Nonprofits and Specific Needs: Using Personalized Technology to Improve Operations in a Nonprofit

Analysis of the Current State of Cybersecurity in Large Nonprofit Healthcare Organizations

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Benjamin Israel

December 12, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

ADVISORS

Kent Wayland, Department of Engineering and Society
Briana Morrison, Department of Computer Science

Introduction

General Research Problem: Improving the Technology Capabilities of Large Nonprofit Healthcare Organizations

How can Nonprofit Healthcare Organizations utilize certain technologies to better fulfill their mission and stay safe from modern cyber attacks?

Non-profit Organizations are an extremely important aspect of society that can often be forgotten about. Nonprofits spend almost 2 trillion dollars per year, but many struggle to upgrade or modernize their technologies, especially cybersecurity. Nonprofits have an incredible potential to improve society that could be utilized with the right technologies. Imagine if a company like Apple or Google fell behind in modern tech (especially scary for cybersecurity), where would they be now? Nonprofits are no different: they still need to function efficiently, effectively, and safely (Wilson, 2020).

There are two driving factors for why nonprofits need to continuously update their technologies: falling behind can cause severe damage and getting ahead can grant tremendous opportunities. Nonprofits that fall behind in cybersecurity can be susceptible to cyber attacks that can steal money, sensitive data, or even lives. Hackers have been known to sell backdoor entries into organizations, where malicious users can buy username and passwords to gain access. In February 2022, Forbes released a report about advertisements offering access to Doctors Without Borders's server, which generates nearly 2 billion USD every year (Brewster, 2022). Even the largest nonprofits are still susceptible to these kinds of attacks. On the other hand, we have the benefits from successfully implementing modern technologies, which include time, money, and donor relations. Smart-tech has saved employees time by using a chat bot to answer frequently

asked questions, robots to deliver meals, and artificial intelligence to scan for possible donors (Fine & Kanter, 2021).

Technical Topic: Building a Personalized App for Meals on Wheels

How can personalized technology be designed for Meals on Wheels to improve its overall organization, effectiveness, and impact?

Meals on Wheels has the mission of providing nutritious meals and meaningful social interaction to hungry, isolated seniors in a dignified way. ZippyMeals was founded by a member of the Board of Directors for Meals on Wheels Charlottesville. With a background in software engineering, he soon realized that much of the day to day work could be organized through a central software. ZippyMeals decided to massively improve and automate parts of Meals on Wheels by moving away from individually managed spreadsheets towards a centralized location for all client and volunteer data. To build the Android version of the app, I programmed solely in Kotlin (Android Studio IDE) in a team of about 10 people split in groups of 1-2 to work on specific tasks.

The actual structure and relationship of objects was already decided, so the front end implementation was the largest part of my project. In building out the app, the most effective strategy that I found was to test things as I moved: code a small piece, make sure it works as intended, then repeat. In terms of project organization, one of the biggest issues was speed of groups, as the future work of one group may rely on the completion of another. In my case, working on the front end, there came a point where my next step was to connect the front end and the database; however, the database group was not yet done setting everything up. At first I felt stuck, but then I decided that instead of halting my progress, I could just manually code "fake" database entries to ensure the front end works as intended. This way, I could continue

working, and when the database was finished, I could simply replace my “fake” data with the real data and everything should run smoothly. Another useful method I used was trying to see the app as if I were a user. For example, for my front end code, would a volunteer driver find it easy to use? What if they are 60+ years old, will that make a difference? There are many things to consider when thinking about how the front end should look, so this exercise proved to be very helpful to me. For this project, it was very important to remember that our clients will tend to be on the older side, as designing for a 21 year old computer science student is very different from designing for a 65 year old who just got their first smartphone. Little things such as increasing button/text sizes, displaying only the key information, and adding a bit more directions can go a very long way.

ZippyMeals has saved Meals on Wheels employees and volunteers hours of time each week to reduce overtime, increase efficiency, and work on other meaningful tasks. When following up with some of ZippyMeals clients, it has confirmed that our solution does in fact save them time and is well liked. While the application has had some success, it can always be improved. Future work for the project includes adding more users, further optimization of routes, and serious cyber security testing to avoid any HIPAA violations. Additionally, as this is a personalized tool for Meals on Wheels, feedback and suggestions from users are often taken into serious consideration, so future changes originating from Meals on Wheels employees/volunteers ideas will be fairly common.

An Analysis of Cybersecurity in Nonprofit Healthcare Organizations

How do large nonprofit healthcare organizations work to protect their private data and handle cyber threats?

