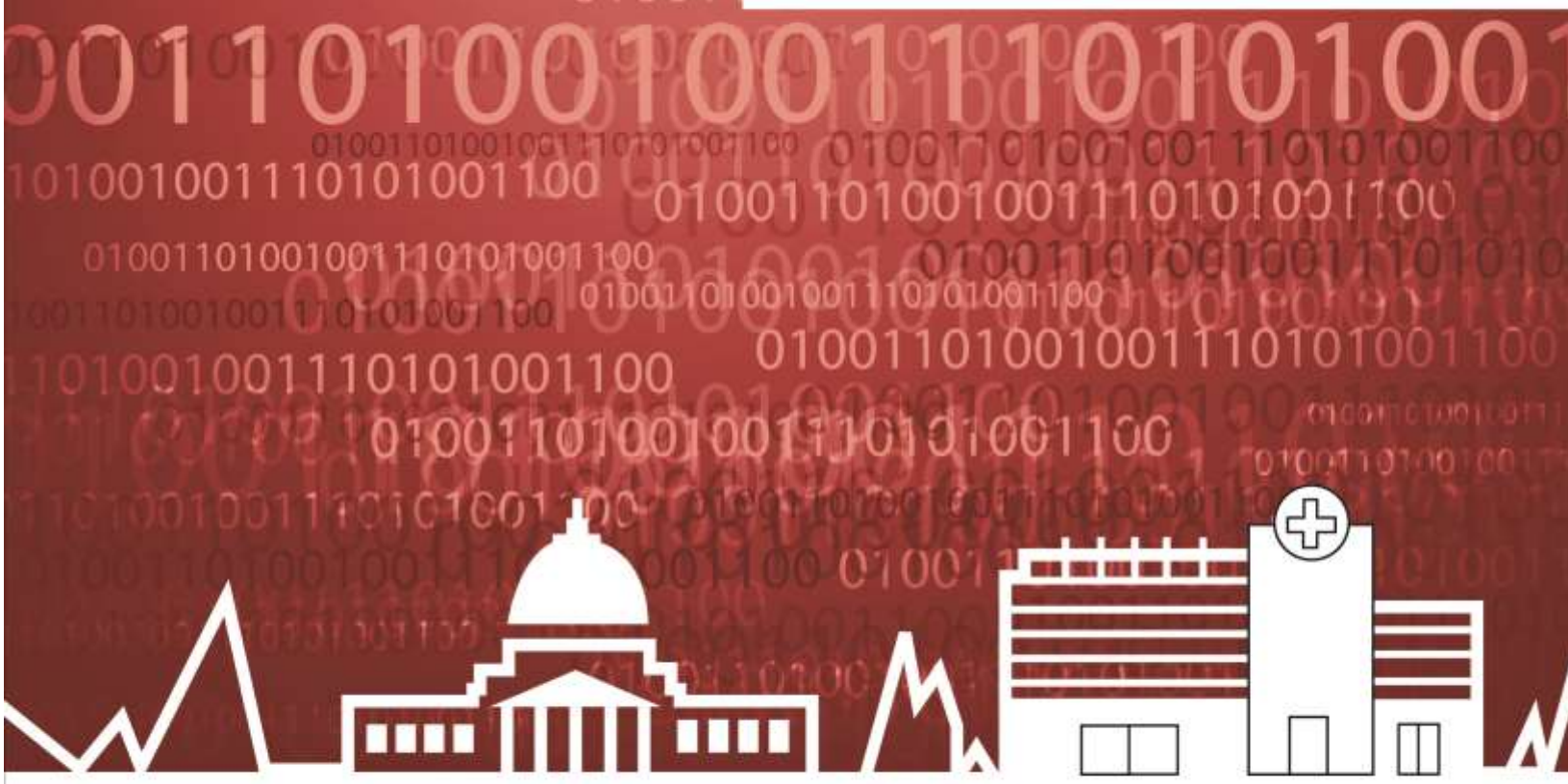
ICIT | Institute for Critical Infrastructure Technology



HACKING HEALTHCARE IT IN 2016

LESSONS THE HEALTHCARE INDUSTRY CAN LEARN FROM THE OPM BREACH

JANUARY 2016

Introduction:

Among all of America's critical infrastructures, the healthcare sector is the most targeted and plagued by perpetual persistent attacks from numerous unknown malicious hackers, intent on exploiting vulnerabilities in their insecure and antiquated networks in order to exfiltrate patient health records. The United States of America spends approximately 18% of its GDP on healthcare. Incidentally, ~47% of the population of the United States have had their personal healthcare data compromised over last 12 months. According to digital security company Gemalto's report "Data Breach Index for the first half of 2015," of the 16 critical infrastructure sectors, the Healthcare industry suffered from the most recent data breaches, an estimated ~21% (188 out of 888 reported events). One could argue that the healthcare sector is the prime target for malicious cyber groups; however, the sector may just be the most susceptible to successful compromise. According to a 2012 SANs institute report, of the malicious traffic targeting the healthcare sector, 72% targeted healthcare providers, ~10% targeted healthcare business associates, and 6% targeted health plan organizations. The remaining 12% of traffic targeted pharmaceutical companies, healthcare information clearinghouses, and other healthcare entities. Though the distribution of malicious traffic may have altered slightly in the past 3 years, the data suggests that attackers are targeting the healthcare entities that are less likely to have modern information security systems. Healthcare providers, the largest target, are focused on their mission: saving lives. Meanwhile, healthcare payers focus on processing the transactions necessary to keep patients healthy and healthcare providers operational. Both providers and payers devote the majority of their resources to fulfilling their mission. Attention, trained personnel, and funding are all limited resources. In the healthcare sector, these resources are

deployed to help as many patients as possible. Sadly, attackers have seen this selfless dedication to human life as sign of weakness. Since 2009, the annual number of cyber-attacks against the healthcare sector has drastically increased; often the number of attacks exceeds the previous year's count by at least 40%. So far, the healthcare sector has remained a succulent target because organizations only began to seriously invest in cybersecurity in the past 5 years.

In KPMG's 2015 "Health Care and Cyber Security" survey, 81% of the participating 223 healthcare CIOs, CTOs, Chief Security Officers, and Chief Compliance Officers revealed that systems at their organization were compromised by one or more cyberattacks within the last year. The remaining 19% consists of organizations whose systems remained secure, organizations that did not willingly admit to KPMG that malicious actors had breached their system, and respondents who did not know whether their system had been compromised. In all three cases, the possibility of an undiscovered or unreported breach is likely because only 75% of the respondents felt that their organization had the capability to detect a compromise. Only 53% of the healthcare providers assessed themselves capable of defending themselves from a cyberattack after detection. Considering all the doubt in the survey results, there is a strong likelihood that the percent of recently compromised systems is greater than the predicted 81%. In either case, the healthcare sector is extremely vulnerable to cyber-attacks. Organizations need to begin to immediately develop and implement multilayer security programs to protect their systems, their employees, and their customers.

Healthcare organizations and federal agencies dynamically integrate new systems into their infrastructure over time, according to their needs. Rick Caccia, CMO of Exabeam, notes, "Healthcare organizations and OPM, like many government agencies, manage an infrastructure built over multiple technology waves, and the layers created often have gaps that enable hacker

access. Coupled with the management of very sensitive data, this is a formula for eventual breach." Gradually, their infrastructure develops into a construction of technology from multiple eras. These heterogeneous systems are liable to software and hardware vulnerabilities at points where different technologies overlap. The systems are cumbersome and system administrators can have difficulty properly managing the assortment of systems. In many cases, the manufacturers of components of the overall system no longer provides support for that product. The software of these legacy systems is no longer updated and no patches are released for the system. Stan Wisseman of HP points out that "Out of date software, unimplemented patches, or even outdated passwords could be the vulnerability that exposes sensitive information of a patient database." Legacy systems, especially those more than a decade old, are extremely vulnerable. They are also often high value targets for attackers because the systems are vulnerable, they often contain valuable data or easy access to data, and they are integrated too deeply into the organization's infrastructure to be replaced.

The Healthcare sector manages very sensitive and diverse data, which ranges from personal identifiable information (PII) to financial information. Data is increasingly stored digitally as electronic Protected Health Information (ePHI). Systems belonging to the Healthcare sector and the Federal Government have recently been targeted because they contain vast amounts of PII and financial data. Both sectors collect, store, and protect data concerning United States citizens and government employees. The government systems are considered more difficult to attack because the United States Government has been investing in cybersecurity for a (slightly) longer period. Healthcare systems attract more attackers because they contain a wider variety of information. An electronic health record (EHR) contains a patient's personal identifiable information, their private health information, and their financial information. EHR

adoption has increased over the past few years under the Health Information Technology and Economics Clinical Health (HITECH) Act. Stan Wisseman comments, “EHRs enable greater access to patient records and facilitate sharing of information among providers, payers and patients themselves. However, with extensive access, more centralized data storage, and confidential information sent over networks, there is an increased risk of privacy breach through data leakage, theft, loss, or cyber-attack. A cautious approach to IT integration is warranted to ensure that patients' sensitive information is protected.” Healthcare networks serve as a larger pool of potential victims. The vast majority of human beings are in at least one healthcare system, while only a fraction of the population is included in government systems. Some threat actors seek to steal identities, some attackers seek information about specific high profile patients, and some attackers want to harm the healthcare providers. As a result, of the wider variety of information available about a larger selection of victims, a wider variety of attackers target healthcare systems. In general, healthcare breaches have a higher impact and greater fiscal return than government breaches.

Nevertheless, in the last year alone systems in both the healthcare sector and the federal government have proven remarkably vulnerable and lucrative to attackers. In fact, according to Rob Bathurst, Professional Services Director of Cylance, “While working and consulting in the healthcare sector, we have noted the sector is currently lagging behind other sectors in deployed prevention, detection, and reactive technologies. In addition some healthcare organizations lack properly trained personnel capable of operating currently deployed technologies.” This means that attackers who are hoping to maximize their return on resource investment will target under-protected healthcare systems (the more vulnerable of the two target groups) while attackers who are sponsored for enemy nation states may attack either government systems or healthcare

systems. Healthcare organizations are subject to greater regulatory pressure than government entities; but, healthcare organizations also have greater fiscal flexibility and greater autonomy. As a result, healthcare organizations have the opportunity to rapidly decrease the risk to their systems by propagating a multilayer information security program within their organizational culture. An effective program would justify budget allowances by deterring cybersecurity incidents, by better adhering to regulation (such as the HIPAA Security Rule), and by providing a definitive competitive operational advantage over other competitors.

Malicious actors will find and expend significant resources to exploit the vulnerabilities in healthcare systems because the data contained within is diverse and valuable. Often, in these integrated systems, old backdoors and compromised user accounts enable adversaries to silently penetrate and persist on a network. Once the attacker has infiltrated the network, they will create additional backdoors to establish a persistent presence on multiple systems across the network. Then, they map the network and they will identify valuable data. Finally, the data will be exfiltrated out of the network. If the organization fails to detect the suspicious activity on the network or if they fail to re-secure their network, then the adversary may continue to revisit the victim systems in order to collect more data. Depending on the quantity and quality of data stolen, the compromised organization will face legal, fiscal, and reputational harm when the breach is discovered and reported.

The healthcare sector must invest in more robust and comprehensive organizational platforms because the value of data contained in their systems combined with the lax security surrounding that data is increasingly more appealing to nation state actors, cyber criminals, and hacktivists alike. Using only phishing attacks and exploit kits available on the dark net, even a "script kiddie" might be able to compromise the system of a major healthcare provider. The actor

that breached OPM, Anthem, and Premera did not use overly sophisticated tools. They used email and their custom exploit kit (which mostly resembles malware kits available on the dark web). Stan Wisseman argues, “The healthcare industry must recognize the need to invest in cyber security programs and have resources dedicated to continuous monitoring and ongoing improvement of their security posture.” A hospital accrues a surprisingly wide amount of information and stores it in one (often-vulnerable) system. A healthcare database contains over 18 PII identifiers (name, address, social security number, etc.), a patient’s private health information (PHI), and a patient’s financial payment information (insurance and credit card information). Rick Caccia adds, “Healthcare firms manage a surprisingly broad amount of sensitive data. They have all of a patient’s personal information, such as address, social security numbers, spouse, children, etc. They have all of a patient’s sensitive health information, and they often have a patient’s payment information: credit cards, bank accounts, etc. Put a different way, your hospital has a greater and broader amount of your private data than your employer or your bank does.” One could argue that healthcare providers, whose mission is to help patients according to the Hippocratic Oath, have a responsibility to protect patient and employee data. By shirking the responsibility to protect critical information assets on a platform of fiscal returns, the hospital is placing its patients and its employees in direct harm.

Throughout 2014 and 2015, cyber-forensic evidence suggests that one advanced persistent threat group targeted heterogeneous systems in the Healthcare sector and the United States Federal Government. The actor, believed to be Deep Panda, concurrently conducted extensive attacks against systems belonging to Anthem, Premera Bluecross, and the United States Office of Personnel Management. All three organizations depended on vulnerable systems that held valuable diverse data about American citizens. Every healthcare and government

system associated with a victim of Anthem, Premera Blue Cross, or OPM is at risk because the threat actor has been known to use information from previous attacks to compromise new victims. The adversary compromised OPM, and likely the other two notable victims, by compromising the systems of a third party service provider. As a result, third party service providers are at an elevated risk of compromise and larger entities are at an increased risk through association. Additionally, current employees at healthcare providers or at associated third parties could pose an inadvertent risk of insider threat if they previously worked for one of the victims. The adversary may attempt to gain access to new victim systems through the account credentials from previously compromised systems in the hopes that employees, who have worked for both a victim and the target, will reuse credentials. Any healthcare employee who has had a background check through OPM, USIS, or Keypoint may likewise pose a risk to their organization because the threat actor will use the stolen information to compromise healthcare employee account credentials.

The OPM breach is arguably the most prolific breach in the history of the United States because the massive amounts of high quality data stolen from undefended legacy systems could hinder the United States intelligence community for decades to come. As a result, the OPM breach has been extensively examined in Congressional hearings and in the media. United States organizations need to learn from the OPM breach. Its example of how large of an impact poorly maintained and defended integrated systems can have, should not go unnoticed. Organizations should infer lessons about how they can protect themselves from similar threats. The healthcare sector, which has already been targeted by this actor, is at the greatest risk. Rather than ignoring the threat hoping that insurance policies are large enough to cover the costs of a breach, the Healthcare sector needs to invest in risk management based information security programs.

Cybersecurity programs should be a multilayered defense that protects the confidentiality, integrity and availability of information whenever it is stored, in transit, or being processed. According to Rob Bathurst, "The importance of a multilayer security program covering people, processes, and technologies cannot be overstated." OPM failed to institute such a multilayered security program in spite of repeated recommendations of the Inspector General. As a result, the OPM breach directly affected 22.1 million American citizens. Similarly, in the healthcare sector, the Premera and Anthem breaches directly put an estimated 11 million and an estimated 79 million American citizens, respectively, at risk. Since the same actor that targeted OPM is attacking the healthcare sector and since the healthcare sector as a whole suffers from the same failings as OPM, the lessons from the aforementioned breaches can guide multilayer cybersecurity initiatives in healthcare organizations.

The Healthcare System's Adversaries:

Adversaries can use the information stolen in healthcare breaches for insurance fraud, identity theft, financial gain, or targeted attacks. Attackers can sell information online or use the information themselves. An adversary or their client may use stolen insurance information to create fake insurance credentials. The actor can then create appointments, undergo surgery, or have other medical procedures performed at the expense of the victim and healthcare organizations. The actor could also use the information to obtain prescription medicine under the victim's identity. According to Computer World, fraudulent billing accounts for 3-10% of annual U.S. health expenditures. The masquerade financially burdens the victim and could lead to legal ramifications. Further, if the actor is a different blood type, then either the actor or the victim could be at risk of serious medical harm.

Similarly, the PII, PHI, and EHR data can be used to steal the identity of patients and employees. The actor might be able to access financial accounts, take out loans, or apply for credit in the victim's name. If unnoticed, the actor might continue to live under the guise of the victim for an extended time. There have been cases of identity theft where the actor purchases property, holds a job, or is arrested under an assumed identity. Because healthcare systems contain information about practically every individual, the possible impacts of identity theft are numerous. As expected, healthcare employees are at the most risk. Doctors tend to earn reasonable salaries and they have the ability to issue prescriptions; consequently, their identities might carry a high value on the Darkweb marketplaces. Additionally, support staff are at risk for short-term financial attacks. When UPMC systems were compromised, the actor used the information to digitally file the income taxes of employees and collect their returns. Afterward, the actor could sell the information on the Darkweb to identity thieves. Conversely, the stolen health information could be combined with the information stolen from OPM to conduct targeted attacks.

