Ryan Yue

Domzalski

Writing 39C

23 November 2016

Information Security: A Multi-Pronged Approach to Protecting Against Ransomware

Hollywood Presbyterian Medical Center, a private hospital in southern California, was hit with a devastating attack sent by a group of hackers. The ransomware attack, a cyber attack that locks or encrypts all of the information on a computer or a set of computers, rendered the hospital’s technology utterly useless. Doctors stated that they were communicating through “jammed fax lines” and had to revert back to the outdated system of written records. Communication slowed down, and precautionary measures had to be taken with the incoming patients to prevent any unwanted complications. All surgeries and other major operations were halted, and patients that required immediate attention were transferred to nearby hospitals. Essentially, the hospital had shut down. After a week in this state of chaos, the hospital president and CEO, Allen Stefanek, had no choice but to pay the ransom of 14,000 dollars to reclaim access to the hospital’s technology (Siwicki, “Ransomware Attackers Collect Ransom”).

The overwhelming reliance on technology within hospitals and other institutions have caused the popularity of ransomware attacks to surge. In fact, it is estimated that technology will replace 80% of doctors’ tasks (Khosla). With hospitals expanding their software systems and the rising popularity of personal devices, there is a large amount of technology being used inside a hospital at any given time.

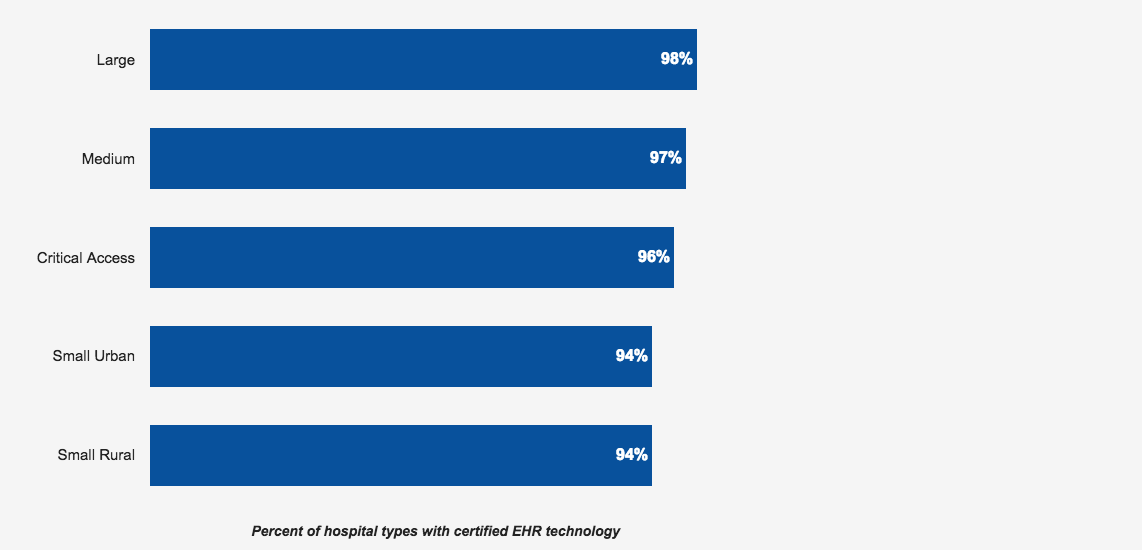


Figure 1: Percent of Hospitals Using Electronic Health Records (Mickelberg)

