UNCOVERING THE ROOT CAUSES OF INADEQUATE CYBERSECURITY IN NONPROFIT HEALTHCARE ORGANIZATIONS

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Benjamin Israel

March 30, 2023

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.

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

In 2020, the U.S. Department of Health and Human Services (2021) reported that there was an “average of 816 attempted attacks per healthcare endpoint”, which was a 9,851% increase from 2019 (p. 4). In quarter four of 2020, healthcare was not only the single most targeted industry by ransomware, but it also experienced the most data breaches out of any other industry. Based on this data, it is clear that not only are the number of cyber attacks increasing, but healthcare is also the biggest, most vulnerable target (U.S. Department of Health and Human Services, 2021). From 2005 to 2019, roughly 250 million individuals were affected by security breaches in the healthcare sector, with about 145 million health records exposed from only 2015-2019 (Seh, Zarour, Alenezi, Sarkar, Agrawal, Kumar, Khan, 2020). 250 million is nearly three quarters of the entire 2019 US population (Malone, 2019). Cyber attacks on healthcare organizations kill people, as a breach can mean an ambulance is rerouted or medical records are permanently deleted. The risks for healthcare breaches are far too serious to allow for weak cybersecurity infrastructure.

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 and 73% still use legacy systems in their organization. Budget was listed as the biggest security challenge across all the participants. The next three most common challenges were staff compliance with policies and procedures, legacy technology, and patch/vulnerability management. Staff compliance issues can stem from many things including lack of technical expertise or training programs. Legacy technology upgrades and patch/vulnerability management can be very pricey and may require a pause on operations. It appears as though all the most common problems revolve around money and time. While budget may not be an issue for all of these organizations, it certainly is a shared problem among many (Healthcare Information and Management Systems Society, 2021).

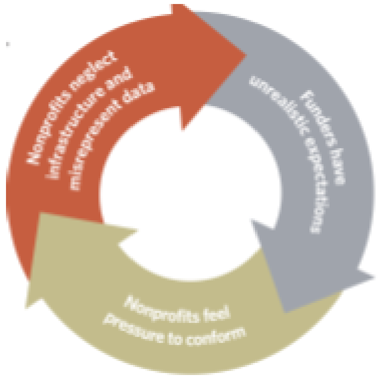
Nonprofits neglect infrastructure and misrepresent data
Funders have unrealistic expectations
Nonprofits feel pressure to conform

Figure 1: The Nonprofit Starvation Cycle: A phenomenon within nonprofit organizations that can explain the difficulties in acquiring adequate funding (Gregory & Howard, 2009).

Sufficient funds can be difficult to acquire for nonprofit organizations. Gregory and Howard (2009), in an article written for the Stanford Social Innovation Review, have identified a "starvation cycle" in nonprofits (p. 50). As seen in Figure 1, the cycle begins with the funders' lack of knowledge and unfeasible expectations about the costs of operating a nonprofit. As a result, the nonprofit organizations are pressured to meet these unrealistic expectations and either skimp on overhead or hide spending to give the appearance of doing more with less. This image of low spending gives the funders confidence in their unrealistic expectations, finishing the cycle that, as Gregory and Howard (2009) say, "slowly starves nonprofits" (p. 50). Nearly half of all 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 (American Hospital Association, 2022). This research focuses on nonprofit healthcare organizations that are situated at a critical juncture where they are the most susceptible and targeted, while having the least resources to fix their vulnerabilities.

The question this research is trying to answer is: How can large nonprofit healthcare organizations protect themselves from cyber attacks without overspending or halting operations? This paper aims to provide and explain recommendations to mend the issue and protect these organizations as the threats continue to increase. The research will support the idea that the problem is not a lack of existing secure technologies, but rather a lack of implementation and communication in the nonprofit healthcare sector. Through working on personalized technology for nonprofit organization Meals on Wheels, I saw first hand how much modern technology can improve a nonprofit organization that has been using outdated technology. Every component of the technology was readily available and the entire platform was initially built by a single person, but nobody had done it yet. Not only can new technologies improve efficiency and organization within a nonprofit, but it can also improve their security by ditching legacy systems and keeping data in a single location. The technical topic addresses the benefits of using modern, personalized technologies in nonprofit organizations, while the STS research attempts to maintain the security of these systems as nonprofit healthcare organizations digitize. The connecting issue is the systemic underspending and outdated technology use in the nonprofit sector.