Attackers could use private health information to extort money or influence from victims. What would an HIV patient pay or do to not have their condition revealed to coworkers? Private health information could also be combined with the information stolen in the OPM breach to create a database of United States intelligence personnel. The information could also be used to locate or harm intelligence assets within the country or abroad. If the scenario seems farfetched, consider that in 2010, Wired Magazine writer Evan Ratliff wrote an article about how to vanish from society by not leave a digital footprint. He then attempted to practice his research by following the steps and hosting the repomen contest in which readers where offered a $10,000 prize if they could locate him within a year. The winner of the contest found Ratliff, states away

at a motel, based on a medical dietary restriction (gluten intolerance). Imagine the impact a malicious actor could inflict if they knew the medical history of intelligence assets who were now overseas. Even seemingly innocuous conditions, such as Ratliff's gluten intolerance, could be life threatening. In further example, during his tenure as Vice President, it was discovered that Al Qaeda operatives were attempting to compromise Dick Cheney's pace maker by exploiting an unsecured Bluetooth connection. Knowing that a target has an embedded device presents a previously unexplored attack vector. Mobile healthcare technologies are in need of a security renaissance and they are only made more vulnerable when attackers also compromise electronic health records. For the sake of their patients, employees, and executive board, healthcare organizations need to invest in security solutions that protect physical devices as well as intangible records.

The most basic cyberattack against an internet enabled system proceeds in three phases. First, the attacker researches their target and the target's network. Next, the attacker searches for vulnerabilities in the outward facing systems that can be exploited. The attacker may run a port scanner against the network to discover ports that were mistakenly left open or the attacker could run a vulnerability scanner against the target network to try to identify old vulnerabilities that the victim failed to patch. The attacker could infect perimeter devices and analyze outbound network traffic with a packet sniffer in order to capture trusted user credentials. The attacker could also steal trusted user credentials by generating a realistic fake website and tricking the user into entering their credentials. The fake website may then redirect the user to the real site as if nothing suspicious occurred. Alternately, the attacker could employ a social engineering campaign featuring phishing emails or interaction with personnel of the target organization in an attempt to trick the employees into revealing specific information. Phishing emails are scam

emails that either contain malware that allows attackers into a system by installing a virus, Trojan, etc., or they trick the user into responding to the email with their system credentials. Though phishing emails were obvious in the 1990's (the Nigerian Prince scam for instance), modern phishing emails are convincing and sophisticated. Phishing emails remain the most effective attack vector against organizations because Americans are culturally programmed to open emails and because attackers obfuscate the insincerity of the message by making the email resemble a legitimate email. In some cases, the emails even feature legitimate information that the hackers stole from other sources. Finally, the attacker leverages a discovered vulnerability to gain access to a system on the target network. Common security exploits include remote access through antiquated protocols (such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), PHP, SSH, and Telnet), through errors in the code itself, or through security exploits such as SQL injection attacks, cross site script attacks, and cross-site request forgery attacks that allow the attacker to inject their own code into an application. Afterward, the attacker may use rootkits or malware to establish a persistence presence on the network or they may laterally move across the network to a more desirable system.

Cyber attackers can be categorized according to their target selection, tactics, techniques, malware and procedures. Any of the attacker groups detailed below (script kiddies, cybercriminals, and nation-state actors) will attack systems based on the vulnerability of the system and the opportunity presented to the attacker. Hacktivists retaliate against opposing political and ideological platforms or against organizational action deemed unsatisfactory or offensive. Cybercriminals attack systems in an attempt to generate a profit through the exploitation or auction of victim data. Finally, nation-state actors operate in accordance with geopolitical agendas.

Script Kiddies:

Script Kiddies are the most basic and least skilled cyber attackers. Script Kiddies tend to purchase, trade, and use tools and malware developed by other attackers. The majority of these tools and scripts are automated during their design because the kiddies who operate them lack anything more than basic technical knowledge. Most script kiddies do not even understand the concepts or code underlying the tools that they purchase from black hat hackers. Kiddies tend to engage in attacks of opportunity against networks that the online community deems vulnerable. In some cases, the kiddie knows the system that they want to target before they even acquire or commission the tool. Individual script kiddies may attack targets in the health sector; however, unless the kiddie possesses a zero-day exploit or the target failed to patch vulnerable systems, most commercial systems are sufficient to repel attacks from script kiddies. Most attackers enter the underground communities as neophytes and most attackers never mature past this initial phase to become more than a script kiddie.

Hacktivists:

Hacktivists are politically motivated attackers that conduct cyber-attacks against systems belonging to organizations that either are opposed to their hacktivist agenda or are high profile enough for the attack to serve as viable platform to propagate their propaganda through the resulting media attention and political backlash. Hacktivist groups may also conduct cyberterrorism attacks as part of a political agenda. Members of the groups range in their skill levels from script kiddie to black hat hacker. Regardless of skill level, the majority of the collective rely on common tools readily available on dark net markets because the tools are both

known to be effective and cheap (if not altogether free). Some more advanced participants may incorporate customized malware into an attack and use the crowd of other users as obfuscation.

The most common hacktivist attack is a denial of service (DDoS) attack, which overloads a server or system with undesired traffic in order to halt the operations of the target organization. Common DDoS tools are Low-Orbit-Ion-Cannon (LOIC) and its newer variant High-Orbit-Ion-Cannon (HOIC). The tools simulate a flood of malicious fake visitor traffic that taxes a website until it crashes. Software built into the tool then prevents the site from recovering from the crash until the attack is halted. HOIC also uses custom scripts called "boosters" to spread the traffic around sub-pages of the target domain in order to spread the defender's resources thin. If LOIC is a pistol, then HOIC is a shotgun. Either variant can be found on Google in less than 5 minutes. The tools are designed to be usable by anyone of any technical proficiency. In the case of HOIC, a user need just download the tool, enter the address of the target website, and turn on the tool. More advanced participants might employ web application attack tools, like SQLi, to steal data from the overloaded site. In this case, the goal of the attack, termed doxing, is to steal confidential information and to reveal that information to the public. Many commercial systems, such as firewalls, can be configured to block LOIC traffic; however, HOIC is newer and more difficult to defend against. Websites are built to withstand considerable quantities of visitor traffic. Attacks against a site of a reasonably sized organization, such as the website of a hospital, payer, or even healthcare.gov, would likely require around 50 attackers operating the tool. Alternately, an attacker could infect vulnerable systems through phishing campaigns, or other simple attack vectors, and create a botnet of infected machines in order to conduct an attack. The healthcare sector should worry about doxing attacks that target patient data or intellectual property. Attackers could also attempt to embarrass the healthcare organization through the

revelation of compromised information or through a breach that is public enough to harm the organization's reputation.

Hacktivist groups tend to be decentralized and lacking any organizational structure. Multiple factions may exist within each group; in some cases, the factions do not agree on choice of target or method. While individual participants may be monitored and investigated, the decentralization and lack of coherent leadership structure and roles makes hacktivists groups difficult to track and predict as a collective. The most popular hacktivist groups at the time of this writing is the global hacker collective Anonymous.

Anonymous is by far the most notorious hacktivist group. Since its birth on the 4chan message boards in 2003, Anonymous has become one of the best-publicized hacker groups in the media, thanks in part to its adoption of the iconic Guy Fawkes mask, its pseudo-anarchistic culture, and its open community. If a user believes in the agenda of the group, then they are welcome to consider themselves an active member. Membership prohibits discussing the group or revealing one's identity for any reason. Anonymous has conducted attacks against politicians, pedophiles, religious fanatics, companies, and governments. Anonymous selects its targets in retaliation of an organization or group's activity of which members disapprove. For instance, on March 20, 2014, an attacker invoking Anonymous support threatened Boston Children's Hospital in response to the diagnosis and treatment of a 15-year-old girl who had been removed from her parent's care by the Commonwealth of Massachusetts. In the following weeks, the hospital CIO, Dr. Daniel J. Nigrin, and incident response team, in collaboration with their IT team, was able to repel multiple attacks and prevent the compromise of patient data. Eventually, the hospital sought the help of third party security companies to assist in defense of their network.

Anonymous' attacks focused on the outward facing systems and the external website. Nigrin had his team create a plan in case all hospital systems "went dark." Eventually, the attacker threatened to target any organization affiliated with the hospital, including NStar, an energy provider to the hospital. In response, Nigrin turned off the external website and the organization email in case either had been compromised. The staff relied on an internal secure text messaging application for communication. Electronic health records were hosted on an internal system, so the hospital continued to operate. When the attack leaked to the press, other members of the Anonymous collective took to twitter to encourage their fellows to cease attacking a hospital. Eventually, the malicious traffic receded again.

Healthcare organizations are neither immune to DDoS attacks nor are they "out of bounds" to a deranged or profiteering attacker solely because the organization does good work. Hospitals and other healthcare providers should note which of their systems have an external connection and which systems depend upon that connection for operation. For instance, Nigrin commented that Boston Children's Hospital's EHR remained unmolested because it is hosted internally; meanwhile its e-prescribing system went down the second the external connection went down. Information security plans cannot be overemphasized to preclude panicked decisions. If protocol requires that external systems, email, or e-prescribing systems need to cease operation in the event of a cyber-attack, then the team needs to disconnect those systems post haste. Secure communications, such as teleconferences, rely on secure exchange of passcodes, especially when users know that the network might already be under attack. Finally, Nigrin recommends that employees be trained to report something if they see something. In the wake of the attacks against Boston Children's Hospital, some employees reported strange phone

calls from an unknown number. Correlation of reports like this can foreshadow attack campaigns before they develop in full-scale attacks.

Cyber Criminals:

Cybercriminals are the stereotypical attacker that targets an organization in order to make money through extortion or through the disclosure of compromised data. Cybercriminal groups range in size from one hacker to larger cyber-crime divisions of major criminal organizations. Known for their annual theft of billions of dollars from consumers and business each year, cyber criminals are the dominant category of hackers in the media. Like script kiddies and hacktivists, cybercriminals may purchase tools and attack kits from underground communities. Unlike the aforementioned groups, Cybercriminals also purchase, sell, and trade private information and intellectual property. Cybercriminals use DDoS attacks and ransomware malware to extort money from health organizations. Cybercriminals may also design and deploy custom malware against specific victims.

Ransomware, a form of malware designed to hold hostage data on infected systems until the owner pays the attacker a monetary reward, is touted to be the primary threat to organizations in 2016. Over the last three years, ransomware has evolved from a primitive malware type into an effective tool. Two common ransomware kits are Cryptolocker and Cryptowall. The malware works by encrypting victim files in a compromised system. If the victim does not pay the ransom within a fixed time frame or if the victim attempts to remove the malware, then the files may be removed or destroyed. Ransomware attacks have become so effective that the FBI has gone on record recommending that organizations just pay the ransom. When an attacker is paid, they may

release the file, they may destroy the files, or they may free the files for a limited period before re-ransoming the data.

The pattern of acquiescing to attacker demands ensures that ransomware will rapidly grow in popularity in 2016. As of 2015, the attack vector mostly targets Windows machines. In the near future, Mac, Linux, and Android variants will inevitably be developed. The health sector, who has already been targeted by ransomware attacks, will be at a heightened risk because any data system, any mission critical asset (MRI, EKG, etc.), and any mHealth device could be at risk of ransom demands. When lives are held ransom, how could a health organization refuse to pay the ransom? Cybercriminals are experimenting with how much victims are willing to pay for the safe release of their data. Through first-degree price discrimination, the attackers can target different markets with different rates.

Cyberterrorist:

Cyberterrorists target systems with the intent to disrupt or destroy a service that is critical to the activities of a target nation, sector, or organization. Cyberterrorists differ from cybercriminals in their cause. Terrorists act for the effect while criminals act for the reward. Cyberterrorists differ from hacktivists in their choice of target. Cyberterrorists target critical infrastructure while hacktivists target people and organizations. Critical infrastructure such as power, facilities, and transport networks are prime targets for cyber-terror campaigns. Of these, the power sector is particularly vulnerable because every other sector relies on the power sector for continued operations. Cyberterrorists act to cause an effect. This could be attacks on the healthcare sector to cause widespread panic or it could be attacks that frame a lesser hacking

group to stir political turmoil. Currently, the main cyberterrorist group is the cyber division of ISIS, Cyber Caliphate. ISIS recently announced the launch of a cyber help desk that helps recruits remain anonymous online. The help desk also teaches basic hacking and the use of tools. In this manner, strategic cyber targets can be delegated to script kiddie operatives as part of coordinated attacks.

Nation State Actors:

Nation State sponsored threat groups launch extensive cyberwarfare campaigns against systems belonging to foreign governments and organizations. Nation State groups entered the public spotlight in 2010 with Operation Aurora and the Stuxnet operations. State-sponsored Advanced Persistent Threat (APT) groups create and rely on advanced malware that is often customized to their target. APTs expend significant resources to discover and exploit previously undiscovered vulnerabilities (zero-day exploits) in target systems. Until zero-day exploits are discovered and exposed, the software developer remains ignorant of the security flaw and any system relying on that code remains vulnerable. Of the attacker categories, APTs leverage the most sophisticated attack and malware obfuscation techniques so that they can conduct the most effective and the longest running attacks. Their malware often incorporates rootkits for persistent presence, encryption to prevent reverse engineering, and code to mask the presence of malware from the system user.

Some state-sponsored groups seek intelligence useful in espionage operations, some collect intellectual property, and others aim to disrupt services. APT groups tend to be well funded; consequently, APTs generally do not conduct cyber campaigns (solely) for financial

gain. Personal identifiable information stolen by APTs is usually not collected to financially harm individuals. That is not to say that the information will not be exploited or sold on underground markets. By misusing PII, the adversary burdens the data owner and the United States government, who must investigate the breach and compensate civilians for the personal and fiscal harms of the compromise. The health sector, as a critical infrastructure sector, may be a target of APTs for the disruption of services or for the collection of PII.

Every year, the number of active APTs increases and so does the potential for cyber-physical warfare. Cyber-attacks that disrupt service can be combined with physical attacks to devastate a geopolitical enemy. To date, Russia is the only nation state who actively deployed a cyber-physical military strategy, in their 2008 conflict with Georgia. In the future healthcare organizations in areas of conflict may be at significant risk. Physical attacks against civilians are devastating, in part, because they tax the already strained resources of the defender. Conversely, physical attacks against medical facilities or personnel are not considerably effective. The attacker can cause considerably more damage by injuring civilians and enemy combatants, knowing that the enemy healthcare system will overload its resources trying to take care of the injured. The defending government will need to expend additional resources to support its healthcare system during the conflict. Essentially the attack strategy is the physical analog of a DDoS attack against the healthcare system. Now, if cyberattacks are incorporated into the strategy, then the attacker can significantly hamper critical healthcare assets such as payroll systems, health record databases, and software based medical equipment (MRIs, EKGs, etc.).

The Chinese nation state threat group dubbed Deep Panda, began attacking the healthcare, government, and energy sectors around 2012. In the United States health care sector, Deep Panda has attacked VAE, Anthem, Empire Blue Cross Blue Shield, and Premera. The

information stolen from the health care sector included social security numbers and other personal identifiable information or personal health information. Deep Panda also compromised systems belonging to OPM twice and exfiltrated the information provided on the SF-86 forms of 22.1 million current and former United States Federal employees. Additionally, the group got their hands on 5.6 million fingerprint files. Deep Panda allegedly conducted the attacks against the United States Office of Personnel Management, Anthem healthcare network, and Premera Blue Cross at the same time. Deep Panda is also believed to have attacked United Airlines shortly thereafter and may be behind attacks against American education institutions. The health, OPM, and travel records can be aggregated to catastrophically impact the United States government over time. Many believe that the stolen information could be used to create a database of US employees for espionage purposes. Conversely, the information may just be studied to discern operational patterns that the nation state actor could use to improve the critical infrastructure of their own government. China's initiative, Healthy China 2020, aims to provide universal health care coverage to all of China's 1.3 billion citizens. The initiative focuses on five target health sectors: health insurance, essential medicines, public hospital reform, primary care delivery, and public health services. Currently, China's lower and middle class are dissatisfied with the level of medical care. Medical costs are increasing while resources are shrinking. Anger has increased, violent demonstrations have occurred, and there have even been a few attacks against doctors and medical staff. This animosity places pressure on the administration to improve their healthcare system rapidly, through any means necessary. One of China's primary resources is a surplus of skilled and dedicated cyber professionals who are employed by the military as professional hackers. One could postulate that China might leverage the resource it has, hackers, to obtain the resources that it needs, healthcare sector operational strategies and

intellectual property. This would lead to an increase in the number of cyber-attacks in the years leading up to 2020.

Alternate reports suggest that Deep Panda may be a cybercriminal group. In early December 2015, China announced that it apprehended the hackers behind the OPM breach. Many online speculate that the arrests are an empty attempt to show America that China is upholding its end of the cyber-treaty between the two nation states. Some online doubt whether the arrested group was behind the OPM breach and if they are even hackers.