The figure above shows the highly popular use of electronic health record technology in all types of hospitals. An increase in use and reliance on technology makes access to the data vital to everyday operations, which incentivizes hackers to hold this data ransom. According to a U.S. Government interagency report, there are an average of 4,000 ransomware attacks per day, a 300 percent increase from the calculated average from 2015 (“FACT SHEET: Ransomware and HIPAA”). In addition, a report done by the SANS institute states that 72 percent of malicious traffic on the internet targets the healthcare sector (Filkins). Therefore, this increase in ransomware attacks has the greatest impact on healthcare-providing organizations. KPMG, a professional service company, has estimated that 80 percent of healthcare-related executives have compromised information somewhere within their company (Maness). Not having access to patient data and other import information can have hazardous consequences to patient care. “If PCs stop functioning and there are delays in information access and information flow, it could cause substantial disruption, and could even cause patient safety concerns” (Copley). Hospitals and other organizations refer to this situation as system downtime. According to a medical journal, “single component downtime can greatly interrupt workflow” and “can dramatically impact other areas, leading to cascading effects that may not be anticipated prior to their occurrence” (Campbell). In the case of system downtime, most hospitals revert to documentation through paper records; however, most hospital personnel are not prepared for these situations. “One faculty physician summed it up this way: ‘It’s funny now. When the computer goes down, we don’t remember how to document on paper’” (Campbell). Hospital systems are used from viewing patient medical history to ordering prescriptions to managing operating rooms. A study done by Dean Sittig and other clinicians revealed that 96 percent of healthcare institutions reported at least one instance of unplanned system downtime within the last three years, which exacerbated the conditions of at least one patient (Bowman). A successful ransomware attack on a hospital can cause delay of operations, a payment to the hackers, and most importantly, danger to patient care.

## Root Causes

Human usage of the technology is the one common denominator across all successful hospital ransomware attacks. According to the Information and Technology department of Mount Auburn Hospital, security awareness best practices state that 10% of safeguards are technical while 90% of safeguards rely on the computer user (“Quality & Safety”, Mount Auburn Hospital). Hospital personnel are responsible for using applications, downloading files from the internet, sending files to other computers, and many other operations.

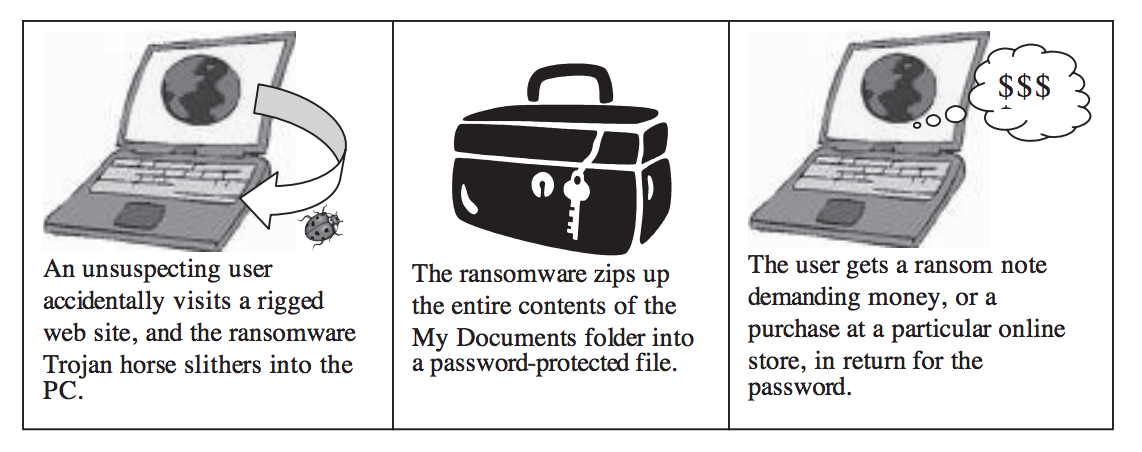


Figure 2: Simplified Progression of Ransomware Attacks (Luo, Xin)

All of these actions could potentially result in vulnerabilities and lead to malware being installed on the computers. Ransomware hackers rely on human error as the gateway in order to infect the computer systems with malicious software.

In addition, hackers have become more knowledgeable and aware of user behavior, which allows them to create more sophisticated attacks. Social engineering is a concept that refers to the psychological manipulation of people by taking advantage of humans’ tendencies to think a certain way (Diana). Phishing is one example of this manipulation. Hackers will imitate real organizations by creating counterfeit websites, emails, or advertisements and ask for user permission into their computer. By combining social engineering with advanced hacking programs, hackers are able to increase their chances of success. According to Verizon’s 2015 Data Breach Investigations Report, 23 percent of recipients open counterfeit emails and 11 percent download the attached files (2016 Data Breach Investigations Report). Users are generally unaware of the implications of downloading unknown files from an email. In addition, computer users rely too heavily on anti-virus programs to detect any signs of threat. Actions, like downloading files and opening emails, are performed countless times by hospital personnel, which could leave the system vulnerable to these attacks.