Given the nature of the issue and the many groups involved, this thesis will use Actor-Network Theory (ANT) as the underlying framework to understand all necessary components. French Sociologist Bruno Latour, alongside colleagues Michel Callon and John Law, are credited with founding and being the major early proponents of the theory. The underlying principle is that human and non-human actors each affect the network in different ways, but all of them are connected in a series of relationships that are always changing and impacting the overall system. (Latour, 2005). Before applying ANT, it is necessary to understand the intricacies of the actual issue that the paper attempts to solve.

UNDERSTANDING ROOT CAUSES AND WORKING TOWARDS A SOLUTION

RECENT CYBER ATTACKS

In the nonprofit sector of healthcare, one might assume that the largest organizations would be able to afford and have access to the best cybersecurity. This assumption would be false: nobody is safe from cyber attacks. CommonSpirit Health, the second largest nonprofit hospital chain in the US, experienced a security breach in the fall of 2022 that forced them to take their systems offline, which diverted ambulances, delayed critical procedures, and disrupted many other hospital functions (Starks, 2022). The size of companies does not intimidate hackers at all. In fact, as seen in Figure 2 below, the median size of companies targeted by ransomware has been on a sharp increase, as hackers can gain the most out of successful breaches on larger organizations (Healthcare Information and Management Systems Society, 2021).

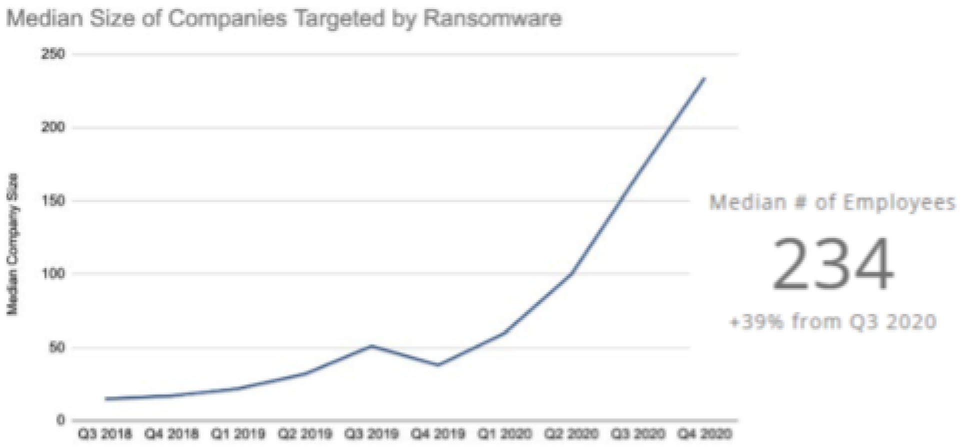

Figure 2: Median Size of Companies Targeted by Ransomware: Highlights that hackers are not afraid to target larger organizations. The data shows a trend that they are targeting larger organizations more frequently (Healthcare Information and Management Systems Society, 2021)

Outside of healthcare, in just the last year, many of the biggest, wealthiest, and most trusted software companies have also experienced breaches, including Twitter, Uber, Google, and

Apple. Even the US House of Representatives were breached in March of 2023 (Drapkin, 2023). There is a reason that these companies release software updates so frequently: nothing should be assumed to be entirely secure. New cyber attack and defense methods are discovered every day, so constant maintenance and testing is a necessity in the digital age. It is important to understand that there is no one-size-fits all solution to the issue of security and nothing is impenetrable; however, the risk and consequences of a security breach can be reduced significantly by implementing relevant security measures.