Deep Panda shows its sophistication through its custom malware and its ability to maintain (and succeed) at multiple campaigns targeting United States critical infrastructure. Nevertheless, like most groups, it relies on the simple but effective social engineering attacks as its initial attack vector. Deep Panda conducts watering hole attacks, uses zero-day exploits, and launches spear phishing campaigns. Even against trained personnel, social engineering attacks are ridiculously effective. This is likely the result of the combination of ingrained behavior to open emails or visit common websites, and national ineffective cybersecurity training. The group also opportunistically adopted some of the exploits and tools from the Elderwood platform. Deep Panda relies on the Sakurel Trojan, the Hurix Trojan, and the Mivast backdoor in its attacks. Shared characteristics in the malware code suggest that Deep Panda developed all three. The malwares all utilize droppers that masquerade as installers for legitimate software applications such as Adobe Reader, Juniper VPN, and Microsoft ActiveX Control. Each malware is capable of opening a named pipe backdoor, each malware contains tools to collect and exfiltrate system data, each malware can execute arbitrary code, and each malware can create, modify, and delete registry keys. The malwares self-obfuscated as technology related applications such as media applications or VPN technologies. The malware groups establish persistent presence on the

system, deploy remote access Trojans (RATs) such as the Derusbi malware, and feature tools to record and seize user sessions. Tools such as PwDump and Scanline are included to steal user credentials, to allow the actor to escalate their privileges, to let the actor create unmonitored accounts, and to assist the attacker in lateral movements to systems across the network. These tools allow the attacker to transition from a third party network onto the target network. Symantec believes that all three malware belong to the same family and that they have been updated and differentially developed over time by the same team. The malware is usually signed by the DTOPTOOLZ Co. signature belonging to a Korean software company while their domains and C2 servers are often registered to Marvel comic book characters.

A Multipronged Approach to Meaningful Cybersecurity

People:

A comprehensive multilayer information security platform begins with a dedicated security team. Lack of a dedicated security team was one of the largest failings of the administration of OPM. Instead, OPM's systems were managed either by its IT team or at the division level with no central oversight. None of the employees possessed the security training necessary to recognize and respond to a cyber-attack. The security team will justify its budgetary burden through improved organizational security posture. While it is impractical to try to measure the number of prevented breaches, the increase in organizational efficiency can be measured easily. Rather than spreading the technical security of the organization across departments and divisions, the security team should centralize system security governance in a systems operation center (SOC). The SOC serves a central point to assess, monitor, and defend

the other enterprise systems. Organization wide applications, such as change management and access limitation applications can be managed through the SOC. The information security team will develop information security policies, implement the policies, and educate the other employees. The information security team is not the same as the Information Technology (IT) team. Though the two teams need to work in concert, the information security team focuses on protecting the organization, its employees, and its customers from harm. The team will assess compliance rates, monitor for insider threats, and develop new ways to more effectively train employees. The information security team will work to improve the security posture of the organization while the IT department maintains the organization systems according to the organization's mission. In the event of a breach, the two teams must collaborate to form a comprehensive picture of the events that occurred.

OPM was breached because one or both of its third party contractors were compromised. 22/47 systems on OPM's network were operated by contractors and were outside the control of OPM's staff. Eleven of these systems were mission critical, but the government could not immediately access them. OPM failed to inventory the servers, databases, or network devices on the network. As a result, and because they could not access nearly half of the systems on the network, the breach remained undetected for over a year. When the compromise was discovered, the impact was not immediately evident. The information security team would have negotiated governance agreements with third parties. The team would have also mapped the entire network and set policy for connecting unapproved devices. OPM, like many other government agencies focused on getting through regulatory audits. In the healthcare sector, it is probable that many organizations likewise focus on meeting the requirements set by HIPAA and its provisions. However, organizations should consider that often-regulatory requirements are minimum "check

box" items rather than comprehensive programs. The organization will be stronger and more profitable in the long term if it exceeds regulatory security requirements.

Patients are the lifeblood of the healthcare sector. From the bottom, patient patronage at healthcare providers and insurance companies supports higher-level healthcare organizations such as healthcare security companies, mHealth developers, and technology firms. For the most part, patients visit the healthcare sector when something is wrong. Consequently, the modern construction of privacy policies centered on notice and choice are antiquated and inefficient. No one cares about how their birthdate will be stored in a database when they are in the middle of a heart attack. Just like those whose information was stored in the OPM database, consumers in the healthcare sector have no real control over how their data is stored or used. Involving patients in the organization's cyber-security plan as an informed and responsible party is negligent. The onus of protecting patient data resides with the healthcare provider, its business partners, and its trusted third parties. When possible, the organization collecting data should minimize its collection to necessary fields. During a hospital visit at UPMC, a patient is repeatedly asked by multiple nurses to confirm their name and birthdate. The check keeps the patient cognizant and repeatedly confirms the patient's identity. The only problem is that multiple nurses need to see a copy of the patient data. Each nurse has the opportunity to absorb information that could be used for identity theft. During the risk analysis process, each employee who accesses the patient data must be treated as a data vessel. Organizations with more data vessels have proportionally larger potential attack surfaces. Patients and the organization can be better protected by only collecting necessary data and by only displaying data according to role. For instance, if insurance and billing information has already been collected, then that information can be omitted from the treatment forms used in internal operation. If only name, birth year, and medical history are

needed for treatment, then address, social security number, and other personal identifiable information can be omitted from treatment forms. Similarly, if medical professionals are only going to refer to patients as “Mr. / Ms. Last-Name”, then first names could be omitted to increase the privacy and anonymity of the patient as a factor of the k-anonymity index. The k-factor measures privacy as proportional to the smallest number of individuals identifiable with the same information. In this case, a patient would be masked within the subgroup of patients with the same last name.

Healthcare organizations are driven by their employees. Healthcare employees are the backbone of the healthcare industry. Unlike in other sectors, in many divisions of the healthcare sector, such as hospitals, the employees are the workforce, the critical resource, and the service provided. Healthcare employees are typically patients of the organization as well, so they bear all of the same risk as patients. Healthcare employees are the target victim pool of attack campaigns against the organization with the goal of financially benefiting from false tax returns. If their information is stolen, employees may also be the victims of identity theft or insurance fraud. As both the majority stakeholder in the organization and potential victim, employees have the most to lose in the event of a healthcare breach. A breach could cost them their job and it could result in compromise of their identity.

Though alternatives are possible, a healthcare breach is highly likely to begin with an attack campaign against employees. Security is only as strong as its weakest point because attackers tend to focus on the point of least resistance. Across all sectors, human beings remain the weakest link in the security system. OPM is believed to have been breached as the result of a third party contractor responding to a phishing email. Anthem, and Premera Blue Cross may have been likewise compromised as the result of a single employee clicking on a malicious link

or attachment in a single email. Phishing remains the easiest, cheapest, and most effective attack vector. Malicious actors have no incentive to hunt for vulnerable external systems or to leverage a zero-day exploit when all they need to do is a little research and send a clever email. Phishing emails are not a trivial threat. They are no longer the obvious "Nigerian Prince" scams of the 1990's. Modern phishing campaigns are complex and effective. The emails are made to appear legitimate by copying the format of an email obtained from another source such as a previous breach. It is sent from a sender address that closely resembles a legitimate sender. For instance, the attacker might change a .gov address to an .org address. In other cases, the entire email is sent from a false account, and the sender address is spoofed in transit to appear to be from a legitimate source. In this case, the victim will see no discernable difference in the legitimate sender address and that of the malicious sender. The content of the email is often relevant to the target. For healthcare employees, this could be company health insurance information or an email from the accounting department. More specific spear phishing campaigns target a narrower pool of victims. In some cases, the target might be only one employee of which the actor obtained information about in a previous breach. Spear phishing emails contain even more specific information, which dissuades target suspicion. These emails tend to appear to come from the target's manager or superior so that the target's paranoia is substituted for panic or eagerness to please. Even in security organizations, such as CERT, the click rate on phishing campaigns fluctuates around 30%. In most sectors, employees are trained during orientation to recognize threats like phishing. Employees need to be trained to recognize a malicious email but they also need to be trained to remain vigilant. Society trains computer users to open emails, to click on links, and to download attachments. Especially in the healthcare sector, where life or death may be on the line, vigilance is a major problem. Software solutions such as Intrusion Detection

Systems, Intrusion Prevention Systems, Firewalls, enterprise email filters, and network segmentation can help to mitigate the human tendency to fall prey to phishing. Anyone who ever hung up on a noisy telemarketer can also attest that phishing campaigns can also occur over the phone. Social media may also be a viable channel. The aforementioned technical controls do not protect against social engineering. In hospitals, where the environment may be fast paced, an attacker might call a department and try to trick a stressed employee into revealing their administrative credentials. If the attacker is clever enough and convincing enough in their delivery, then patient records could also be at risk. In the case of both instances of social engineering, employees need to know how to stop, breath, and think before responding to a suspicious request for information. Here the information security team is critical because they can train employees to retain their training.

Phishing emails can be recognized through a healthy dose of paranoia and some subtle tells. In the healthcare sector, one way to minimize the risk might be to limit who receives emails from the organization. Doctors might need email access whereas nurses might receive all of their instructions while at work. In any case, users should only open emails from sources from whom they expect to receive email. This means that a nurse should be suspicious if he receives an email from the Executive Chair. To assist in this control, management needs to adhere to the organizational command structure. If the Executive Chair really does need to contact that nurse, then she should contact his manager or administrator first. Phishing emails can often be recognized by their incorrect sender information. Further, emails written by foreign actors often contain erroneous sentence structure and misspelled words. Hovering the cursor over a link allows the user to see if a link in an email matches the displayed hypertext. Overall, the easiest solution is for employees to not click on links in emails and to not download attachments unless

they are certain of the sender. Suspicious emails should be reported to the information security team.

Every employee has a role in the security of the organization. Employees in the advertising department need to be trained for many of the same threats as the employees on the information security team. Healthcare employees already receive training according to their position and to HIPAA regulation. The information security team can develop or deploy training modules and regular refresher courses to this regime. The healthcare environment consists of doctors, nurses, support staff, and technical professionals of different educational backgrounds and different skill sets. In the healthcare sector more than anywhere else, an information security team needs to develop different training delivery media (seminar, video, activity, etc.) to support different types of thinkers. The team can also measure company susceptibility over time by conducting an in-house attack against the company. Employees who click on the link in the tester email may be referred for further training. Departments within the organization can be trained with a focus on their security and privacy responsibilities within the organization. Rob Bathurst recommends that, "At the IT level they need to know their specific role as the front line for how to implement and operationalize security development lifecycle and privacy by design. Sales and marketing needs to understand everything from cookie management basics and web/app design to enable security and privacy as well as the brand damage that could occur if the enterprise has an issue. At the executive / management level, they need to understand and be trained on their role in an incident as well as the core interplay of cyber risks into the enterprise risk picture. And finally any product/service team also needs to understand all aspects of these if the company also creates or is planning to create products/services that use technology." Healthcare employees are trained to secure patient data and to protect patient privacy. The information security team can

assist the organization by training employees to secure data and protect privacy on approved software and on mHealth devices as they are introduced to the organization. In addition to personnel training programs, monthly or quarterly industry specific cybersecurity newsletters can assist in keeping employees alert to emerging threats.

The executive management of the organization is the last human component of the organization. In addition to their specific roles, executives bear the risk and responsibility of patients and employees. If a breach occurs, the executive management is held accountable to its shareholders and the victims. Specific attacks such as spear phishing and privileged account compromises target those in roles of governance. One example of such an attack was the 2014 Sony email breach in which executive accounts were compromised and their correspondence was used to harm the reputation of the organization. Executives must be vigilant in their actions and in their communications. They need to fully support information security initiatives within the organization. If the boss does not follow policy, employees will be less compliant as well. The information security team should begin each initiative by obtaining the support of the board. For their part, managers need to remain aware of cybersecurity so that they can pass informed decisions down the organizational structure. In support of this objective, the Institute for Critical Infrastructure Technology aims to help responsible decision makers remain informed about sectoral cybersecurity trends and solutions.

Certain employees, such as executives and members of the information security team, might need accredited security certifications. Certifications do not guarantee acceptable security practices; rather they certify that members of the organization know what minimum security practices the organization must meet. Senior security managers and members of the information security team should hold a variety of security and privacy certifications (CISSP, CISM, etc.).

Healthcare professionals might be especially interested in obtaining Healthcare Information Security and Privacy Practitioner certification (HCISSP). Security professionals developing or applying software solutions should obtain a CSSLP certification. ICIT Fellows (ISC)2 and ISACA offer a number of certification programs across the spectrum of cyber-security roles. They also offer training exercises that teach executives and information security teams to think like attackers and to respond to breaches.

Organizational certifications tell the community that the organization can be trusted to handle information with certain values in mind. Individually certified employees can better manage and account for the employees under them who may not have as much training. In some cases, organizational certifications depend upon individual certifications. The organization needs to be careful to acquire and train new talent so that it remains certified and compliant if the certified personnel leaves the organization. The organization should regularly audit its certifications and its compliance with certification requirements. Policies requiring third party vendors to hold certifications can be one control to ensure that vendors' operations can be trusted. As part of its contract, the organization should require an audit of the vendor's certification compliance.

Finally, one of the reasons that the healthcare sector is extremely vulnerable is that it employs a startling small proportion of qualified cyber security professional compared to other industries. In many healthcare organizations, cybersecurity professionals require at least a bachelor degree and many require additional education or years of experience. In the healthcare sector, applicants must also have knowledge of accounting, HIPAA, HITECH, and PCI DSS. This increases the time and difficulty in finding qualified personnel. Organizations can

collaborate with institutions that have cyber security programs to ensure that knowledge pertinent to the healthcare sector is taught to new students prior to graduation.

Policies & Procedures:

The first step in developing a multilayer security platform is for the information security team to conduct a risk assessment. Identify what assets are essential to operation and identify what assets are core to the organization's mission. Those assets are of the most value and need protection according to their value. These are not necessarily the assets that would have the largest immediate impact if stolen. In a healthcare organization, employee and patient databases would be the former category while organization financial account information might be the latter category. The distinction is that without employees, the organization could not operate and without securing patient information, the organization would violate its mission statement. Insurance would cover the financial accounts if they could not be recovered prior to exploitation. 45 CFR 164.308(a) (1) already requires organizations to conduct a HIPAA risk assessment. The information security team could improve the security of the organization by conducting yearly audits of the security program, governance of the program, and information security policy compliance. After assets are identified, the security team should build a set of scenarios (we are hacked, patient data is compromised, etc.) and use the scenarios to construct a risk profile. The scenarios should incorporate data from past incidents and industry data as its foundation. The profile will help to prioritize technology solutions and it will quantitatively fiscally justify the security program in the budget.

Industry leaders often have difficulty finding value in information security investments because they believe that the expenditure does not generate a return on investment. In the 2013 Target breach, Target upper management declined a $10 million investment to secure a $1

million system. The breach resulted in over $1 Billion in lost sales. Company leaders and the internal security team all left the organization. Target's reputation suffered while its competitors became more profitable. A dedicated and qualified information security team is responsible for providing the insight necessary to correct catastrophic assumptions. Information security budgets are best analyzed according to the net present value of the system, not the return on investment. Net present value can be determined by comparing the posture of the company with the posture of the organization after a hypothetical breach. If the net present value is greater than zero (and sometimes even if it is negative) then upper management should approve the expenditure. Poor investments or lackluster security assets can sabotage an organization's cybersecurity posture. Through thoughtful quantitative analysis, the Information Security Team and industry security leaders can construct a plan for future security investments. Strategic planning by knowledgeable minds can preclude the organization from potentially wasting millions of dollars on ineffective security platforms.

The organization should audit its security posture to identify where it is most vulnerable and to identify what security technologies it should adopt first. The audit should consider how well systems are maintained, how compatible the systems are with newer systems, and how frequently patches are administered. The audit should also consider regulatory requirements and legal obligations. The information security team should assess systems for compromise on a bi-annual basis. In a compromise assessment, a specific system is treated as compromised until the information security team can assess that the system can be trusted with at least 95% confidence. The team, or outside consultants, should conduct penetration tests against the organization's network and against its systems at quarterly intervals. Finally, at the end of the year, the information security team should review the network architecture prior to requesting the budget

for the following year. The budget request should not be a competition between the executives and the information security team. Instead, budget requests should be a collaborative effort to grow the organization, to secure the critical assets, and to adhere to the Company's mission.

The information security team needs to draft clear and concise policies according to the organizational structure and subject to approval by the executive board. Policies increase information security awareness. When information security policy is properly implemented, employees become invested in the security of the organization. A governance policy sets policy compliance requirements, policy adherence metrics, and policy enforcement measures. Next, a roles and responsibilities policy is needed to define employee access to information and employee accountability. Roles and Responsibility policies clarify the organizational structure and improve internal operating efficiency. OPM systems were compromised using stolen user credentials. All system access should be limited according to least privilege access. In essence, users should only be able access information according to their needs. Notably, this does not mean that users should have access according to their rank or job. A doctor needs access to his patient records, not the records of the entire hospital. Because administrative accounts are associated with the greatest risk, the roles and responsibilities policy should limit privileged accounts by number and according to function. Administrators should only use privileged accounts when necessary, deferring to standard user accounts for other tasks.