Introduction

Cybersecurity is a persistent threat for every single organization that uses any sort of technology or web service (vast majority). While there is no way to 100% guarantee that nobody can hack you, as cyber attack strategies evolve quickly, many steps can be taken to drastically reduce chances of a breach. I want to investigate the current steps that large nonprofit healthcare organizations are taking to protect their data and what they plan to do to improve on their shortcomings. Before any analysis, it is essential to understand the current state of cybersecurity in nonprofit healthcare organizations.

Background

There are many groups involved in my research, but the major ones include large nonprofit healthcare organizations, recipients of nonprofit assistance, hackers, and donors. Nonprofits and healthcare organizations have become a societal norm in the US, perhaps the world, where everybody knows what they are and has probably contributed to one in their lifetime. Even from a young age, many schools will organize their students to participate in some charity work at some point. In 2019 alone, nearly 30% of adults in the US volunteered, totalling to 5.8 billion volunteer hours (National Philanthropic Trust, 2021). The link between healthcare and nonprofits is very strong. More than half of the hospitals in the United States are nonprofit, as well as other health organizations like the International Committee of the Red Cross, Doctors Without Borders, and many others.

Nonprofits spend upwards of a trillion dollars per year, with major companies donating immense amounts of money to them. With this much money going through, the nonprofit industry stands to lose a lot in the face of a serious cyber attack. However, the current state of cybersecurity in healthcare nonprofits has much to improve on. In a 2021 survey done by the

Healthcare Information and Management Systems Society, nearly 35% of respondents did not have a dedicated percentage of the IT budget for cybersecurity. Budget was also listed as the biggest security challenge across all the participants. Based on this alone, I can already see that budget will be a major focus of my research. It is also interesting to note that the next three biggest security challenges were staff compliance with policies and procedures, legacy technology, and patch/vulnerability management. Staff compliance would undoubtedly increase with the implementation or improvement of cybersecurity training programs for employees. Legacy technology upgrades and patch/vulnerability management can be very pricey and may require a pause on some operations. It seems as though all the most common problems revolve around money. To really stress how much of an issue this is in some healthcare operations, of the 73% of respondents with legacy operating systems, the two most common were Windows Server 2008 and Windows 7. For reference, Windows 8 was released in 2012. It has been nearly 10+ years and some of these organizations still have not updated from an outdated (and potentially vulnerable) operating system. This is different than simply not having the latest technology, this is continuing to use technology that has been outdated for years and no longer used because of vulnerabilities. While budget may not be an issue for all of these organizations, it certainly is a shared problem among many (HIMSS, 2021).

The final piece of background that is necessary to understand the full scope of the system is cybersecurity standards. There are many different standards in cybersecurity, but we will focus on two in particular: National Institute of Standards and Technology (NIST) guidelines and the HIPPA Security Rule. The NIST Cybersecurity Framework is a government created set of rules and standards that are widely used and accepted by all sorts of organizations in the US. The HIPPA security rule contains additional specifications that organizations dealing with HIPPA

information must follow. With such an abundance of implementations, guides, and other resources about these two standards, these should be the expectation for organizations that take their cybersecurity seriously. This is not to say that these organizations are not meeting these standards, but to show that there is no lack of resources or guidelines about cybersecurity technologies.

Literature Review

In order to gain a deeper understanding of the relationship between cybersecurity and large nonprofit healthcare organizations, I will perform a case study of a recent cyber attack on the International Committee of the Red Cross. In addition, an analysis of healthcare cybersecurity for 2020 done by the U.S. Department of Health and Human Services will help to identify some trends in the industry.

In January of 2022, the ICRC first confirmed internally that servers holding sensitive information of at least 515,000 people were compromised by an advanced attack. It was determined that the breach happened on November 9, 2021, so the time to detect was around 70 days (compared to the average 212 days). The breach was possible due to an "unpatched critical vulnerability in an authentication module" that the hacker was able to exploit, granting access to the systems. Upon entry, a sophisticated offensive tool disguised the hacker as a real user. Although the ICRC applies the proper patches annually to all their systems, this breach took place between patches, so a potential mistake was not patching often enough. Additionally, after a deep analysis of the breach, it was discovered that the vulnerability management processes and tools failed to halt the attack. Following this attack, the ICRC has begun work with its Movement partners to rally others around protecting humanitarian organizations and data (International Committee of the Red Cross, 2022 June). Alongside "ensuring effective practices and

compliance with them", humanitarian organizations also need to share good practice and build a mutually beneficial group to protect data. On the government side, it calls for States to commit to a responsibility "to respect and protect humanitarian organizations and their staff, information and assets, online as well as offline". (International Committee of the Red Cross, 2022 May).