WEAK SECURITY INFRASTRUCTURE WITH KNOWN SOLUTIONS

An interesting complication in the problem is that the technology currently exists to mitigate risk, but the proper steps are not being taken to incorporate this technology. For example, in a 2018 study of 250 nonprofits across the United States, more than 50% of respondents did not require multi-factor authentication to log into online accounts (Nonprofit Technology Enterprise Network, 2018). Similarly, in a survey of 167 healthcare cybersecurity professionals, only 34% of the respondents have completely incorporated multi-factor authentication across their organization (Healthcare Information and Management Systems Society, 2021). Microsoft receives over 300 million fraudulent attempts to log into their cloud services every single day and claims multi-factor authentication can block over 99.9% of these attacks (Microsoft, 2019). Another aspect of cybersecurity is in detection and response. Technologies such as security AI and automation and extended detection and response (XDR) have been shown to drastically decrease the time it takes to identify and contain a breach. In a 2022 study done by IBM, organizations with fully deployed AI security detected and contained breaches about 74 days faster on average than those without, while organizations with XDR technologies reduced detection and containment time by 29 days on average. While these numbers can look small compared to the average of 277 days, thinking about them in the setting of a hospital can emphasize the significance (IBM, 2022). For the most part, the weak cybersecurity in nonprofit organizations does not stem from a lack of solutions, but rather from a failure to implement them. This lack of implementation is the core of the research: understanding possible reasons for not utilizing technology that has been shown to reduce the risk and mitigate consequences of cyber attacks.

CONSEQUENCES OF SECURITY FAILURE

In a healthcare environment where the stakes are much higher than other sectors, weak cybersecurity is simply unacceptable. In the case of a breach on a big social media company like Facebook or Twitter, consequences can include leaked phone numbers, identity theft, and loss of money. However, in a hospital, these consequences can very easily result in downed systems and delay of critical treatment, which can ultimately lead to death. In one 2019 instance reported by NBC News, a hospital in Alabama was sued after a baby died as a result of botched care during the delivery of the child. The baby was born with some complications, as the umbilical cord had become wrapped around her neck. However, the computer systems were down as a result of a cyber attack, so critical information about the baby’s condition, such as heart rate, could not be gathered. Had the obstetrician had this information, a cesarean section could have been performed and allowed the umbilical cord to be removed from the baby’s neck much faster. Due to lack of oxygen, the baby developed life-threatening brain damage and subsequently died nine months later. Without the computer systems, there was no way to know that the cord was wrapped around the baby prior to delivery. In this instance, the hospital stayed open and operating during a security breach, which ultimately led to the death of a baby (Collier, 2021). The alternative would be to send patients to a different hospital during a breach or system outage, but this does not always fix the issue. In 2020, a woman died in Germany after receiving delayed treatment due to a cyber attack. The closest hospital to her was experiencing a security breach resulting in loss of services, so she was turned away and rerouted to the next closest facility. As a result, her treatment was delayed by an entire hour, which can be all it takes for a situation to turn deadly (Ralston, 2020). In a survey done by the Ponemon Institute, a think tank in Washington, D.C., of 600 IT professionals working in healthcare facilities, one in four claimed ransomware attacks were directly linked to increased mortality rates at their organizations (Collier, 2022). There is no reason that these healthcare organizations should be held to a security standard any lower than the top technology companies; if anything they should be held to a higher standard given the severity of the risks.

STS FRAMEWORK: ACTOR NETWORK THEORY

Applying Actor-Network Theory to the issue of inadequate cybersecurity in nonprofit healthcare organizations, we first have to define our actors, both human and non-human (Latour, 2005). On the human side, we have entities such as the nonprofit healthcare management staff, donors, hackers, medical device manufacturers, and IT professionals. On the non-human end, the primary actors are legacy systems, modern systems, medical devices, budget, and software vulnerabilities. All of these are connected to each other in various ways and these connections have an impact on the overall system, as visualized in Figure 3 below. The relationships in the Actor-Network from Figure 3 fall into three major categories: business, engineering, and technology.