## Centralized Defense

An information security (IS) team is a team of cybersecurity professionals tasked to develop, educate, and implement security protocols within an organization (Rouse). This is separate form the information technology team that many businesses have. According to the article by Kristine Bruno, “the role of an [information technology] professional is to research and implement new technologies that will help [the] business grow”, while “the role of an information security specialist is to protect [the] business’ secure and confidential information” (Bruno). An IS team concentrates the cybersecurity efforts into one central group rather than spreading the responsibility of security across the entire organization, increasing the effectiveness of preventative efforts. The information security team provides better organization to cybersecurity defenses within the hospital and works in conjunction with the information and technology department to discover the hospital’s vulnerabilities. To reduce the number of successful ransomware attacks, hospitals should incorporate an information security department to secure private information, educate hospital personnel, and scan for potential cyber threats. This team can improve multiple aspects of a hospital’s cybersecurity, and proposes a multi-pronged solution to ransomware attacks.

The information security team can help reduce the amount of sensitive information stored in and accessed from an organization’s database. Sensitive information will be efficiently distributed among multiple databases and systems. According to Jim Thackston, a cybersecurity expert at International Data Group, “Large databases of aggregated information … are ‘honey pots’ since they are very sweet targets for hungry hackers” (Thackston). In a decentralized database, a hack that occurs in one database will only affect a fraction of the patient data will be encrypted by the ransomware. Decentralizing of data may decrease efficiency of data retrieval, but it will also minimize the organization’s potential attack surface. Potential attack surface measures the total sum of vulnerabilities in a certain device or network (Rouse). According to the 2015 Internet Security Threat Report done by Symantec, an organization with more data stored and accessed has proportionally higher potential attack surface (*ISTR 20 Internet Security Threat Report*). For example, if the patient needs to fill out information regarding their health insurance, it should be separated from other irrelevant and unnecessary information. Through this separation, hackers will not have access to all of a patient’s records at the same time. In addition, this information can help the information technology department and the information security team develop better defense architecture for the hospital’s systems. By minimizing these access points to patient data, hospitals can reduce their potential attack surface, which reduces the number of vulnerabilities in their networks and helps prevent hackers from exploiting those vulnerabilities.

Another improvement that the information security team can bring to healthcare organizations is the development of user education and training programs for the hospital staff members. User education and training addresses the human error component of cyber attacks. According to a study from the Impact of Education on Security Practices in ICT (Information and Communications Technology), the hypotheses that higher levels of education correlate to higher levels of email security, web security, and computer security are statistically significant for more than 90 percent of the time.

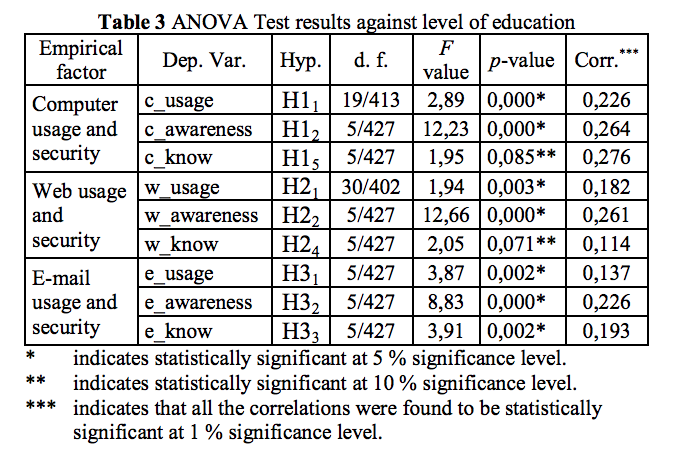


Figure 3: Correlation Between Usage, Awareness, Knowledge and Security (Boston, Atila).