Access to systems is controlled through authentication and identification. None of the OPM systems required multi-factor authentication or identified the user. OPM, Anthem, and Premera were compromised with stolen credentials alone. Patients need to be taught to create unique and robust user credentials. A password policy can assist in governing user accounts. Credentials must be unique to the system. Passwords should not contain personal information.

Personal information is memorable; however, personal information is often the target of attackers and it does not change over time. This means that once personal information is compromised, it can be used to compromise a user's accounts or sold to another attacker, until the user no longer relies upon personal information to secure their cyber-identity. Security questions should not relate to public information such as "where were you born?" or "what is your mother's maiden name?" With the advent of social media, many of the answers to those security questions can be found online. Security questions exist for account recovery purposes and there is no penalty if they are not registered with honest responses. Their single purpose is to help authenticate a user who has forgotten their password or had their account stolen. Users can make up the responses so long as they remember from where they drew information. Security questions should instead focus on information that a specific person knows. For example, a healthcare site security question might ask, "What song is your guilty pleasure?" Sites can increase security even further by allowing the user to input their own security question and response and then redisplaying the question to the user at login as a secondary check, in the same fashion that banking sites use for "security phrases".

A complex password consists of at least 15 characters consisting of upper and lowercase letters, numbers, and special characters. Users should utilize a different username and password combination for each account on each website. Users should change their passwords every three months and they should enable multi-factor authentication where possible. Most users, including many in the cyber-security fields, ignore these best practices because in the real world, it is difficult to remember all of the different accounts that a user owns, let alone a different 15 character complex password for each account. The majority of users believe that their accounts are not worth compromising, so they fall complacent in shoddy cyber-security and they reuse a

set or a few sets of credentials. Other users store their credentials on their devices or they employ password managers. Some users record their login credentials on paper or in their mobile device. Only a very, very small portion of users adheres to ideal cyber-security practices. As a result, public and private organizations are regularly breached through compromised credentials.

Users can make easy to remember complex passwords using information that they know or information that can access instead of information relating to their personal identity. Often, users find one "really good" password to which they grow attached and either never change or reuse on other accounts. Vigilant users must resist that temptation. Rather than grow attached to a particular password, focus your mind's sentiment towards developing and adopting a unique password generation schema that will assist you in rapidly and in repeatedly creating new memorable passwords. One such schema would be to open a book on your desk or mobile device and either remember or record the page number on a post-it. Take the first sentence and develop a pattern. For instance, one could take the first letter of each word in a sentence, alternate the capitalization, and end the password with a special character and the number of words. Song lyrics (as you remember them), children's' rhymes, or other seed data could likewise be used to create robust passwords. Users who wish to forgo schema creation should develop their own method for complex password creation and retention. Apathy is no excuse for lackluster security because a single compromised account can affect millions of other people. Users who wish to randomly generate passwords or use complex passwords that are difficult to remember can split the password and record the halves on two separate mediums, such as half on paper and half in a mobile device. News of recent breaches indicates that password managers or password vaults are often not as secure as advertised. This is in part because these applications are single points of failure which draw the attention of attackers because compromising the single application

directly leads to stolen credentials which aid in a number of other avenues of attack. Users should only resort to reliance on these applications when all other methods fail.

In a healthcare environment, where time is critical, employees may not have the time to enter robust passwords. In that case, multi-factor authentication can be accomplished through a combination of tokens and biometrics. Tokens are something that the user possesses, while biometrics information is about the identity of the user. Token such as keycards or encrypted RFID chips provide fast access and are safe if correctly managed. However, a token can be lost or stolen. Policy makers must account for this eventuality. The best solution is to combine the token with an extra layer of either passwords or biometrics. Biometrics algorithms uniquely identify users according to their genetic traits. Interestingly enough, implementing biometrics in a hospital environment is uniquely complex. Fingerprint scanners cannot be used because most employees wear gloves. Facial recognition is inefficient because some employees wear masks. Dr. Marios Savvides of the CyLab Biometrics Center of Carnegie Mellon University is developing a facial recognition system that might be viable in the healthcare sector because it recognizes subjects based on the shape, spacing, and size of their eyes. If no biometric can be developed for operation in a healthcare environment, then the information security team might suggest a mobile authentication solution. Most United States citizens own a cell phone. Mobile authentication is a token based system based on a certificate downloaded to employees phones. Unlike keycards or small tokens, employees are likely to immediately notice if their phone is lost or stolen. The missing device can be immediately tracked or it can be remotely wiped.

Mobile devices introduce new threat vectors to the organization. Employees and patients expand the attack surface by connecting smartphones, tablets, and computers to the network. Healthcare organizations can address the pervasiveness of mobile devices through an Acceptable

Use policy and a Bring-Your-Own-Device policy. Acceptable Use policies govern what data can be accessed on what devices. BYOD policies benefit healthcare organizations by decreasing the cost of infrastructure and by increasing employee productivity. Mobile devices can be corrupted, lost, or stolen. The BYOD policy should address how the information security team will mitigate the risk of compromised devices. One solution is to install software to remotely wipe devices upon command or if they do not reconnect to the network after a fixed period. Another solution is to have mobile devices connect from a secured virtual private network to a virtual environment. The virtual machine should have data loss prevention software that restricts whether data can be accessed or transferred out of the environment.

Finally, the organization should have an incident response policy that assigns roles and procedural action plans in the event of a cybersecurity incident. Formulating a plan ahead of time prevents decision making under stress. OPM lacked an incident response plan. When their system was breached, the impact of the incident was not minimized. Forensic evidence was not preserved. As a result, when the incident was investigated, the administration could not report to Congress when the systems were breached, how the attackers behaved, or what data was stolen.

Technical Controls:

When security solutions fail, and an attacker breaches a system, they need time to adjust to their environment. The process is reminiscent of a burglar breaking into a home. When the burglar breaks into a home, it must quietly and cautiously move through a dark and unknown environment if it wants to avoid detection, ejection from the home, and criminal charges. More time is required if the burglar encounters further security measures or locked doors inside the

house. Similarly, the adversary needs to map the system that they are on and to analyze its resources. If the infected system is not the target system, then the adversary needs time to map the network, to determine which system it needs to infect, and to figure out how to move to that system. This process is complicated by the necessity that the adversary move slowly and carefully through the compromised network to avoid detection. The impact of a breach is proportional to the amount of time that an adversary can remain undetected in the compromised system. The OPM, Anthem, and Premera breaches all lasted for extended periods (often more than a year) before anyone noticed.

Before replacing systems or investing in new systems, the organization should purchase and deploy a monitoring system. Monitoring systems, such as log monitoring systems, IDS, and IPS, can detect suspicious activity on legacy and modern systems. Intrusion Detection Systems and Intrusion Prevention Systems can help the information security team detect a threat before it becomes a breach. Computers are built from a technology and architecture that is inherently insecure. No level of added security is a solution; at best, it is an engineering hurdle. It lasts until the attacker figures out a way around it. Overall, monitoring systems reduce attacker dwell time. Alternately, the security team can use the monitoring information to determine if attackers already compromised the network before spending their budget on proactive systems. Instead, reactive systems or measures can be implemented to halt the actor early in their attack cycle. The information security team can also measure whether new solutions are effective. This outer layer helps demonstrate measurable value ahead of modernization or improvement projects, which could take years to deploy fully.

Healthcare networks are complex and dynamic because they need to protect highly sensitive data while remaining accessible to a large employee base who have varying levels of

cybersecurity awareness. Healthcare networks need to be Secure, Open, Flexible, and Available (SOFA). The application of technical controls, physical controls, administrative controls, and software solutions can protect the network. A network firewall can protect the perimeter from inbound malicious traffic. The public network (for patients) should be protected by a firewall that is periodically updated to block malware based on identifiable signatures. The employee network should be protected by a more comprehensive firewall that uses signatures and a whitelist to permit or deny traffic. All unnecessary ports and protocols should be blocked on both networks. Physical access to ports should likewise be blocked or restricted. This can be managed through an active directory system or through a "low-tech solution" such as damaging or removing the ports. SSH and Telnet access should be disabled by default on all devices. Reverse proxies can be used to prevent DDoS attacks by distributing network traffic across multiple servers. Routers and switches can be used to filter DDoS attacks that rely on packets with the same source and destination addresses. These devices also serve as the first authentication point for user access. Application traffic can be restricted through rules curated by the information security and IT teams.

All network activity should be logged at a central location. These logs will support User Behavior Analytics (UBA) systems, dynamic antimalware systems, and the System Enterprise Incident Management system (SEIM). The log server should be backed up regularly on a redundant server. Traffic can be directed into a demilitarized zone (DMZ) where it can be analyzed by IDS and IPS and then directed along specified network segments. Traffic can also be forced to pass through a HTTP proxy to prevent malicious websites from delivering malware directly onto host systems. The network should be segmented according to function, access privileges, and need. Employee traffic, patient traffic, and critical asset access should each reside

on a different subnet. Remote access to the network should be highly restricted or blocked entirely. Virtual jump boxes that institute an additional authentication control should stand between the network and critical systems that require remote access. Access of mobile devices belonging to employees, belonging to patients, or generated from mHealth devices can be controlled at the VLAN layer during segmentation. It is recommended that the fax and print servers either be delegated to a dedicated network segment or only be connected to select trusted systems. DHCP servers will issue valid IP addresses to devices connected to the network and subnetworks so that attackers have a more difficult time masking their presence by spoofing an IP address. Patch and update servers maintain organization systems according to group policies (ACLs). End-to-end encrypted virtual private networks can protect data while in transit. Backup servers provide redundancy and fault tolerance in case the network is compromised. The information security team should monitor the organization's cybersecurity posture from the security operations center (SOC) while the IT team maintains the network operations center (NOC). The NOC and the SOC must work together. Finally, access to restricted areas and or company devices should be restricted by multifactor authentication wherever possible.

Rick Caccia remarks, "Unusual behavior is always in the system logs. If you detect it early, you can prevent or minimize damage. To me, an obvious lesson is that effective monitoring and analysis technology are table stakes. If you can't detect and assess risky behavior, you are going to lose data." A User Behavioral Analytics (UBA) system, such as those developed by ICIT fellows Securonix and Exabeam, monitors system users for suspicious activity. OPM could have benefitted most from a User Behavioral Analytics (UBA) system. UBAs monitor user activity over a predetermined period and create a profile baseline. Provided that user thresholds are established prior to a breach and that identity access controls prevent the

creation of unknown accounts, the system will detect and report anomalous user behavior such as log in attempts at strange hours, access to databases outside of job function, and other suspicious activity. Currently, phishing attacks are the easiest, the most prevalent, and the most successful attack vector. Phishing attacks can be used to pass malware from a trusted device onto the network, or they can be used to collect a user's credentials and pass them back to the bad actor. Once inside the network the users with valid credentials are considered "trusted." OPM, like many other organizations, had no idea that a normal legitimate user was acting in an anomalous and illegitimate way because it lacked a UBA system and an information security team. OPM also lacked monitoring tools, such as IPA, to detect a remote attacker controlling malware inside the network with legitimate login credentials.

UBA systems greatly enable an insider threat-monitoring program to detect threats within the organization. For instance, in a hospital, a UBA, paired with multifactor authentication measures, could be used to monitor whether a nurse was accessing drugs more frequently than required by her job. Further, UBA's can assist or serve as a data loss prevention program if configured to flag suspicious or large data transfers. Qualified information security personnel are required for effective deployment of behavioral analytic systems. While initially costly and resource intensive, the cost of UBA programs lessens after baseline establishment. UBA systems mitigate breach attempts from stolen credentials and insider threats. Behavioral analytic systems grant organizations the potential to process raw sensory data in near real time to act to mitigate active threats. Some systems can also fingerprint automated processes or machines to mitigate attacks from those vectors.

The information generated by the monitoring systems and UBA systems can be used for event correlation. In event correlation, aggregate microscopic details are used to piece together a

macroscopic picture. This process is similar to how forensic investigators use the details found a crime scene to piece together an idea of what happened. The primary difference is that an event correlation platform should inform the information security team of predictive trends before the organization suffers harm. Event correlation is specifically complicated in the healthcare sector. EHRs are shared across organizations to enhance research efforts and benefit patients; however, data sharing complicates behavioral monitoring by widening the scope of activity beyond the boundaries of the organization. Joint behavioral analytics systems across organizations and over information sharing channels could recapture the lost insight.

The HITECH Act, the HIPAA Security Rule, and the EHR Meaningful Use Incentive Program attempt to mitigate the risk to patients introduced by the adoption electronic health records by regulating healthcare providers to take minimal precautions to protect patient data. Similarly, the Omnibus Rule increases civil and criminal penalties for violating HIPAA regulations. None of the regulations comprehensively address the new environment. For instance, none of the regulations mentioned mandate that EHRs be encrypted while at rest, or in transit. The 80 million records stolen from Anthem and the 22.1 million records stolen from OPM were likewise unencrypted.

Contrary to media outcry, encryption would not have prevented the data from being stolen. Nevertheless, encryption could prevent the actor from using the data. If the encryption algorithm is adequately sophisticated, then either the actor would have to expend significant resources to decrypt the data or they would have to abandon the data and dedicate their resources elsewhere. If an actor begins exfiltrating data and is unable to use any of it, they may abandon the system mid-breach on the assumption that the stolen data will not be worth the further time and other resource dedication. Different field level encryption algorithms could be employed to

encrypt different fields according to their sensitivity. That way, even if the attacker manages to crack the private key for one field, the remainder of the data remains secure. Field level encryption would not definitively prevent attacks. If the actor predicted which field contained social security number, for instance, then they might be able to access the social security numbers of all of the patients in the stolen data; but they would not have the associated names, addresses, or other information unless all of those other fields were also decrypted. Different attacks require different amounts of data. Filing for a fake credit card requires a different amount of information than filing a false tax return or false medical claim. Organizations could encapsulate the data set in a second layer of encryption (using a different encryption algorithm) to protect extremely sensitive data. Encryption thereby, scales the benefits that an actor can realize to the time, dedicated personnel, and computing power available to their operation. Criminal operations would likely seek easier targets because they often do not have the resources to spare. For them, time is money and more money can be made from less secure targets. Nation state sponsored threat groups are generally less interested in financially exploiting breach victims than they are in compromising systems to steal national security information or intellectual property. In short, healthcare organizations should encrypt PII, PHI, and EHRs at rest and in transit. Ideally, the information would only be decrypted during processing. Encryption and decryption does require increased computing resources and may slow some database queries. One way that healthcare organizations can acquire the resources to invest in the necessary infrastructure would be to publicize the increased protection. The increase in reputational value should adequately account for the expenditure, especially if competitors decline to seize the same opportunity.

Secure mobile healthcare devices can be a considerable competitive advantage for hospitals and device manufacturers. Mobile healthcare devices and mHealth platforms, such as those developed by Phillips, stand to revolutionize the healthcare sector by making healthcare more accessible across the globe. Noninvasive devices can actively monitor symptoms and immediately administer treatments according to user needs. The PHI collected by mHealth platforms advances research to develop alternative medicines and treatments.

In "Geekonomics", David Rice recounts how the 1970's auto industry sold insecure models to consumers to generate greater profit. Risk of harm shifted from the manufacturer to the customers. As such, consumers were used as crash test dummies for insecure products. Rice accuses software manufacturers of using the client base in the same manner. In the healthcare sector, many mHealth devices are insecure at the expense of the user. According to some, the FDA is a "toothless dragon" because it fails to adequately regulate the market or punish manufacturers of devices that are flawed by accident or design. In a 2013 study sponsored by the Mayo Clinic, security researcher Billy Rios found roughly 300 vulnerable medical devices from 40 vendors. The insecure devices ranged from insulin pumps to defibrillators. Some devices can only be compromised physically, but others, especially those with an unencrypted Bluetooth connection, can be accessed from any internet connection. Healthcare organizations need to demand mHealth security from manufacturers. Some, such as Phillips have already launched mHealth security platforms. These companies have a long-term competitive advantage above other manufacturers. In the manufacturing sector, Alcoa's Paul O'Neill demonstrated that a focus on the safety and security of employees and customers not only generated significant returns on investment, it generated lasting brand value. Hospitals, patients, and employees deserve mobile healthcare technology that they can stake their lives on.

Healthcare in the Digital Age:

The Internet of Things:

The internet of things is the throng of non-computer and non-phone devices that are connected to each other and the internet through embedded electronics, software, and sensors. In practice, the internet of things is mostly about the quality, quantity, and type of sensors embedded into devices. In theory, each object collects and exchanges data in order to improve the experience of the user. In the healthcare sector, the internet of things will increase access to diagnostic testing, comprehensive treatment, and preventative care.