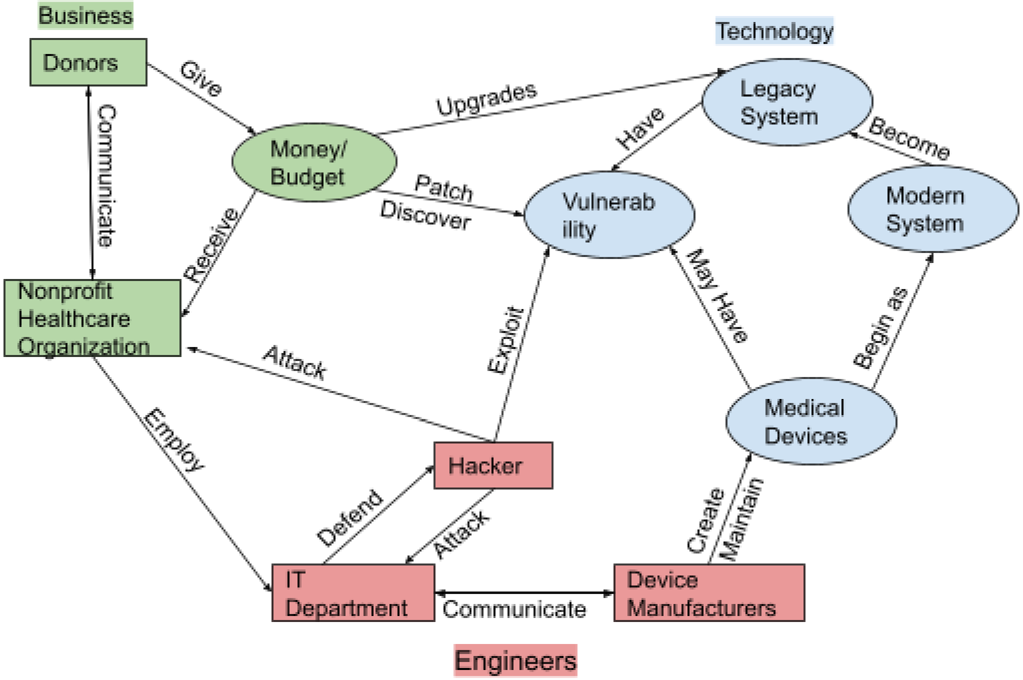

Figure 3: Actor Network Model: Proposed solution to inadequate cybersecurity in nonprofit healthcare organization derived from analysis of relationships between human and non-human entities in the system (Israel, 2023).

THE BUSINESS AND FINANCES

Donors and healthcare management staff have a very important relationship because a majority of the root causes for poor cybersecurity involve money. With infinite funds, there would be many ways to reduce the threat of data breaches, including upgrading security solutions, attracting technical experts, and acquiring new security solutions (Healthcare and Information Management Systems Society, 2021). As discussed earlier, the nonprofit starvation cycle can severely limit an organization’s ability to perform maintenance, testing, and patches (Gregory & Howard, 2009). Nonprofits need adequate funds to be allocated to the organization to support routine system maintenance, testing, and security patching. The donors hold most of the power (money) in this relationship, but it is not entirely their responsibility to fix the issue.

The main obstacle in this relationship is highlighted by a quote from a nonprofit CEO, Ben Paul, in Gregory and Howard's (2009) article: "Donor's don't want to pay for an organization's rent, or phone bill, or stamps, but those are essential components of everyday work" (p. 53). Naturally, donors want to save money where they can, but at the same time there are many minor costs associated with running a nonprofit that add up and someone has to pay them.

THE ENGINEERS

There are several engineers in this system: the hackers, medical device manufacturers, and IT professionals. In Rundle's 2023 article, he reports that in many hospitals, different medical devices often have different manufacturers, so the software used can vary drastically across devices. The technology used in hospitals is very diverse, including older information systems, cloud systems, and internet-connected medical devices. The job of the IT department is made more difficult by this diversity, as instead of having to secure a single system from a single manufacturer, they have to manage many different systems from all different sources. This in turn forces the IT department to entrust third party software providers with certain functions of the devices, which can include security (Rundle, 2023). In cybersecurity, breaching one part of the whole system can make it significantly easier to attack other parts. The only solution in the current system is for the hospital's internal security team, if they even have one, to discover every single vulnerability on their own, which is unrealistic. Chief Information Security Officer Rob Suarez of medical device manufacturer Becton Dickinson & Co. suggests greater transparency about vulnerabilities and an abandonment of legacy systems and equipment would help to combat the problem (Rundle, 2023).