Cyber attacks on healthcare organizations can kill people. There are not many industries that can say the same. If a financial industry is breached maybe someone loses money, but in healthcare a breach can mean an ambulance gets rerouted or someone's medical records get permanently deleted. The risks for healthcare are far too serious to allow for weak cybersecurity infrastructure. In 2020, there was an "average of 816 attempted attacks per healthcare endpoint", which was a 9,851% increase from 2019. In addition, the median size of companies being targeted by ransomware attacks has been on a steep increase, growing nearly 400% from fall 2019 to fall 2020. Healthcare was the single most targeted industry by ransomware by an entire percentage point in quarter 4 of 2020. Based on this data, it is clear that not only are the number of cyber attacks increasing, but healthcare is also the biggest target (U.S. Department of Health and Human Services, 2021).

In order to further my research, the single most important resource that I could use would be an interview with a chief information security officer (CISO) of a large nonprofit healthcare organization, ideally a large one that has had cyber troubles like the ICRC. This would be the most valuable perspective to have in looking at the system, as a CISO has both the technical and organizational knowledge at play in the system. Given this may be difficult to set up, the next best thing would be some sort of public interview or discussion with CISOs. What I hope to learn from a CISO would be why some of the issues discussed in this paper even exist in the first place. For example, I need to talk to somebody on the inside to truly understand why a nonprofit

cannot simply update their legacy systems or increase their cybersecurity budget if those are such common problems. I want to dig deeper to figure out if it is a problem with technical expertise, funding, or something else entirely. Going off this, a detailed analysis of a real budget from one of these organizations, specifically cybersecurity spending, would give additional insight into the role money plays in the system. In addition, more case studies of past cyber breaches could reveal patterns or other helpful information to prevent future hacks.

Conclusion

I hope to learn about why the current cybersecurity infrastructure in healthcare nonprofits is the way it is and how to improve it. From my technical experience, I have seen first hand how personalized technology can benefit nonprofit organizations, especially those structured with a wide net of many local offices that operate very similarly to each other. We have discussed the state of cybersecurity in healthcare nonprofits today, case studies to highlight the risks of weak cybersecurity, and how security leaders are working to solve the problem. It seems that money and budget have been a common trend as a root cause of problems for healthcare organizations. As I see it, most of the technology is there and will continue to come, but there is a limitation in how much organizations can implement due to lack of resources. The risks are great enough that a change needs to be made to incentivize nonprofits to allocate proper resources to cybersecurity. There are definitely a lot of aspects to this that I will not understand as someone only associated with the cybersecurity defense part of the system, but direct information from a CISO in a larger healthcare nonprofit organization would be tremendously helpful.

References

Brewster, Thomas. (2022 February 23).*Hacker's Sell Backdoors Into A $2 Billion Nonprofit, A Californian Hospital, And Michigan Government*. Forbes.com. Retrieved from https://www.forbes.com/sites/thomasbrewster/2022/02/23/hackers-sell-access-to-a-2-billion-nonprofit-a-californian-hospital-and-michigan-government/?sh=4724fb995758.

Fine, Allison, & Kanter, Beth. (2021 December 09). *How Smart Tech Is Transforming Nonprofits*. Harvard Business Review. Retrieved from https://hbr.org/2021/12/how-smart-tech-is-transforming-nonprofits#:~:text=For%20example%2C%20food%20banks%20deployed%20robots%20to%20pack%20meals%3B%20homeless,software%20to%20identify%20potential%20donors.

Healthcare Information and Management Systems Society. (2021). *2021 HIMSS Healthcare Cybersecurity Survey*. HIMSS. Retrieved from https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf.

International Committee of the Red Cross. (2022 June). *Cyber-attack on ICRC: What we know*. ICRC. Retrieved from https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

International Committee of the Red Cross. (2022 May). *Safeguarding Humanitarian Data.* ICRC. Retrieved from https://rcrcconference.org/app/uploads/2022/05/16_CoD22-Safeguarding-Humanitarian-Data-Background-document-FINAL-EN.pdf.

Mierzwa, Stan, & Scott, James. (2017 February). *Cybersecurity in Non-Profit and Non-Governmental Organizations: Results of a Self-Report Web-Based Cyber Security Survey with Non-Profit and Non-Government Organizations*. ICIT. Retrieved from https://icitech.org/wp-content/uploads/2017/02/ICIT-Brif-Cybersecurity-and-NGOs.pdf.

National Philanthropic Trust. (2021). *Charitable Giving Statistics*. National Philanthropic Trust. Retrieved from https://www.nptrust.org/philanthropic-resources/charitable-giving-statistics.

U.S. Department of Health and Human Services. (2021 February 18). *2020: A Retrospective Look at Healthcare Cybersecurity*. U.S. Department of Health and Human Services. Retrieved from https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.

Wilson, Sevetri (2020 November 11). *How Technology Can Help Nonprofits Prove Their Value To Donors*. Forbes. Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2020/11/12/how-technology-can-help-nonprofits-prove-their-value-to-donors/?sh=750179bc21d8.