Business strategy theory uses the term "Red Ocean" to describe a market segment that is heavily contested by established incumbents (i.e. there is blood in the water from fighting sharks). Barriers to entry are significant. The returns to stakeholders are relatively static. Because the market boundaries are well defined, there is little innovation or growth compared to more dynamic markets. In contrast, a "Blue Ocean" is a market that is untapped because established sector leaders do not yet realize the market potential enough to warrant significant competition. According to a 2015 MarketResearch.com report, the healthcare segment of the Internet of things is poised to grow to $117 billion by 2020. Goldman Sachs estimates that the internet of things technology can save patients, providers, and payers billions of dollars for asthma care alone.

In the healthcare sector, the internet of things can be segmented into discrete technologies. Affordable and effective implementations of sensors in healthcare operations and systems will improve efficiency and accountability. Telehealth solutions will provide unprecedented levels of patient care to overpopulated areas and areas unaccustomed to regular healthcare. Embedded medical devices can save lives by automatically delivering medication and

monitoring patient symptoms. Behavioral adjustment devices enable users to take a proactive interest in their health. Cloud technologies streamline healthcare processes and may serve as a convenient platform for information sharing between stakeholders. Finally, mobile devices and applications increase the accessibility and ubiquity of mHealth solutions.

A marriage of critical infrastructure with the internet of things should not be undertaken until the information security team and the IT department performs risk analysis and a detailed adoption and deployment plan for each technology. Merging a network onto the internet of things also means expanding the cyber-attack surface of the organization in ways that could allow any petty bad guy to hack any device on the network from the other side of the planet. Some applications, such as the cloud, may be piloted in low risk segments of the hospital network before commitment to the solution. Unbeknownst to hospital personnel, many devices in operation are already internet enabled despite the lack of risk analysis. Old systems may have unnecessary ports or connections (such as telnet or USB) that are not disabled. Newer devices may also have insecure Bluetooth or Wi-Fi connections. For many IOT devices, such as mobile sensors, mobile devices, etc., the attackers can purchase a unit to practice on for a low sum relative to the financial gain that they will receive should they successfully breach a single system. Other devices, such as MRI machines may be too large or too expensive to purchase and practice on; however, the attacker may be able to study the underlying software if it was developed in an open source environment or if the source code is available on the deep net. Since many healthcare providers rely on the same or similar technologies, once an attacker compromises one network, it will be trivial to compromise others in the sector. This aspect of the industry is particularly troubling because unlike in other critical infrastructure, such as the

financial sector, the healthcare sector does not openly warn other stakeholders of vulnerabilities or adversaries.

The best mitigation strategy to ensure trust in a network connected to the internet of things, and to mitigate future cyber events in general, begins with knowing what devices are connected to the network, why those devices are connected to the network, and how those devices are individually configured. Otherwise, attackers can conduct old and innovative attacks without the organization's knowledge by compromising that one insecure system. Most major breaches, such as OPM, Anthem, and Premera, succeeded because the attackers knew more about the organization's network than the people paid to protect it did. If a cyber network is a castle, then every insecure device with a connection to the internet is a secret passage that the adversary can exploit to infiltrate the network. Security systems are reactive. They have to know about something before they can recognize it. Modern systems already have difficulty preventing intrusion by slight variations of known malware. Most commercial security solutions such as firewalls, IDS/ IPS, and behavioral analytic systems function by monitoring where the attacker could attack the network and protecting those weakened points. The tools cannot protect systems that IT and the information security team are not aware exist.

People fear the unknown because invisible, unanticipated attacks are the most devastating. Behavioral monitoring depends on the adversary leaving a trail of suspicious activity. Similarly, incident response plans tend to respond to the adversary's movement through the network. Neither system nor any aforementioned tool responds to an attacker who compromises one unreported internet of things system and never moves further into the network. Attacks of this variety are uncommon, but not nonexistent. Typically, they are conducted to subtly or visibly disrupt operations. For instance, the Stuxnet attacks targeted air-gapped

centrifuges through the USB ports of computers that were not connected to the internet. The attacker may have loaded the malware by dropping infected USB devices in the facility parking lot and letting personnel infect their own systems by checking the devices in the target computers. The malware caused the centrifuges to spin slightly faster than they should have while the computer program measuring centripetal force remained ignorant to the change in rotational velocity. As a result, researchers were unaware of the attack for a considerable period of time, nearly one fifth of the centrifuges in Iran's nuclear program had to be replaced, and years of scientific research had to be scrapped. In a healthcare environment, these cyber-physical man-in-the-middle attacks could cause major consequences. In some cases, the outcome could be immediately obvious, for example if an automated surgical tool made a 1-inch incision instead of a 1 cm incision or if a medical delivery system expelled its provisions significantly faster than expected. In other cases, the long-term impact of slower attacks may be much greater. Imagine the outcomes of a device that misrepresents the amount of radiation delivered to patients. Neither the patient nor the technician may ever notice the attack.

Organizations need to be concerned about software integrity. Technical controls and policy should govern the change management of systems so that any the information security team can detect when malware compromises a system and alters minute details such as operation instructions. Developers should produce code with a security by design structure instead of implementing security as an afterthought. Given that the majority of breaches (OPM, Anthem, Premera, Target, etc.) occur due to third party negligence, it behooves software and device developers to ensure that security and privacy protections are implemented in their products throughout the development cycle. The healthcare sector should hold these parties accountable through their third party agreements. The integrity of a device or application is not certain.

Something could be compromised an hour after it is checked. The manufacturer cannot prevent the installer or an inside threat from impregnating the device with malware after it has shipped. The device could be also be intercepted mid-transit by attackers so that they can install a backdoor in the software. ICIT fellow Phillips Healthcare conducts regular penetration tests on its medical devices. We suggest that other organizations follow their lead. The healthcare information security team and developers should conduct annual penetration testing on products before trusting the system.

Despite organizations efforts, the cyber-attack surface surrounding the healthcare sector will increase with the internet of things and with mobile technologies. Network defenders are forced into an asymmetric relationship with attackers who are much more knowledgeable. The greatest vulnerability in the organization is the lack of understanding of the actor's means, motive, and opportunity. The information security team needs to know what attackers are capable of attacking, how they could attack, and what is valuable. They need to know how an attacker could operate before they can fortify the network to preempt the attack. If you know an intruder can enter your house through the front door, you lock your door. This does not necessarily mean putting bars on everything. You are just adding layers of control over the threat model. You look at where attackers could enter and build concentric circles of defenses. Oppositely, you could work outwards from an asset. Every IOT system should be assumed insecure until proven otherwise to a reasonable degree of trust.

Sensors:

Sensors are small devices that enable data to be collected and communicated at relatively low costs. Moreover, The Globe and Mail estimates that the average price of traditional sensors, such as radio frequency identification (RFID) chips will drop from $0.50 to $0.38 by 2020. Sensors can be used in innumerable applications, limited only by the user's imagination. General Electric is building an autonomous factory that subsidizes the majority of labor costs by replacing personnel with sensors. Cloud based company Temboo, produced a video entitled "Aging in Place and the Internet of Things" which shows how to integrate sensors into medical devices in order to monitor an independent retiree who lives alone. Their design seamlessly incorporates a microphone, motion sensors and other basic sensors into a living space. Collected information can be streamed to a mobile phone through email or text messages, or the subject's activity can be logged in a Microsoft Power BI database. If something were to go wrong, such as extended periods of inactivity, sudden motion, or suspicious behavior, then SMS messages can notify family members or emergency services.

Hospitals can use RFID chips to increase accountability and efficiency. Patients can be tracked through RFID equipped wristbands, similar to those currently used at Disneyland. The patient's treatment and test information can be stored on the wristband so that the patient receives consistent and timely treatment even when treated by different doctors and nurses over the course of their visit. RFID wristbands minimize the time spent recounting test results or asking redundant questions. Consequently, greater time is allocated to patient care than to paperwork. The hospital benefits from the increased productivity of its personnel. The hospital can aggregate the data from the active wristbands to dynamically optimize the schedule of tests

and resource allocation to ensure that patients receive the right amount of access to the right equipment at the right time.

The information collected by the RFID bands provides a higher level of intelligence about the operational efficiency of the facility. The data can be used to improve the flow of patients through the hospital or to optimize the impact of nurses and doctors. The data can also be used for predictive analysis to discern patterns and anticipate changes in the hospital environment. If for instance, a number of patients with similar symptoms seek treatment at the same facility, then the already digitized RFID data should be able to predict the trend faster than would inputting each patient's symptoms into the computer database. On a greater scale, if healthcare providers share anonymous or pseudo-anonymous information through a cloud, then multiple local facilities can aggregate their data to identify local trends. The hospitals could potentially stymie the potential outbreak of an infectious virus before it spread or they could order more medication in anticipation of an influx of patients.

Hospitals tend to overstock certain medication to prevent running out during an emergency. RFID sensors can provide an accurate inventory of supplies at a moment's notice to improve the hospital's resource management. RFID sensors can improve drug supply management. Medication containers can be fitted with RFID tags. This adds confidence that the drug is real and it can identify the owner. Further, the tags can monitor the expiration date of batches of medication. In the event that expired or mis-produced medication is distributed to patients, the hospital can check the database logs to see how the medication moved throughout the facility. In short, sensors can be applied to physical health records or medication to prevent breaches of confidentiality or data integrity. The RFID sensor can be a form of authentication, so that concurrent RFID monitoring of personnel, patients, tangible files, medication and equipment

ensures a comprehensive accountability model that can be governed with comprehensive policies.

Healthcare technology developers can use sensors in place of invasive procedures or cumbersome technology. Chaotic Moon Studios developed circuit board temporary tattoos based on conductive inks that sit on the surface of the skin. They allow for medical monitoring of heart rate, blood pressure, and other vitals. These sensors can be wirelessly monitored through a smartphone app as patients go about their normal daily activities. The sensors supersede invasive chest cathodes and arm monitors. The temporary tattoos can also be used as surgical reference marks for aligning and calibrating treatment machines to increase treatment consistency. WuXi PharmaTech and TruTag Technologies are developing smart medication that helps monitor medication regiments and health. These smart pills can help drug companies and healthcare providers collect data about patient response to medication and can mitigate risk in procedures. Through sensor-based solutions, such as smart medications, technology developers can effectively miniaturize medical equipment and simplify complex procedures that were previously outside the budget or expertise of smaller healthcare institutions. Patients will have access to effective healthcare solutions from a greater number of locations. As a result, the quality of medical care in the United States will improve. Moreover, since a majority of the administration and monitoring can be done in smaller facilities and in the cloud respectively, healthcare networks will benefit from decreased costs and decreased patient congestion at larger healthcare facilities.

Sensors solutions are not holistic solutions. The RFID chips need to be secured with strong encryption to prevent an attacker from reading or altering the information from within the facility. The information security team needs to maintain a record of every sensor in circulation

so that no malicious sensors are placed on the network. Finally, the RFID may interact with some medical tests; consequently, the patient RFID bracelets will need to be removable for those tests, but otherwise difficult to remove to prevent a malicious actor from commandeering someone else's bracelet. All RFID tags will need to be wiped either after a set period of time or by a sensor at the exit.

Telehealth:

The Center for Connected Health Policy defines telehealth as "a collection of means or methods for enhancing healthcare public health, and health education delivery and support using telecommunication technologies." Telehealth is the practice of delivering healthcare through a remote telecommunication platform, such as mobile phone, video conferencing, or email. Telehealth covers a broad range of fields and applications such as: dentistry, counselling and mental health, physical and occupational therapy, healthcare for homebound patients, monitoring and management of chronic diseases, disaster management, and consumer and professional management to name a few. Telehealth could be as simple as a WebMD style platform that is actually supported by practicing doctors. It could take the form of video conferencing between a patient and their doctor or specialist. Telehealth could just be a platform for securely transferring ePHI in the form of X-rays, videos, or documents between patients and medical professionals over secure email, over a secure mobile application, or securely over a cloud network.

Telehealth is emerging at the behest of millennials that spurn the long wait times and inadequate care attributed to what they see as a bloated healthcare system. Millennials do not tolerate poor service and opaque transactions. They will not pay high healthcare costs for

diminished services. The patient engagement model needs to change to accommodate the new generation; otherwise, they will either seek treatment at local quick stop clinics or try to self-diagnose through services like WebMD. The national standard of healthcare will erode in a few years. Telehealth is a consumer centric solution that improves the user experience while simultaneously cutting operating costs for healthcare organizations. Basically, it satisfies millennials expectations while adhering to the realistic capabilities and resources of the healthcare sector. In June 2015, Goldman Sachs predicted that connected devices and IOT solutions could potentially save $300 billion in annual costs to the United States healthcare sector, mostly through telehealth and remote patient monitoring. Goldman Sachs predicts that telehealth can save healthcare providers and payers over $100 billion annually. The mostly untouched "Blue Ocean" market around telehealth solutions is estimated at $12 billion annually.

In the first half of 2015, 136 new companies raised $2 million or more to enter the market. Recently, telehealth company Teladoc filed for an IPO based on its subscriber base for on-demand video, mobile, and phone consultation services. Teladoc saw its subscriber base jump 100% to 8 million in less than a year. Theranos, a digital health start up is disrupting the lab test market with inexpensive direct-to-consumer lab tests that bypass physicians. Large corporations, such as Virgin Pulse, are developing devices for employer sponsored health programs because employers are having a hard time keeping up with healthcare costs and insurance premiums. Employee health and wellness programs promote healthy lifestyles that keep employees out of the hospital and doctor's office. Theranos, Teledoc, and Virgin Pulse are luring patients away from healthcare providers by offering digital platforms that are cheaper, more accessible and more secure.

Telehealth solutions expand patients' healthcare options beyond their local area. Patients do not need to schedule an appointment weeks or months in advance when they can seek medical attention from home. Little or no time is spent in the waiting room. Patients with sensitive or embarrassing conditions such as rashes or mental health issues can seek professional help without the shame of scheduling a medical visit. Because patients do not have to plan the day around their medical appointment, patients will not need to take time away from their jobs as frequently. Patients, who cannot leave home due to medical conditions, lack of transportation, or lack of a babysitter, are able to receive medical advice and treatment more frequently.

Patients in rural and remote communities benefit most from telehealth solutions. Rural hospitals often lack specialists, imaging equipment, and diagnostic centers. Consequently, rural patients often must schedule a second appointment at a larger hospital after seeing their local primary care physician. For many whom already have difficulty finding the time to attend to their health or the money to pay for healthcare, the secondary appointment is an excessive burden. The trend may be one reason that rural citizens do not use the healthcare system as extensively as city dwellers. In addition to the aforementioned telehealth applications, mobile imaging centers and travelling lab specimen kiosks can collect samples and conduct basic imaging and diagnostic tests. Results that are not immediately available can be distributed through secure email or web based applications to rural doctors or in some cases, directly to patients. Telehealth can decrease emergency room and open clinic wait times and expenditures by decreasing the traffic of patients with non-serious conditions. Finally, one interesting application of telehealth specific to rural citizens is the concept of patient peer groups. Sometimes for support and advice, a patient really needs to converse with a groups of other people who have also suffered from the same condition. Depending on the condition, in less

populated rural areas, there may not be a community of peers. Further, in either rural or metropolitan areas, patients may be less willing to attend a support group if there is a chance that other members could recognize them outside of the group setting. Telehealth based community solutions, such as PatientsLikeMe.com, exist to connect patients across a geographic region or over the internet. These platforms are often available at little or no cost to the patient, who can access the application from their mobile phone or computer.

An account on a trusted telehealth platform costs physicians $30 - $50 per month and costs patients nothing. Healthcare providers can cut the overhead costs associated with their practice (office space, secretaries, and magazine subscriptions). Patients interact with fewer personnel. This, combined with a decrease in the amount of customary idle chatter, means that medical personnel can help more patients in a given amount of time. The emergence of telehealth solutions means that medical educators must teach future physicians how to effectively use telehealth to ensure that patients receive the proper quality of care. Accordingly, twenty new institutions recently joined American Medical Association's effort to bring medical education into the 21st century through efforts that include advanced simulation and telemedicine solutions. New preparation methods might include roleplaying practice remote evaluations and by roleplaying difficult discussions.

Telehealth solutions also connect doctors with patients in developing countries. Organizations, like the Population Council, that conduct meaningful medical research for the benefit of human beings, can rely on telehealth solutions because telehealth capable devices are relatively inexpensive in comparison to the opportunities gained and the logistical costs avoided. Telehealth can be used to treat individuals through the digital transmission of images, the sound of coughs, or scans from portable devices. Data about entire groups of people in a region can

help organizations like the Population Council to track epidemics, to develop better treatments and to create cures for populations in need.

In the face of concerns of theft or violence, some organizations might be wary of investing in medical equipment or computer technology to send to developing countries. Rather than embrace fear, these organizations should emulate the non-profit group One Laptop per Child. In order to mitigate violence and theft of the educational laptops sent to developing communities, the non-profit designed their laptops to look and feel like a child's toy. Besides the distinguished appearance of the computer, the tactile feel of rugged plastic instead of slick metal was enough to prevent adults from taking the units from children who were trying to learn. OLPC's design decision had the added benefit that the laptops were cheaper to make and more durable. Telehealth developers would do well to design their units to be recognizable and to appear in such a way that quells potential vandal's desire to tamper with the unit.