THE TECHNOLOGY

In the technology aspect of the system, a key relationship to look at is use of legacy systems and its connection to budget and software vulnerabilities. A legacy system is any outdated software or hardware that is no longer maintained by the manufacturer. For all legacy systems, there was a point in time when that was actually the modern system. As technology develops, modern systems become outdated and unsupported, leading to their new legacy status. Using legacy systems will likely increase the risk of cyber attacks, as legacy systems do not have ongoing security maintenance and support. However, making the switch from legacy systems to modern systems can require a sizable investment of time and money (Grensing-Pophal, 2021). These upgrades can be thought of the same as rewiring a house. The owners would have to pay for the new hardware and the installation. During the installation, they might not have access to electricity. There may also be new switches or controls that they have to learn. Upgrading the core systems of an organization is no different, as it often requires operational downtime, re-training staff, and an investment into the newer technology. However, the incentives to upgrade legacy systems include increased efficiency, better security, and the potential for expanded operations. Modern technologies have shown massive potential to greatly increase the capabilities of any organization and can reduce many of the extra costs from the limits of legacy systems (Grensing-Pophal, 2021). As vice president of emerging tech content at O'Reilly Media, Mike Loukides, puts it, "Legacy systems are frequently inflexible, and inflexibility has a way of costing a business money. Lost money means lost opportunities" (Grensing-Pophal, 2021, p. 1). In this situation, we circle back to the donor and management relationship, where the power to initiate upgrades from legacy systems is split between them. The money to perform technology maintenance and upgrades will not be given if donors are unaware of or do not understand the problem with the current systems. If nonprofits can show donors that an investment into upgrading legacy systems will actually result in less spending overall, that could go a long way in fixing the budget problem.

ACTOR NETWORK THEORY TAKEAWAYS

As an overall reflection of the actor network theory application, there are some clear trends that have been brought to light. Three core areas in the network have been identified: business, engineering, and technology. The business side of things involves the discussed relationship between the donors and management staff. Increased funds and better allocation of budget can resolve many of the issues of the other two areas. Next is the engineering, which involves the relationship between the software developers, IT departments, and hackers. The software developers and IT departments need to communicate in order for the products to be effective, efficient, and safe from hackers. The final identified area is the technology used by these organizations, which needs to be modernized, tested, and understood. Without these three things, the technology used will be vulnerable to security breaches and possibly inefficient. It is important to note that the technology needed does currently exist, the issue lies more in implementation of the technology.

COMBATTING THE PROBLEM

MEDICAL DEVICE MANUFACTURERS

Progress has been made over the last few years, but this thesis aims to emphasize that there is still more to be done. In recent years, there has been a call from hospitals and the government to hold medical-device manufacturers more accountable and increase security in their products (Rundle, 2023). In Rundle's (2023) *Wall Street Journal* article, he notes that chief information security officer Jesse Kinser of healthcare organization LifeOmic Holdings LLC has seen many device manufacturers try to "bolt security on after the fact", but believes they are changing their ways and have acknowledged that this is unacceptable (p. 1). Kinser calls for the manufacturers to realize that the security and effectiveness of their products directly impacts the lives of the patients. Rundle also mentions that the new Omnibus Spending bill has helped this push, giving the FDA power to set minimum security requirements for medical device manufacturers. In addition, the International Medical Device Regulators Forum is working to develop standards for transparency about product life cycles and a model of shared responsibility for legacy system users (Rundle, 2023).