As seen in the figure, the variables of knowledge, awareness, and usage are highly correlated, even in studies of over 400 participants (Boston). Because security is composed of these three major categories, this study can also depict the correlation between user education and better security practices. According to Dr. Roy Baumeister, “humans are much better than any other animal at changing and orienting [their] behavior toward long-term goals, or long-term benefits” ("Breaking Bad Habits”). If we apply this concept and the data from the study above to cybersecurity practices, it is clear that user education can help hospital staff members make behavioral changes that improve cybersecurity. User education has already made a positive impact in healthcare cybersecurity. According to a report by the US State of Cybercrime Survey by Pricewaterhousecoopers, 42% of people said that security education played a key role in prevention of cyber attacks (Mickelberg). User education and training plays a vital role in preventative action against ransomware attacks. The report also compared organizations that held mandatory employee security trainings with organizations that had no training requirement. Results showed that companies with trainings averaged a financial loss of $162,000 while companies without trainings averaged a financial loss of $683,000 (Mickelberg). Although there is no way to determine the cause and effect relationship between training and financial loss, the correlation between these two parameters is very strong. In addition, according to a study done by Wombat Security Technologies, the average cost of employee education in phishing attacks is $3.69 per user. In comparison, the estimated amount of money saved through employee education is $188.40 per user or $1.8 million per organization ("The Cost of Phishing & Value of Employee Training"). Ultimately, the information security team facilitates trainings and is in charge of implementing security policies within the organization, which can decrease monetary loss.

Finally, the information security team is in charge of scanning the system for potential threats. Particularly, this team can help detect phishing links or other social-engineered cyber attacks. This eliminates another cause of success ransomware attacks and will help hospitals increase awareness of these counterfeit items. If we just look at phishing emails, it is evident that there is already a huge problem. According to the 2016 Internet Security Threat Report by Symantec, 1 in 1,846 emails are phishing-related. In addition, an estimated 22 percent of all phishing attacks are targeted at the healthcare sector, with an average of 2.1 attacks per organization (*ISTR 20 Internet Security Threat Report*). By monitoring the emails, the information security team can detect unofficial email address, false links, and suspicious popups. In addition, the team can implement the use of anti-phishing browsers and phishing detection programs to reduce the number of attacks. Having the information security team scan and detect phishing attacks can save the hospital a great deal of money. In addition, the cybersecurity professionals in the team can help perform ethical hacking or penetration testing of the hospital’s systems in order to reveal the potential threats or vulnerabilities in the software. According to a report written by WhiteHat Security, the average remediation rate for vulnerabilities found through self testing can range from 16 percent to 35 percent (*Website Security Statistics Report 2015*). This rate is not very high; however, each additional test means that the hospital will have 16 to 35 percent less vulnerabilities. This ultimately reduces the hospitals potential attack surface and makes it difficult for hackers to gain access to the system.

# Cost Benefit Analysis

One limitation in implementing this solution is finding qualified individuals and integrating their expertise into the hospital’s daily operations. Although there are many talented information security experts, the process of gathering a group of these individuals can take a lengthy amount of time. According to a report done by Glassdoor, it takes an average of 51.8 days to hire program analysts, which hold similar positions to the members of the information security team (Chamberlain). It takes even more time for these individuals to get acquainted with the hospital’s structure and systems. According to an article by *U.S. News*, it can take new employees from three to six months until the employees know what they are doing ("Information Security Analyst."). Integrating an information security team into the hospital takes a huge amount of time, which can detract from effort and time needed to focus on other important projects. However, this is a one-time process during the setup phase of the information security team and is the same for the creation of any other department.

The creation of a new department in the hospital will impose a greater financial burden given the already stringent healthcare budgets. On average, health centers allocate 2.5 percent of their budget towards their IT department, which disproportionate to the importance of information and technology within the hospital (Halamka). According to *U.S. News*, the median salary for information security is $88,890, and the average size of an information security team is 3.7 members in North America ("Information Security Analyst."). In addition, there are costs of computers, servers, and many other factors for the information security team. However, this cost is comparatively less than the average 1.8 million dollars saved by organizations or 188.40 dollars per user with employee education or training ("The Cost of Phishing & Value of Employee Training"). This calculated numerical average does not factor in long term benefits of implementing the team and will increase as hospitals hire and replace staff members. Using cost-benefit analysis, we can see that the cost of running an information security team is relatively low compared to the amount of money saved from user education and protected data. In addition, this team can provide other benefits to the hospital, such as minimization of unnecessary data points. With the relatively low costs and relatively high amount of benefits, the implementation information security team is a financially sound decision for healthcare organizations.