Telehealth solutions need to be secure enough to ensure the confidentiality, integrity, and availability of data where data is stored, processed and when it is in transit and they need to protect the privacy of the patient. Solutions should encrypt data in an end-to-end encrypted tunnel to prevent attackers from listening to the data stream. If the platform is purchased from a third party (for instance, Microsoft Skype) then the healthcare provider needs to take additional measures to secure and protect data because the organization has no visibility about the safety of the data while the third party handles it. Third party contracts should address who is liable in the event of a breach. Solutions need multifactor authentication at both the doctor and patient sides of the communication to ensure that both parties are whom they claim prior to communication. This could prove difficult for handicapped patients and will require innovative solutions. As with most communications, the record that two parties spoke is a powerful enough piece of

information to suggest an invasion of privacy. For instance, if a spouse knew that their significant other telecommunicated with medical professionals, they might become worried and ask questions that their significant other may not want to answer. One method of protecting patient privacy would be to dissociate patient information from the patient account until the user is identified and authenticated. Dissociation, though more resource intensive within the databases, also affords a layer of protection to patients in the event of a breach because the adversary must dedicate resources to attempting to reconnect the data points.

One application of telehealth is to allow remote family members to join the patient and their doctor in the examination room. This application really helps patients who need emotional support. It also benefits doctors if the patient is known to become emotionally distraught easily because the doctor can convey treatment instructions to the patient's family members. This novel application still does not account for ways to account for eavesdropping on the other side of the screen. Organizations must also examine the legality of the solution because it may be illegal in some states if the health organization cannot guarantee that the audio and video of the appointment are not recorded. If recording of the appointment is permitted, then the compliance office and human resources office must decide what conditions bound the recording. The healthcare organization can likely avoid at least one lawsuit by deeming recordings from telehealth inadmissible in court.

Remote Monitoring:

One facet of the telehealth market is dedicated to remote monitoring systems that enable the elderly and homebound patients to remain at home. Remote patient monitoring is driven by

innovation in healthcare reimbursement models that recognizes the value in preventing hospitalization and readmission by promoting population health management and proactive intervention. A doctor can connect from any computer to an IP bridge to monitor a patient's condition in real time. The doctor can adjust medication or issue instructions as necessary. The Kaiser Family Foundation estimates the average 2013 hospital inpatient cost around $1700. Remote monitoring systems remove the cost from patients, providers, and payers by allowing the patient to stay home. Of Goldman Sachs' estimated $300 billion in savings from the integration of IOT and the healthcare sector, almost $200 billion is elimination of redundant and wasteful inpatient expenditures due to remote patient monitoring. The "Blue Ocean" created by the $200 billion cost reduction is estimated to be worth about $15 billion annually. Chronic disease management accounts for about one-third of all US healthcare spending. Remote patient monitoring can greatly decrease these costs in particular. In addition to the elderly and homebound, remote patient monitoring can help those with heart disease, COPD/asthma, or diabetes.

Remote monitoring devices could enable attackers to track the activity and health information of individuals over time. This possibility could impose a chilling effect on some patients. While the effect may lessen over time as remote monitoring technologies become normal, it could alter patient behavior enough to cause alarm and panic. As in telehealth, the healthcare organization needs to address third party use and solutions to the signal intelligence problem. Remote monitoring systems can be hacked either remotely to harm the patient or locally to obscure suspicious activity from the healthcare provider. Vendors should consider developing devices with security as a priority at every stage. One startup, Body Guardian, disassociates patient information from observation data within their system. Data is encrypted in

storage on device and during transmission. Other firms should consider similar solutions that segment the patient information so that if the device is compromised from one end, the attacker only compromises half the data. Pain medicine pumps and other devices that distribute controlled substances are likely high value targets to some attackers. If compromise of a system is as simple as downloading free malware to a USB and plugging the USB into the pump, then average drug addicts can exploit homecare and other vulnerable patients by fooling the monitors. One of the simpler mitigation strategies would be to combine remote monitoring technologies with sensors that aggregate activity data to match a profile of expected user activity.

Behavior Modification Devices:

Behavior modification devices encourage patients to adopt healthier lifestyles through the use of appealing technology, social pressure, and exercise gamification. As a result, patients are healthier and hospitals treat fewer patients for the trivial health conditions that result from inactivity (sprained wrist, poor diet, lethargy, etc.). Already, there are behavior modification devices to promote exercise and curb the obesity epidemic, to improve user lifestyle through diet management, and to assist in smoking cessation. It is difficult to estimate the total savings that these devices bring to the healthcare sector because their impact is projected into savings in other market segments. The commercial opportunity for developers sits around $6 billion; however, the segment is rapidly increasing. Business Insider estimates that 3.3 million Fitbits were sold in 2014; meanwhile, the BBC estimates that Apple sold 2 million Apple watches as of July 2015. As more devices are sold, more competitors are entering the market and the cost to consumers is dropping. This results in more users entering the market in proportion to the falling price.

Behavior modification devices are becoming ubiquitous in American society. Most behavior modification devices do not collect personal identifiable information and therefore only pose minimal risk to consumers (how much do they exercise, etc.). Some argue that information such as user's gait is identifiable information. There is some merit to the argument since gait recognition software is an emerging biometric; however, the main threat posed by behavioral adjustment devices is that users are often not informed of the data collected and most are ignorant of how the data is shared with third parties. Regulation that placed behavior modification devices under the purview of HIPAA would end most cases of data misuse.

Embedded Devices:

On the edge of the Internet of Things, embedded devices, software driven physical devices that are surgically implanted into a patient's body, deliver medication, monitor body functions, or support specific organs. The majority of embedded devices connect through Wi-Fi or Bluetooth to an application on the patient's smartphone. Common embedded devices are pacemakers, insulin pumps, and medicine administration devices. One emerging variants is a blood monitoring implant developed at Ecole Polytechnique Federale de Lausanne (EPFL) in Switzerland, that can notify a patient and their doctor before a heart attack occurs.

Unlike cell phones and other trendy technologies, embedded devices require years of research and development; sadly, cybersecurity is a new concept to many healthcare manufacturers and it may be years before the next generation of embedded devices incorporates security into its architecture. In other sectors, if a vulnerability is discovered, then developers rush to create and issue a patch. In the healthcare and embedded device environment, this

approach is infeasible. Developers must anticipate what the cyber landscape will look like years in advance if they hope to preempt attacks on their devices. This model is unattainable.

Most reports of breaches focus on violation of the requirement of confidentiality in the form of the unauthorized disclosure of data. In the case of embedded devices, the integrity of the data is the highest priority. Developers need to ensure that both the information received by the device and the information reported by the device is valid. In multiple demonstrations at the annual Blackhat conferences, at hospitals, and as reported on technology websites, hackers have been rapidly able to compromise embedded systems with little effort. One reason for the negligent amount of security on the device is the current architectural limitations inherent to the technology. In healthcare, every device and person has a maximum lifecycle. Every action has accompanying risk and expected results. Even the surgery to install an embedded device has a measurable risk associated with the procedure. So far, no life threatening incidents involving the compromise of embedded devices has been reported. Conversely, it is possible that the incidents are unreported because monitoring of the devices is limited in scope or that compromises are more serious than trivial inconvenience. Stakeholders need to decide whether securing embedded devices is worthwhile. Encryption is generally the solution for authentication of devices; however, as Cylance V.P. of Strategy Jon Miller points out, the encryption process adds overhead to the processors and could decrease the shelf life of the device from years to months. Developers need to collaborate with healthcare providers and patients, to invent a solution that limits harm while maximizing device utility according to each stakeholder's realistic expectations. Developers do not want to be sued over insecure or faulty devices. Patients may not want the additional surgeries necessary to replace the secured devices. Hospitals do not want to incur additional patient layover from more frequent surgeries. Any stakeholder might be

willing to risk continuously using an inherently flawed device if it means that patients are satisfied and that millions of dollars do not need to be allocated to researching a solution. Nevertheless, patients still might be susceptible to man-in-the-middle attacks and signal intelligence efforts. The easiest solution to mitigate these problems, until a less resource intensive form of multifactor authentication is found, would be to set the embedded devices to not advertise their presence by default. This method of obfuscation prevents basic attackers from knowing that there is a vulnerable device in the first place.

Mobile Applications:

Mobile healthcare applications precede many of the other healthcare technologies discussed above. Mobile applications are the support for some telehealth platforms, most remote monitoring devices, practically every behavior adjustment device, embedded devices, and the cloud. Mobile applications in any sector are notoriously insecure because the application market demands rapid development at minimal cost in order to churn a profit. As with any model that relies upon the notice and choice concept propagated by theories of privacy by policy, users tend to suffer because only a small percent reads the privacy policy and only a fraction of those readers fully understand how their information is stored, used, shared, and disposed.

According to a 2013 study by Deloitte, 97% of young adults own a cell phone and a very high proportion of those consumers use a smartphone capable of running mHealth applications. mHealth platforms are divided into four categories of increasing complexity: Single use mHealth, Social mHealth, Integrated mHealth, and Complex mHealth. The first category "focuses on a single purpose for a single user, typically consumer initiated." This covers

smartphone and wearable technology applications that record anonymous or pseudo-anonymous data. Social applications integrate social networks into the single purpose model. This increases user interaction and involvement, but it also increases the threat landscape because the user can be easily identified. An example of a social application is a fitness app that connects to Facebook. Integrated mHealth applications connect devices to the formal healthcare system through an electronic health record (EHR). For instance, technology to schedule an appointment or to interface with the medical community would qualify as an integrated mHealth application. Finally, Complex mHealth applications leverage data analytics to support decision capabilities at the point of care. Any application that utilized the recorded data for predictive analysis or that manages a chronic condition qualifies as a complex application. As with all data in information security, these applications need to be secured according to their complexity and the value of the data that they can access. Mobile application security needs to include encrypted information storage, and encrypted information transfer. The applications need to include multifactor authentication in the form of, at the very least, a password and one-time text message code (per sign-in). The application should also contain measures to prevent any malware resident on the phone or any other applications from leeching the secure data from the healthcare application. If the applications are developed or maintained by third parties between the user and the healthcare provider, then the third party needs to be held to the requirements of HIPAA, HITECH, and stringent requirements set by a collaboration of healthcare providers, payers, and patients so that patient privacy and information security is a top priority. According to a 2015 HIMSS mobile technology survey, 84% of healthcare organizations have attempted to incorporate mobile technologies such as mobile phones, tablets, and other technology, into their healthcare model. Only 18% of affiliated medical professional thought that the implementation was viable. In the

healthcare sector, Nurses are the frontline of the healthcare providers. Nurses are vital to successful patient interactions, data collections, and healthcare assessments. Nurses take all the initial measurements of patient condition. They make all the initial observations of patient wellbeing. Nurses are one of the primary users of healthcare apps. In many cases, they develop the apps. Nurses need to be included in the stakeholder discussions. Nurses need to be trained to safely use mHealth applications.

Data Sharing in the Cloud:

Health data is one of the most sensitive forms of data and it is capable of damaging careers, reputations, or lives. Attackers are extremely efficient at sharing information about targets, attack techniques, and malware. If one attacker figures out how to do something, then the populace eventually figures out how to do it. Due to efficient information sharing and the ease at which malware can be adapted into a new variant, there are 100,000-200,000 pieces of unique malware created every day. In order to combat their adversaries, the healthcare industry needs to improve its information sharing model. Digitizing and streamlining the sharing of healthcare data has the potential for dramatic gains in efficiency significant cost savings. To this end, the healthcare sector is looking to social, mobile, analytic and cloud (SMAC) technologies that are capable of using predictive algorithms to analyze big data, indicators of compromise, and electronic health records (EHRs) for emerging trends. Computer World predicts that big data analysis will result in a reduction of patient deaths and treatment costs by 10% by 2018.

Legislation and Collaboration:

Federal grants or the incorporation of encryption requirements into the HIPAA Security Rule could encourage healthcare providers to adequately secure patient records. Eventually, policy makers and healthcare industry security professionals will need to issue revisions to HIPAA that cover cyber-security practices and guidelines. Given the increased ease of stealing digital records over stealing paper ones, the penalties for information security breaches in the healthcare sector may need to be increased. One of the reasons that OPM's infrastructure was so poorly secured was that its administration strove to only meet some checkbox regulatory requirements. The Office of the Inspector General was very clear in the hearings that OPM had been advised about what systems to update, replace, or implement. For decades, OPM regulated security to an end-of-the-budget item. The administration did not see the value of investing a greater portion of its budget in improving the cybersecurity posture of OPM until it was far too late. Consequently, a foreign adversary stole 22.1 million records belonging to Federal employees that possess a security clearance. The national security of the United States will be at risk for the next 10-30 + years. Federal employees and Americans in general have all but lost trust in the competency of the Federal Government. Lastly, OPM is now investing $93 Million in taxpayer dollars to repair its antiquated system. Security best practices should not be limited to recommendations or guidelines.

In most industries, adhering to cybersecurity standards is a prisoner's dilemma. Companies believe that if they dedicate resources to improving their cybersecurity and their competitors do not, then they will lose competitive advantage in the market. This rationalization is flawed. Declining to improve internal cybersecurity is the equivalent of piling all of your company's money and assets into a house and then declining to hire guards, monitor cameras, or

install a security system. Sure, locking the front door will deter unskilled malicious actors, but eventually evolved adversaries will find a way to the poorly secured treasure. In fact, the situation worsens when you consider that in a breach in the healthcare sector, the victims are predominantly patients and employees. Their wealth and wellbeing leave with the attacker. Who wants to be in the chair that angered eyes turn to when they discover that their livelihoods were stolen because "there was not enough left in the budget?"

The Federal Government has the power and the responsibility to end industry wide cybersecurity apathy. Healthcare service providers, healthcare manufacturers, and security experts can instigate and support initiatives to change the status quo. Penalties for noncompliance need to be implemented and enforced. Though further regulation is not ideal, organizations benefit internally and externally from supporting change. Within the organization, cybersecurity is improved. Employees feel better about the organization. Customers trust the organization more. The reputation of the organization improves and recruiting new talent becomes easier. In the external marketplace, competitors are subject to the same regulations. Smaller, industry-disrupting organizations might experience a barrier to entry. Only the organizations who meet regulations will survive. As a result, the industry as a whole will improve. After a few years, the healthcare genre will not be the most vulnerable sector. Attempted breaches will decline within the sector as attackers try to compromise less secure systems in other spaces. In the medical device market, the FDA already has the power to effect stricter security requirements. So far, they have declined to do so. New regulations should at a minimum, require an external audit of organizations systems, access management, data masking procedures, and data storage security.

The healthcare threat environment is a dynamically changing cyber landscape. Legislation on the other hand, is stagnant. In many cases, by the time a law or regulation is passed and implemented, the adversaries have evolved beyond the scope of the control. In the financial sector, if an individual's identity is compromised, they get their money back, but financial institutions have to compensate for the loss. The FS ISAC has developed ways for companies to come together to share indicators of compromise so that those aggregate losses are decreased. FS ISAC pooled resources from its members and built its own information-sharing platform. Further, the financial sector is beginning to investigate the interdependencies between sectors in order to measure the impact that a breach has on other sectors because breaches are no longer cloistered incidents. Because adversaries are targeting multiple sectors, multiple stakeholders need to be into brought to the discussion. At the very least, healthcare providers, payers, patients, governing bodies, and the Federal Government need to be included in the discussion about how to improve data interoperability, data protection standards, and sector response to emerging threats.

At their December 2015 event, the Bipartisan Policy Committee expressed a near term focus on developing a secure exchange of health information. EHR interoperability is a priority for 2016. This includes making health data ready and usable for patients, standardizing EHR systems, increasing market transparency, and making EHR systems more efficient. By the end of 2016, the Office of the National Coordinator for Health IT wants to facilitate the creation of secure information highways across state lines. The agency is also hosting application challenges, which will reward developers and providers for creating secure apps that allow patients to access their health data. Additionally, the ONC will create a prototype app store

where industry professionals can access approved applications ranging from user interface applications to data access applications.

In October 2015, Sen. Bill Cassidy (R-La) and Sen. Sheldon Whitehouse (D-RI) proposed the Transparent Ratings on Usability and Security to Transform Information Technology (TRUST IT) Act of 2015. TRUST IT requires the ONC to institute a system to rate product security, usability, and interoperability. Product performance results are to be published on the ONC website. Consumers can use the results to compare products based on performance and make an informed decision about which product to select. Additionally, the bill requires an open and transparent stakeholder input system in creating the ranking system and it includes a process for the collection and verification of confidential feedback from healthcare providers, patients, and others who experience problems with the devices. “Vendors must provide information concerning user practices that may inhibit interoperability.” Every two years, vendors would be required to report on the performance of their health IT products. Fines and product decertification would be levied against manufacturers who do not report. The Inspector General of the Department of Health and Human Services must investigate allegations of information blocking and impose penalties as necessary.