NONPROFITS AND DONORS

As identified by Gregory and Howard in their 2009 Stanford Social Innovation Review article, potential solutions to the nonprofit starvation cycle include open and honest communication between nonprofits and their funders. They believe this could lead to more realistic expectations and a reevaluation of the costs of running a nonprofit organization. Increased funds could lead to increased technical expertise in nonprofits and legacy systems could finally be upgraded to more efficient, secure systems. Even in 2009, Gregory and Howard identified an organization in their study which yielded an extra $350,000 off of a single investment in improving technological infrastructure, as it gave employees more time to perform other work and improved overall efficiency (Gregory & Howard, 2009). Weak cybersecurity comes with outdated technological systems, but improving those systems can have other benefits outside the realm of cybersecurity. There is a two-way argument to be made for upgrading and modernizing the systems used by nonprofit healthcare organizations. Modernized technology can improve the efficiency and operational capabilities (Sevetri, 2020), while failure to upgrade technology increases risk for security breaches that bring severe, life-threatening consequences. The responsibility falls on nonprofits to show both sides of this argument to their donors, but it then moves to the donors to listen.

SUMMARY OF RECOMMENDATIONS

It is necessary to understand what success of a solution would look like to gauge progress in the right direction. Once steps have been taken to strengthen cybersecurity in nonprofit healthcare organizations, data will be crucial in determining the effectiveness of said steps. The ultimate goal is to have zero successful security breaches, but this is unrealistic, so the key sign of progress will be a downward trend. A massive part of this is a decrease in legacy system usage, which could actually get down to zero if the organizations are able to perform routine upgrades and maintenance. Additionally, an increase in specific security measures like multi-factor authentication, staff training programs, and patch/vulnerability management would further decrease the chances that an attack is successful. Many of these organizations already know that they need to move away from legacy systems and increase use of security tools, yet they cannot do anything about it because, as a healthcare cybersecurity professional in Jalali and Kaiser's 2018 study puts it, "healthcare doesn't get paid very much, so revenue doesn't go towards cybersecurity" (p. 1). An increase in a dedicated cybersecurity budget would be a huge step in combating the issue and would create opportunities to implement the suggested technical solutions. In order for the budget to increase, the organizations must have enough funds to support all of their other operations and expenses. As Gregory and Howard (2009) argue, this can be made possible through an increase in transparency and communication between nonprofit healthcare organizations, donors, and medical device manufacturers. The organizations need to stand up for themselves by being honest about their operational costs and showing donors that they cannot do more with less. Donors should take this honesty and communication to set a more realistic expectation of what it costs to run such an organization. Nonprofits cannot simply ask for more money, but should instead prove to donors that they need more money. This will require effort from the organizations to understand their operational costs at a deeper level (Gregory & Howard, 2009). As for the medical device manufacturers, there is a need for increased transparency about product life cycles and responsibility for the security of their products (Rundle, 2023). Budget is at the root of all the issues, but it is heavily reliant upon honest and open communication between involved parties. Therefore, the first step in breaking the starvation cycle and solving the issue of inadequate cybersecurity in these organizations should be increased communication and transparency.

FUTURE WORK

One of the hardest parts of this research has been the unavailability of extremely recent data. Most of the statistics about the organizations in this research have come from studies done from 2019-2021. It would definitely be interesting to compare this data with an updated 2022-2023 version of similar categories, especially since most of the data in this research contains the Covid-19 years. Many healthcare organizations were unprepared and had to make quick changes to their technology and organizational structure during this time, which could have temporarily weakened their security. Perhaps some of the issues discussed, like multi-factor authentication for example, have since been implemented in greater numbers. While it would be helpful to see which goals are being met, the more crucial information would be which goals have seen a lack of or reverse progress. That would be a focus of an extension to this research. Analyzing the problems that are not being addressed or getting worse would be extremely helpful in uncovering more root causes. In addition, more input from various people within these organizations would be crucial to understanding the problems. A conversation between donors and organization management about the starvation cycle would be very helpful in identifying any issues that may have been overlooked by this paper.

FINAL WORDS

While some of the recommendations in this paper would take more work, the first step is simple: be transparent and communicate more. This research highlighted many of the consequences and intricacies of the issue, but there is no harm in taking that first step. This is not to say that honest and open communication is an easy feat either, as it will require effort on all parties to improve. The connection between cybersecurity strength and budget is clear, so is the link between communication and budget. People are dying and having their medical records stolen and this paper is simply asking for there to be an open conversation about it. Opening the dialogue will start to unravel the complexities of the issue and show clear paths to technical solutions.