# Other Possible Solutions

There are many governmental and private organizations that provide user education programs specifically aimed at cybersecurity for companies. According to an article by Dr. Qinyu Liao and Dr. Xin Luo, employees within the company are unable to quantify the amount of risk that lack of cybersecurity standards creates. “The key is to show employees how ransomware induced by a security lap can directly impact them and their company. For example, the company could lose stock value or important customers. The company could be shut down. When people understand how their behavior can affect their customers, their company, or themselves, they are more likely to take steps to protect themselves and comply with the policy, procedure, and regulations” (Luo). The data stated earlier about the benefits of user education reaffirms this claim in this report. The U.S. government in addition to many cybersecurity firms, like Symantec, Sophos, and Cisco, all have literature or programs to support user education. The SANS institute has many security awareness modules “that provides training that changes user behavior and helps [the] organization manage risk” ("Security Awareness Training for End Users.").

Even though these materials are readily available to all healthcare organizations, the methods of educating employees used are mundane and ineffective. These training programs, like the one provided by the SANS institute, mainly under the categories of passive computer-based training and formal training sessions (Cone).

Passive computer-based training provides accessibility at the cost of effectiveness and customizability. Computer-based training, or CBT, allows users to learn at their own pace and according to their own schedule; however, “its disadvantage is that training and awareness becomes a monotonous slideshow that fails to challenge the user and provides no dialogue for further elaboration. Often, users attempt to complete CBT sessions with minimal time or thought” (Cone). This type of disengaging training will not help users learn about cybersecurity threats. Instead, hospital employees will view it as another useless task in their already busy schedules.

Formal training sessions have a higher level of engagement, but they do not allow for convenience in scheduling. These sessions involve third party companies sending cybersecurity experts to host trainings with the hospital staff. “The success of this approach depends upon the ability of the training facilitator to engage the audience” (Cone). Because not all facilitators will cover the exact same topics with the same level of depth, there is high variability in the effectiveness of the trainings. In addition, most companies that host security trainings are not having these trainings often enough. According to the 2015 U.S. State of Cybercrime Survey, only 50 percent of respondents stated that they run periodic security training programs, and only 50 percent of respondents stated that they provide this training to new employees (Beard). This could be caused by scheduling conflicts, underestimating cyber threats, and other potential factors. With a built-in information security team, hospitals have much higher flexibility in scheduling security training sessions because hospitals will have constant access to their teams. In addition, the information security team can tailor each training to the specific needs of individuals or departments within the hospital.

# Conclusion

Hospitals contain thousands of patients’ personal information, and it is the hospital’s responsibility to keep this information secure. Currently, hospitals and other organizations are not centralizing their efforts in this war against cybersecurity. It is not enough to just hold basic and unengaging security trainings for employees. An information security team can not only provide tailored security training to each hospital staff member but also reduce the hospital’s attack potential. This is done by effectively organizing hospital data and scanning for abnormalities within the system. The upfront cost of implementing a new department is outweighed by the amount of money saved through educating users on best cybersecurity practices.

In a world where almost everything is digital, very strict standards must be in place to protect against hackers with malicious intent. Hospitals need to upgrade their security and ask information security experts for help with this problem. With a dedicated information security team, doctors can worry about saving lives without having to deal with system crashes and encrypted patient data.

Works Cited

*2016 Data Breach Investigations Report*. N.p.: Verizon, n.d. PDF.

*An ISTR Special Report: Ransomware and Businesses 2016*. Mountain View: Symantec, 19 July 2016. PDF.

Beard, Charles, Kevin Mickelberg, Emily Stapf, and Don Ulsch. *US Cybersecurity: Progress Stalled Key Findings from the 2015 US State of Cybercrime Survey*. N.p.: PricewaterhouseCoopers, July 2015. PDF.

Boston, Atila, and İbrahim Akman. "Impact Of Education On Security Practices In Ict." *Tehnicki Vjesnik / Technical Gazette* 22.1 (2015): 161-168. *Academic Search Complete*. Web. 14 Nov. 2016.

Bowman, Sue. “Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications.” *Perspectives in Health Information Management* 10.Fall (2013): 1c. Print.