In February 2014, NIST released its most recent cybersecurity framework. In accordance with a request from the American Hospital Association, NIST attempted to keep the framework flexible and voluntary in the private sector. Overall, the framework mirrors the recommendations in the HITRUST Common Security Framework. NIST’s framework is not compliance based; instead, it is risk-based. The framework uses a common language to address cybersecurity risk with cost effective solutions based on business needs rather than regulations. The framework is comprised of three sections: the Core, Profiles, and Tiers. The Core section provides a high-level

view of an organization's management of cyber risk according to five functional groups of: Identify, Protect, Detect, Respond, and Recover. The Profile section directs the creation of an organizational roadmap for reducing cybersecurity risk. The roadmap is guided by organizational goals, regulatory requirements, industry best practices, and risk management priorities. Finally, the tier section segments activities into levels based on the rigor of risk-management practices, the degree that the activities reflect business needs, and the how the activities are integrated into the risk-management process. NIST is seeking comments on improving the framework and information about how the framework is being implemented by February 9, 2016.

In November 2015, Bloomberg published the story of how hacker Billy Rios tried to change the security culture surrounding medical devices. Rios is not the first researcher to publically challenge device manufacturers in an attempt to galvanize industry wide reform or regulatory measures. For instance, at Def Con 2011, researcher and diabetic Jay Radcliffe, demonstrated how he could hijack his Medtronic insulin pump and manipulate it to deliver a potentially lethal dose. In fall 2013, the Mayo clinic hired white hat hacker Billy Rios and others to test assess the cyber security vulnerability of 40 medical devices ranging from MRI machines to ultrasound equipment. "Every day, it was like every device on the menu got crushed," Rios says. "It was all bad. Really, really bad." The numerous vulnerabilities in the devices were focused around undefended operating systems, generic hardcoded passwords, and other basic information security taboos. The Mayo Clinic used the results to draft a set of security standards which medical device suppliers had to meet to prior to entering into a contract with the Mayo Clinic. At home, Rios found that he could connect a Hospira infusion pump to his home network and digitally press the buttons as if a human were standing in front of it. Rios sent his findings to the FDA and Hospira, but received no response. Nevertheless, he continued to purchase and test

medical devices at his home. Hackers like Rios and Radcliffe receive neither praise nor gratitude for their work. Instead, device manufacturers and hospital administrators criticize these free penetration testers, claiming that they scare the public away from devices that do more good than harm. These critics are forgetting that they are in a nascent market. They are forgetting the word "now." These devices might do more good than harm now. Every year more medical devices are infected with malware. It is only a matter of time before an attacker uses the devices for a cyber physical attack or to cause mass panic. Imagine the financial gain a criminal syndicate could accomplish if they held hostage every IoT enabled pacemaker using simple ransomware programs. Imagine the impact a cyberterrorist group could have if they shut off those pacemakers to send a message. In any other sector, device manufactures and hospital administrators would have bug bounty programs to invite researchers like Rios and Radcliffe to find these critical vulnerabilities. In the end, Rios had to make a public video to get the FDA's attention. The video included instructions on how to exploit the vulnerabilities in the Hospira pump and the exploit code needed for the attack. This led to an FDA advisory, which is the first time the FDA has denounced a product based on cybersecurity. The advisory did not compel Hospira to patch the devices in operation or to look for flaws in similar models. Medical devices are expensive for researchers to purchase on their own and test. Virtualization solutions could work, but few exist now. Rios is trying to establish a lending library of devices so that he and others can look for flaws in other medical devices. Hospitals and suppliers are encouraged to donate old and new medical devices for testing. Similarly, the FDA advisory caused more researchers and security firms to enter the space and begin to look for vulnerabilities in medical devices housed in hospitals and out of the package.

Like Rios, San Diego based security firm TrapX Security recognizes the dire straits that the healthcare sector is meandering. In fall 2014, TrapX installed virtual replicas of tangible medical devices on the networks of 60 participating hospitals. To an adversary, these devices appear to be real, connected to the internet, and running. The devices allow TrapX to track attacker activity through a network. After 6 months, 100% of the hospitals contained one or more infected devices. Many of the devices contained ransomware that had not been activated yet. Some attacks began with spear phishing campaigns that targeted hospital staff. Many attacks targeted systems operating on Windows XP or Windows 2000 platforms. In one case, the hacker penetrated the computer at a nurses' station and from there spread malware through the network. Eventually, the malware spread to radiological machines, blood gas analyzers, and other devices. Hospital antivirus scrubbed the nurse station computer, but did not remove malware from other systems. According to Carl Wright, general manager of TrapX, the participant hospitals rely on device manufacturers to secure the devices. However, device security is sporadic and reactive at best. Wright adds "These medical devices aren't presenting any indication or warning to the provider that someone is attacking it, and they can't defend themselves at all." Hackers established persistent presences on the unmonitored devices and used them as a beachhead for other attacks. TrapX believes that the goal of the attacks was to steal personal medical data, which is ten times more valuable than credit card information online. In one case, TrapX's fake systems recorded attackers exfiltrating medical records to a server in Eastern Europe. The attackers were believed to be a Russian cybercriminal organization. In this case, the attackers were logging into a blood gas analyzer from their control server in Eastern Europe, and then navigating to where medical records were located on the network. Records were then transferred back to the infected device and then transferred out to the attackers. TrapX confirmed this theory

by checking the BGA and finding patient data, which was not supposed to be there, in its memory. As with the devices that Rios hacked, many of the medical devices that TrapX examined were made vulnerable by manufacturers who preprogrammed hardcoded generic passwords as technician backdoors. These passwords are almost always just a Google search away. TrapX's work gives credence to Rios's call for cybersecurity reform in the healthcare sector. Denouncing a single vulnerable device does little to nothing if the devices are left "in the wild" alongside devices that are equally exploitable. Each vulnerable device erodes any security deployed by healthcare providers.

In 2011, the FDA launched the Case for Quality Initiative that suggests that device manufacturers focus on predictive and proactive measures instead of adhering to the bare minimum security requirements. Recently, the FDA released guidelines that recommend, but do not require, that device manufacturers consider cybersecurity risk in their design and development phases and that they submit documentation to the agency identifying any potential risks discovered. Providers and regulators are also supposed to identify and document risks as well. After the guidelines were released, the American Hospital Association sent a letter to the FDA urging it to do more to "hold device manufacturers accountable for cybersecurity." Device vendors need to respond faster to discover vulnerabilities and release patches before the vulnerabilities are exploited. Device manufacturers argue that their devices can only be breached if the hospital network is initially vulnerable. This is a strawman argument that attempts to shift responsibility for a flawed product onto the buyer and the users. In the auto industry for instance, if a product (a car) were to directly put the lives of its users (passengers) at risk during regular operation, then the device would be recalled according to federal mandate. Similarly, in the

healthcare sector, either device manufacturers need to stand behind their products or the FDA needs to hold them accountable.

Regulating the healthcare device space is difficult because the FDA has to draft regulations that are specific enough to matter and general enough to outlast threats that develop and permeate faster than the products that they target. The FDA deregulated the wearable technologies market on the basis that fitness devices do not collect enough information to pose a threat to their owners. In an attempt to lure innovators into the market, the FDA has also loosened oversight around healthcare apps, though it reserves the ability to enforce stricter standards if necessary. These decisions also allow the FDA to tighten broad regulations around other medical devices. Afterward, the FDA released guidance documents for mHealth devices and wearable technologies.

The guidelines closely follow NIST's recommendations. In their premarket device submissions, manufacturers justify their choice and implementation of security on their device. To improve security, basic vulnerabilities that result from technician backdoors and hardcoded generic passwords should be mitigated. The premarket submission should include a hazard analysis, mitigation strategies, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with a given device. The submission should include a specific list of the cybersecurity risks that were considered in the design phase and a specific list and justification for all the cybersecurity controls that were built into the device. The justification should include a traceability matrix that links cybersecurity controls to cybersecurity risks considered in the design of the device. Manufacturers should summarize a plan for providing software updates and patches throughout the lifecycle of the device and a summary of the controls that are built into the device, including how they are configured. Finally,

submissions should include instructions for proper product use according to the cybersecurity controls and the intended use environment.

21st Century Cures Act:

Overall, the FDA is slowly embracing its role as cybersecurity monitor. It has even begun to include patients in the regulatory discussions. Conversely, the House of Representatives recently passed the 21st Century Cures bill to increase funding to the FDA and, ironically, to ease regulatory hurdles for advanced devices by removing the clinical trial phase. An *InsideHealthPolicy* investigative report asserts that the FDA worked with the Advanced Medical Technology Association (AdvaMed), a medical device lobbying group, on provisions of the 21st Century Cures bill. The provisions in question include the review process for devices and quality assessment requirements. Information supporting the report was acquired from a Freedom of Information Act request. The FDA contends that it met with "a diverse group of stakeholders" in development of the bill. Moreover, some doctors such as Susan Molechan, M.D., James Rickert, M.D., and John Powers, D.M.D., argue that the construction of the provisions of the bill will make newly approved drugs and medical devices less safe and less effective while innovation is dampened and the cost of medical devices increases. Privacy advocates fear that the language of the bill allows a healthcare provider to share all research with any HIPAA covered entity and to disclose personal health information at cost to pharmaceutical companies and medical device manufacturers for research purposes. The former provision was included to fix an inconsistency with HIPAA that prevented hospitals from publishing observational research that improved patient care. Only time will tell how the FDA manages to balance the pressures from

manufacturers and legislators who receive funding from manufacturers with the need to improve security and privacy controls in the healthcare sector.

Telehealth Solutions for Veterans:

In 2014, 677,000 veterans sought healthcare from phone or online services; additionally, 306,000 of these veterans are located in rural areas where comprehensive healthcare solutions are further away and may be less specialized. 122,000 veterans used telehealth specifically to obtain mental health services from their home. According to a letter written by Health IT Now Executive Director Joel White, the VA is a "leader in telehealth". White also claims that telehealth solutions reduce hospital admissions by 35 percent and the number of days of inpatient care by 59 percent. In the letter, White states, "Despite these advances and outcomes, artificial geographical restrictions on the use of telehealth constrain its growth within the VA." White wrote, "Under current law, the VA can only waive state physician licensing requirements if both the physician and patient are located in a federally-owned facility. We applaud your efforts to remove these restrictions by allowing physicians to treat veterans in their home, regardless of location. In a modern world of increased travel and technology utilization, health care should not be restricted by state borders." The *Veterans E-Health & Telemedicine Support (VETS) Act of 2015* (S. 2170) eliminates the requirement that VA physicians be licensed in each state in which they treat a veteran. This permits VA physicians to use telehealth to treat veterans who are not in the local vicinity. Senator Joni Ernst (R-Iowa), who co-sponsors the bill with Senator Maie Hirono (D-Hawaii), estimates that at the moment, 12 percent of veterans use telehealth in some form and that the service saves an average of $2000 per patient on medical costs. The bill has received support from the American Telemedicine Association, the American Legion, Veterans

of Foreign Wars, Paralyzed Veterans of America, Concerned Veterans for America, Iraq and Afghanistan Veterans of America, and the Health IT Now Coalition. The Federation of State Medical Boards suggests their own Interstate Medical Licensing Compact as a solution that would provide greater accountability and oversight. FSMB Chief Advocacy Officer Lisa Robin claims, "In its current form, the proposed VA legislation falls short of ensuring these protections, and it should be amended to strengthen them." However Physician-Patient interstate operability is resolved, veterans do benefit from the availability of telehealth solutions. Telehealth solutions can be used to deliver mental health treatment, physical therapy regimes, and in home medical monitoring and evaluations to veterans. Telehealth solutions would greatly assist veterans who are homebound, those who are not located near specialized care, and those who need mental health treatment but are too embarrassed or reluctant to seek treatment in person.

Telehealth Access Expansion:

Over the past year, there have been over 200 pieces of legislation meant to expand telehealth delivery methods in 42 states. The National Law Review reports that 29 states and Washington D.C. have enacted legislation requiring private insurers to reimburse medically necessary telemedicine. Other states have adopted restrictive telemedicine policies, which deter telehealth adoption by requiring that the patient be accompanied by an in-person health professional during the telehealth session, that the patient physically be in a medical facility during the telehealth session, or that the patient sign special consent forms. Hawaii, Indiana, and Ohio set minimum distance requirements in order to qualify for Medicaid coverage. These laws reduce healthcare availability for the elderly, infirm, isolated, and busy. Conversely, some

federal legislation aims to expand healthcare availability and Medicare coverage for those in need.

In November 2015, the Centers for Medicare & Medicaid Services (CMS) approved a Medicare payment model for hip and knee replacement that allows patients to utilize telehealth solutions. The Comprehensive Care for Joint Replacement (CJR) model restricts coverage to office visits and consultations made through an interactive two-way telecommunication platform with real –time audio and video. The patient connection must be initiated from a medical facility in a "Health Professional Shortage Area" or a rural county that is outside any Metropolitan Statistical Area. The *Telehealth Innovation and Improvement Act* would modernize Medicare to cover additional telehealth services. This would especially help seniors in rural America access specialty care that is otherwise unavailable in their areas. The sponsors, Senator Gary Peters (D-MI) and Cory Gardner (R-CO), claim that the legislation also incentivizes innovation in the industry. According to CMS, currently Medicare covers office visits and consultations between doctors and patients over two-way telecommunication systems that rely on audio or video for patients that live in remote areas. Remote patient monitoring, electronic healthcare record storage and forwarding, interstate services, and consultations without video or outside a rural setting, are not covered under Medicare. The Act requires the Department of Health and Human Services to permit eligible healthcare providers to test telehealth services through the Center for Medicare and Medicaid Innovation (CMMI). CMMI would then independently review and evaluate telehealth models for cost, effectiveness, and how much quality of care is improved without increasing the cost of delivery. If the solution meets CMMI's criteria, then it will be covered under Medicare. If the Act passes, then a pilot program would be launched prior to nationwide reform. Finally, Senator Brian Schatz (D-Hawaii) has stated his intent to submit a bill that

enables healthcare providers to employ telemedicine technology in telestroke programs and other alternate payment programs covered under Medicaid Advantage.

Prescription Drug Monitoring:

The House Oversight Committee is examining the Office of National Drug Control Policy (ODCP) for reauthorization. The ODCP creates a database of prescription opioids. Prescription information can be used to pinpoint signs of opioid dependence or addiction in patients or irresponsible prescriptions by medical professionals. At the moment, only about 25% doctors participate in prescription drug monitoring programs (PDMPs). PDMPs need to be more accessible to doctors and they need to include benefits like timely alerts when patients are identified as dependent/ addicted. Depending on the state, PDMP's databases change the behavior of 41-74% of prescribing providers. This change in behavior could be beneficial oversight or it could be a chilling effect. Only Oklahoma requires real time data reporting. Most programs are poorly designed and take too much time interacting with an unintuitive interface to access useful information. PDMPs would be more useful to Physicians if they were integrated into EHRs. According to CMS, provided that a PDMP is declared correctly, it can count as a specialized registry; therefore, its integration will meet meaningful use requirements.

In 2010, the Drug Enforcement Administration revised regulations to allow healthcare providers the ability to issue electronic prescriptions for controlled substances (EPCS) and to authorize pharmacies to receive, dispense, and archive e-scripts. EPCS decrease costs by eliminating the need for patients to visit the doctor's office to renew a paper prescription. The U.S. Justice department predicts that e-prescribing could result in annual cost savings of $700

million. EPCS increase safety and accountability by documenting patient use information and the doctor's DEA number into the patient EHR. Many providers and pharmacies have had difficulty implementing EPCS systems due to two-factor authentication and software system interoperability requirements. Some legislation, such as Ohio Senate Bill 129, addresses the barriers by suggesting a prior authorization system bound by mandatory response time limits. Fifteen other states have also enacted legislation to improve prior authorization.

EHR Interoperability:

The 2009 stimulus package approved by Congress and the Obama Administration offered $29 billion in incentives to U.S. healthcare providers to adopt electronic health record (EHR) systems. According to a 2010 White House report, the driving vision behind the incentives was to create an interoperable and intercommunicating system that would allow a healthcare provider to locate a patient's records with a single query. Despite the incentives, it is difficult for healthcare providers to interface commercial systems, like EPIC, with clinical or billing software made by other companies, let alone to interface with other EHR systems. Vendors such as EPIC and Athenahealth area accused of deliberately walling their systems off in a strategic attempt to gain customers. Further, Politico reported that independent practices are accusing larger healthcare providers of using their records systems, most of which rely on EPIC or Athenahealth, and pressing smaller providers, who use different EHR systems or still rely on paper files, into joining their networks. In June 2015, Connecticut became the first state to pass legislation prohibiting the use of EHRs to block the flow of data in this manner. Other states may follow suit in 2016.