"Breaking Bad Habits - NIH News in Health, January 2012." *U.S National Library of Medicine*. U.S. National Library of Medicine, Jan. 2012. Web. 17 Nov. 2016.

Bruno, Kristine. "What's the Difference Between Information Technology and Information Security | GraVoc Associates." *GraVoc Associates*. Gravoc, 04 June 2015. Web. 22 Nov. 2016.

Campbell, Emily M. et al. “Overdependence on Technology: An Unintended Adverse Consequence of Computerized Provider Order Entry .” *AMIA Annual Symposium Proceedings* 2007 (2007): 94–98. Print.

Chamberlain, Andrew. "Why Is Hiring Taking Longer? New Insights from Glassdoor Data." *Glassdoor*. Glassdoor, 18 June 2015. Web. 17 Nov. 2016.

Cone, Benjamin D. *A Video Game for Cyber Security Training and Awareness*. Monterey: Naval Postgraduate School, 2007. PDF.

Copley, Doug. "POTENTIAL EFFECTS OF RANSOMWARE IN HEALTHCARE." *Potential Effects of Ransomware in Healthcare*. Forcepoint, 29 Feb. 2016. Web. 14 Oct. 2016.

Diana, Alison. "Social Engineering Targets Weakest Security Link: Employees."*EnterpriseTech*. EnterpriseTech, 19 May 2015. Web. 21 Oct. 2016.

*FACT SHEET: Ransomware and HIPAA*. N.p.: HHS.gov U.S. Department of Health & Human Services, n.d. PDF.

Filkins, Barbara. *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*. N.p.: SANS Institute, Feb. 2014. PDF.

*Hacking Healthcare IT In 2016*. N.p.: Institute for Critical Infrastructure Technology, Jan. 2016. PDF.

Halamka, John D., MD. "The Cost of Information Technology." *Life As A Healthcare CIO*. N.p., 27 Nov. 2007. Web. 17 Nov. 2016.

"Information Security Analyst." *US News*. U.S.News & World Report, n.d. Web. 17 Nov. 2016.

*ISTR 20 Internet Security Threat Report*. Mountain View: Symantec, 2015. PDF.

Khosla, Vinod. "Technology Will Replace 80% of What Doctors Do." *Fortune*. Time, Inc., 03 Dec. 2012. Web. 21 Oct. 2016.

Luo, Xin, and Qinyu Liao. "Awareness Education as the Key to Ransomware Prevention." *Information Systems Security* 16.4 (2007): 195-202. *Taylor & Francis Online*. Web. 21 Nov. 2016.

Maness, Carter. "Hackers Will Probably Hold Your Medical Records Hostage. Here's What To Do About It." *GOOD Magazine*. GOOD Worldwide Inc, 01 July 2016. Web. 11 Oct. 2016.

Mickelberg, Kevin, Laurie Schive, and Neal Pollard. *2014 US State of Cybercrime*. N.p.: PricewaterhouseCoopers, 2014. PDF.

"Quality & Safety." *- Mount Auburn Hospital*. Mount Auburn Hospital, n.d. Web. 13 Oct. 2016.

Rouse, Margaret. "What Is Attack Surface?" *WhatIs.com*. WhatIs.com, Nov. 2014. Web. 14 Nov. 2016.

"Security Awareness Training for End Users." *Cyber Security Awareness Training | End User Computer Based Training | SANS*. SANS Institute, n.d. Web. 21 Nov. 2016.

Siwicki, Bill. "Ransomware Attackers Collect Ransom from Kansas Hospital, Don't Unlock All the Data, Then Demand More Money." *Healthcare IT News*. Healthcare IT News, 24 May 2016. Web. 06 Oct. 2016.

Thackston, Jim. "Cybersecurity Woes Can Be Remedied through Decentralization." *CSO Online*. CSO, 22 Nov. 2016. Web. 22 Nov. 2016.

"The Cost of Phishing & Value of Employee Training." *The Cost of Phishing & Value of Employee Training*. Wombat Security Technologies, n.d. Web. 14 Nov. 2016.

*Website Security Statistics Report 2015*. Santa Clara: WhiteHat Security, 2015. PDF.