Another barrier to EHR interoperability is lack of a common framework. So far, vendor and cross vendor solutions have not worked. Non-profit Health Level 7 (HL7) is developing the Fast Healthcare Interoperability Resource (FHIR) as a standard for electronic exchange of electronic healthcare information. Many hospitals are predicted to upgrade to technology that supports FHIR-based APIs in the next two to three years. Another solution would be to issue a national patient identifier system under the Department of Health & Human services under the language of HIPAA. Until now, single patient identifier systems have been dismissed on the basis of privacy concerns; however, inaccuracies in 8-14% of medical records and the significant costs of aggregating patient records between providers are two of the largest barriers to EHR interoperability.

EHR adoption barriers exist for healthcare professionals in specific settings as well. Ambulatory surgical physicians are excluded from receiving EHR meaningful use incentives because ambulatory surgery centers were not covered under the provisions of HITECH in 2009, which set the incentives for EHR adoption. Congress is considering legislation, such as the Electronic Health Fairness Act, H.R. 887, to grant ambulatory surgical center physicians the same payment incentives for meaningful use of EHR as doctors in other settings. The bill went to the Senate and was amended to say that "until such time as EHR technology is certified specifically for use in the ambulatory surgical centers, patient encounters that occur in such a center should not be used when calculating whether an eligible professional meets meaningful use requirements." CMS defines a meaningful EHR user as a healthcare professional who has 50 percent of their outpatient encounters occur at practices equipped with EHR technology. The Senate clause will no longer apply three years after HHS certifies EHR technology for use in ambulatory surgical centers.

mHealth IRB

A University of California, San Diego research team is developing the Connected and Open Research Ethics (CORE) project, which aims to construct ethical best practices for research studies involving participants' personal data and confidential healthcare information. At the moment, there are about 6,000 Institutional Review Boards (IRB) that govern ethical research practices involving human data subjects. IRBs have not developed ethical standards around mHealth technologies because the technology has developed so quickly. One aspect of the project is a Web resource for IRBs and private research groups to ethically conduct mHealth research using the data collected from mobile applications, devices, sensors, and social media platforms. The Web resource will ensure that IRBs can make informed decisions on mHealth studies. One major reason that mHealth applications are failing to deliver benefits to users is that developers either do not know how to protect private data or that privacy protection is considered unnecessary. IRBs can set standards for data collection, treatment, and storage. Further, compliance with the standards will ensure data operability based around security and privacy. IRB standardization can preempt data sharing and privacy issues that could stymie the growth of mHealth sectors.

Conclusion:

The OPM breach was a direct result of administrative mismanagement, unreliable third party contractors, and an antiquated approach to cybersecurity. 22.1+ million American citizens have suffered as a result. The assumed actor, Deep Panda, has since continued to target healthcare organizations post Anthem and Premera breaches; breaches which have put at risk over 91 million American's electronic health records. The remainder of the healthcare sector

needs to learn from these prolific breaches before their organizations are the next to fall and place patients at risk. Cybersecurity reform must encompass the people in the organization, the policies and procedures in place, and the technologies deployed. While the internet of things will drastically expand the cyber-threat landscape surrounding the healthcare sector, the benefits to organizations and our population warrant taking the consideration of how to adopt the emergent technologies in ways that heal the security posture of the organization rather than putting it under the knife of a merciless adversary.

The healthcare sector is the most targeted yet underprepared genre within our Nation's critical infrastructures. The already massive and expediently expanding IoT attack surface of this industry offers script kiddies a domain to wreak havoc, mercenaries an all-encompassing plane upon which to exfiltrate records for capitalization and state sponsors an unprotected target to accumulate a database from which to derive future surveillance and adversarial positioning. With each item connected to the internet of things there is a universe of vulnerabilities. Empirical evidence of aggressive penetration testing before and after a medical device is released to the public must be a manufacturer requirement. This will not stifle innovation; rather it will create more opportunities through the perfection of technology. Through identification, analysis and patching of vulnerabilities, organizations will be forced to innovate in a more diversified arena thus increasing the rate and space of innovation. Dissecting latent exposure, unwarranted backdoors and viewing the device's position as a 'part' of the whole of the healthcare macrocosm forces technologists to analyze the all-encompassing risks of their medical device in the open domain, thus tossed into a tumultuous sea of adversarial intent.

The human element of cybersecurity continues to be the weakest element. Ongoing training must be paramount in any responsible healthcare organization. Adversarial initiatives

typically start with targeting staff via spear phishing and watering hole attacks. The act of an ill-prepared executive clicking on a malicious link can trigger a hurricane of immediate and long term negative impact on the organization and innocent individuals whose records were exfiltrated or manipulated by bad actors.

Staff education, pre-market dissection of technology and patching of vulnerabilities that stimulate innovation and protect the public, and legislation that protects patient privacy and enforces device cybersecurity at the manufacturer level are only the first steps in creating better national cybersecurity hygiene. A cybersecurity-centric culture must demand safer devices from manufacturers, privacy adherence by the healthcare sector as a whole and legislation that expedites the path to a more secure and technologically scalable future by policy makers.

Acknowledgements

Expert research for this brief was contributed by the following:

- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)
- Dan Waddell (ICIT Fellow – Director, Government Affairs, $(ISC)^2$)
- Jon Miller (ICIT Fellow – V.P Strategy, Cylance)
- Rob Bathurst (ICIT Fellow – CISSP, Professional Services Director, Cylance)
- Malcolm Harkins (ICIT Fellow – Global Chief Information Security Officer, Cylance)
- Greg Cranley (ICIT Fellow Sr. Director of Federal, Centrify)
- Danyetta Magana (ICIT Fellow – President, Covenant Security Solutions)
- Seth Nylund (ICIT Fellow – V.P. Federal, Exabeam)
- Michael Seguinot (ICIT Fellow – Regional Sales Director, Exabeam)
- Stacey Winn (ICIT Fellow – Sr. Product Manager, ForcePoint)
- Ashok Sankar (ICIT Fellow – Security Evangelist, ForcePoint)
- Steve Curren (Acting Director, Division of Resilience, HHS)
- Rob Roy (ICIT Fellow – Public Sector CTO, Hewlett Packard Enterprise)
- Stan Wisseman (ICIT Fellow – Security Strategist, Hewlett Packard Enterprise)
- Montana Williams (ICIT Fellow – Cybersecurity Evangelist, ISACA)
- Jerry Davis (ICIT Fellow & CIO, NASA Ames Research Center)
- Kevin Stine (Leader, Security Outreach and Integration Group, NIST)
- Elisabeth George (ICIT Fellow – V.P. Global Regulations & Standards, Philips)
- John Menkhart (ICIT Fellow – V.P Federal, Securonix)

Contact Information

Legislative Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies, Executive Branch and Fellow Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Works Cited:

Beckers Hospital Review:

http://www.beckershospitalreview.com/healthcare-information-technology/the-opm-and-ucla-breaches-5-lessons-learned.html

Business Insider:

http://www.businessinsider.in/Goldman-Sachs-says-a-digital-healthcare-revolution-is-coming-and-it-could-save-America-300-billion/articleshow/47873180.cms

CIO

http://www.cio.com/article/2947896/healthcare/the-digital-health-revolution-and-what-it-means-for-us.html

http://www.cio.com/article/2981481/healthcare/how-the-internet-of-things-is-changing-healthcare-and-transportation.html

http://www.cio.com/article/2933020/healthcare/healthcare-it-makes-improved-customer-service-an-urgent-priority.html?nsdr=true

http://www.cio.com/article/2682872/healthcare/how-boston-childrens-hospital-hit-back-at-anonymous.html

Daily Caller:

http://dailycaller.com/2015/10/28/us-healthcare-under-tidal-wave-of-chinese-hacking/

Dark Reading:

http://www.darkreading.com/compliance/healthcare-information-security-still-no-respect/d/d-id/1113755

Electronic Health Reporter:

http://electronichealthreporter.com/three-steps-healthcare-organizations-can-take-for-a-more-secure-network-2/

Bloomberg:

http://www.bloomberg.com/features/2015-hospital-hack/

Embedded Computing Design:

http://embedded-computing.com/articles/minimizing-software-todays-medical-devices/

Extreme Tech:

http://www.extremetech.com/computing/151134-worlds-smallest-blood-monitoring-implant-talks-to-a-smartphone-but-whose

Fierce Health IT:

http://www.fiercehealthit.com/story/opm-hack-teaching-moment-healthcare-providers/2015-08-17

http://www.fiercehealthit.com/story/lawmakers-rethink-requiring-encryption-hipaa/2015-02-09

http://www.fiercehealthit.com/story/fda-toothless-dragon-med-device-security-researchers-say/2015-11-13

http://www.fiercehealthit.com/story/health-data-interoperability-urgent-matter-need-more-active-government/2015-10-21

http://www.fiercehealthit.com/story/anthem-hack-employee-access-not-encryption-problem/2015-02-11

http://www.fiercehealthit.com/story/premera-says-data-breach-may-affect-11-million-consumers/2015-03-

18?spMailingID=11717063&spUserID=MTg5MTY1NDgyMjkS1&spJobID=463795780&spReportId=NDYzNzk1NzgwS0

http://www.fiercehealthit.com/story/independent-researcher-discovers-infusion-pump-security-flaws/2015-05-27

http://www.fiercehealthit.com/story/interoperability-government-officials-make-plans-2016/2015-12-09

http://www.fiercehealthit.com/story/how-nists-cybersecurity-framework-will-impact-healthcare/2014-02-13

http://www.fiercehealthit.com/story/nist-seeks-comments-use-cybersecurity-framework/2015-12-11

http://www.fiercehealthit.com/story/future-physicians-need-telemedicine-education-training/2015-12-11

http://www.fiercehealthit.com/story/report-fda-worked-lobbying-group-21st-century-cures-provisions/2015-12-15

http://www.fiercehealthit.com/story/docs-21st-century-cures-measures-make-drugs-med-devices-less-safe-and-effec/2015-09-25

http://www.fiercehealthit.com/story/doug-fridsma-why-amending-hipaa-makes-sense-research/2014-12-03

http://www.fiercehealthit.com/story/21st-century-cures-act-raises-privacy-questions/2015-07-21

Fierce EMR:

http://www.fierceemr.com/story/senators-propose-bill-create-health-it-rating-system/2015-10-07

Fierce Health Payer:

http://www.fiercehealthpayer.com/story/anthem-hack-compromises-info-80-million-customers/2015-02-05

http://www.fiercehealthpayer.com/story/cyberattack-opm-may-be-linked-anthem-premera-breaches/2015-06-08

Fierce Mobile Healthcare:

http://www.fiercemobilehealthcare.com/story/research-team-aims-develop-ethical-best-practices-standards-mhealth-studies/2015-12-06

http://www.fiercemobilehealthcare.com/story/nurse-involvement-development-mhealth-tools-sight-sore-eyes/2015-11-16

Forbes:

http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/

Gizmodo:

http://gizmodo.com/circuit-board-tattoos-that-actually-work-will-make-your-1744403982?sidebar_promotions_icons=testingon&utm_expid=66866090-67.e9PWeE2DSnKObFD7vNEoqg.2&utm_referrer=http%3A%2F%2Fio9.com%2F%3Fsidebar_promotions_icons%3Dtestingon

http://gizmodo.com/5883146/what-is-hoic

Healthcare Information Security:

http://www.healthcareinfosecurity.com/interviews/breach-response-fighting-persistent-intruders-i-2981

http://www.healthcareinfosecurity.com/interviews/phi-breaches-just-healthcare-sectors-problem-i-2979

Healthcare Finance News:

http://www.healthcarefinancenews.com/news/bill-would-give-ambulatory-surgery-centers-incentives-meaningful-use-electronic-health-records

Health IT:

http://www.healthit.myindustrytracker.com/en/article/123534/2016-will-be-a-big-year-for-health-it?referer=left-div

http://www.healthit.myindustrytracker.com/en/article/123494/1-in-3-health-records-will-be-compromised-in-2016-5-things-to-know?referer=left-div

http://www.healthit.myindustrytracker.com/en/article/120987/fda-a-toothless-dragon-on-med-device-security-researchers-say

Health IT Security:

http://healthitsecurity.com/news/what-healthcare-can-learn-from-the-opm-data-breach

http://healthitsecurity.com/resources/white-papers/meeting-the-challenges-of-hipaa-compliance-phishing-attacks-and-mobile-secu

http://healthitsecurity.com/resources/white-papers/managing-cybersecurity-risk-in-a-hipaa-compliant-world

http://healthitsecurity.com/resources/white-papers/dealing-with-data-breaches-and-data-loss-prevention

http://healthitsecurity.hs-sites.com/why-data-awareness-protection-matters-in-healthcare?__hstc=40652093.4d256794fc4967b89caeb894560f29b3.1447092306734.1447092306734.1447092306734.1&__hssc=40652093.1.1447092306734&__hsfp=2063373969

http://healthitsecurity.com/news/breaking-down-the-evolution-of-healthcare-cybersecurity

Healthcare IT News:

http://www.healthcareitnews.com/blog/risk-analysis-could-have-prevented-opm-misery

http://www.healthcareitnews.com/news/top-5-security-threats-healthcare

http://www.healthcareitnews.com/directory/privacy-security

http://www.healthcareitnews.com/news/5-ways-telemedicine-can-boost-care-rural-communities?page=0

http://www.healthcareitnews.com/news/7-cyber-threats-other-phi-or-pii-breaches

The Hill:

http://thehill.com/policy/cybersecurity/262002-chinas-cyber-shift-prompts-scrutiny

HIMSS:

http://www.himss.org/News/NewsDetail.aspx?ItemNumber=40536

HIT Consultant:

http://hitconsultant.net/2015/12/08/epcs-and-prior-authorizations-prescriptions-for-better-patient-care/

Home Healthcare News:

http://homehealthcarenews.com/2015/12/medicare-bill-could-lead-to-more-tech-driven-home-health/

iHealthBeat:

http://www.ihealthbeat.org/articles/2015/11/17/cms-finalizes-medicare-payment-model-with-telehealth-implications

http://www.ihealthbeat.org/articles/2015/11/25/advocates-argue-state-policies-restrict-telemedicines-full-potential

http://www.ihealthbeat.org/articles/2015/11/19/senate-committee-considers-bill-to-expand-va-telehealth-services

http://www.ihealthbeat.org/articles/2015/12/4/senate-bill-aims-to-boost-access-to-telehealth-in-rural-areas

http://www.ihealthbeat.org/articles/2015/11/19/senate-committee-considers-bill-to-expand-va-telehealth-services

Info Risk Today:

http://www.inforisktoday.com/handbooks/state-healthcare-information-security-today-h-32

ISACA:

http://www.isaca.org/CERTIFICATION/Pages/default.aspx

(ISC)2:

https://www.isc2.org/hcispp/default.aspx

iSight Partners:

http://www.isightpartners.com/news/same-groups-may-be-behind-opm-healthcare-hacks/

Krebs on Security:

http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

MakeUseOf:

http://www.makeuseof.com/tag/4-top-hacker-groups-want/

Medical Device and Diagnostic Industry:

http://www.mddionline.com/blog/devicetalk/e-viruses%E2%80%94tackling-next-frontier-healthcare-06-17-15

mHealth Intelligence:

http://mhealthintelligence.com/news/support-builds-for-va-telehealth-legislation

http://mhealthintelligence.com/news/telehealth-scores-big-in-joint-replacement-bundled-payment-plan

http://mhealthintelligence.com/news/congress-set-to-see-a-flurry-of-telehealth-activity

mHealth News:

http://www.mhealthnews.com/news/demanding-mhealth-security-cloud-HIPAA-encryption

Nuix:

http://www.nuix.com/2014/09/30/one-step-ahead-how-and-why-do-hackers-choose-their-targets

Politico:

http://www.politico.com/tipsheets/morning-ehealth/2015/12/prescription-drug-monitoring-programs-in-spotlight-facts-figures-211546

Population Council:

http://www.popcouncil.org/about

Sans Institute:

https://www.sans.org/security-resources/idfaq/role.php

Tech Republic:

http://www.techrepublic.com/article/cybersecurity-professionals-the-healthcare-industry-needs-you/

Upmatters:

http://www.upmatters.com/news-upmatters/peters-introduces-bill-to-expand-access-to-telehealth-services

U.S. Food and Drug Administration:

http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ImplantsandProsthetics/

USA Today:

http://www.usatoday.com/story/tech/2015/06/05/opm-china-anthem-primera/28545997/

WatchGuard Security Center:

http://watchguardsecuritycenter.com/2015/12/03/watchguard-2016-security-predictions-1-ransomware/?utm_source=twitter&utm_medium=social&utm_campaign=2016predictionsblog

http://watchguardsecuritycenter.com/2013/05/30/hacker-profiles/

Wired Magazine:

http://www.wired.com/category/vanish/

http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

Xconomy:

http://www.xconomy.com/wisconsin/2015/12/09/as-criticism-mounts-health-records-firms-chart-path-to-data-sharing/