REFERENCES

American Hospital Association. (2022). Fast Facts on U.S. Hospitals, 2022. *American Hospital Association*. https://www.aha.org/statistics/fast-facts-us-hospitals.

Brewster, Thomas. (2022 February 23). Hacker's sell backdoors into a $2 billion nonprofit, a Californian hospital, and Michigan government. *Forbes*. 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.

Collier, Kevin. (2021 September 30). Baby died because of ransomware attack on hospital, suit says. *NBC News*. https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465.

Collier, Kevin. (2022 September 8). Cyberattacks against U.S. hospitals mean higher mortality rates, study finds. *NBC News*. https://www.nbcnews.com/tech/security/cyberattacks-us-hospitals-mean-higher-mortality-rates-study-finds-rcna46697.

Drapkin, Aaron. (2023 March 28). Data breaches that have happened in 2022 and 2023 so far. *Tech.co*. https://tech.co/news/data-breaches-updated-list.

Fine, Allison, & Kanter, Beth. (2021 December 09). How smart tech is transforming nonprofits. *Harvard Business Review.* 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.

Gregory, Ann Goggins, & Howard, Don. (2009). The Nonprofit Starvation Cycle. *Stanford Social Innovation Review*, 7(4), 49–53. https://doi.org/10.48558/6K3V-0Q70.

Grensing-Pophal, Lin. (2021 July 29). Letting Go of Legacy Systems. *Society for Human Resource Management*. https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/letting-go-legacy-systems-hr-tech.aspx.

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

Hulshof-Schmidt, Robert. (2018 November). State of Nonprofit Cybersecurity. *The Nonprofit Technology Enterprise Network.* https://word.nten.org/wp-content/uploads/2018/11/Cybersecurityreport2018NTEN.pdf.

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

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

Israel, Benjamin (2023 March). Actor Network Model: Proposed solution to inadequate cybersecurity in nonprofit healthcare organizations derived from analysis of relationships between human and non-human entities in the system.

Jalali, Mohammad S & Kaiser, Jessica P. (2018 May). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5). doi:10.2196/10059.

Latour, Bruno. (2005). Reassembling the Social: An Introduction to Actor-Network Theory. *Oxford University Press Inc.*

Malone, Leslie. (2019 December 30). 2019 U.S. population estimates continue to show nation's growth is slowing. *United States Census Bureau*. https://www.census.gov/newsroom/press-releases/2019/popest-nation.html.

Maynes, Melanie. (2019 August 20). One simple action you can take to prevent 99.9 percent of attacks on your accounts. *Microsoft*. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/.

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. *Institute for Critical Infrastructure Technology*. https://icitech.org/wp-content/uploads/2017/02/ICIT-Brif-Cybersecurity-and-NGOs.pdf.

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

Ralston, William. (2020 November 11). The untold story of a cyberattack, a hospital and a dying woman. *Wired*. https://www.wired.co.uk/article/ransomware-hospital-death-germany.

Rundle, James. (2023, February 13). Medical-device makers face push to protect their wares from hacks. *Wall Street Journal.* https://www.wsj.com/articles/medical-device-makers-face-push-to-protect-their-wares-from-hacks-32e84445#:~:text=Mounting%20cyberattacks%20against%20hospitals%20and,be%20in%20operation%20for%20decades.

Seh, Adil Hussain & Zarour, Mohammed & Alenezi, Mamdouh & Sarkar, Amal Krishna & Agrawal, Alka & Kumar, Rajeev & Khan, Raees Ahmad. (2020 May 13). Healthcare Data Breaches: Insights and Implications. *Healthcare, 8(2).* https://doi.org/10.3390/healthcare8020133.

Starks, Tim. (2022, October 6). An ‘unprecedented’ hospital system hack disrupts health-care services. *The Washington Post*. https://www.washingtonpost.com/politics/2022/10/06/an-unprecedented-hospital-system-hack-disrupts-health-care-services/.

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.* 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*. https://www.forbes.com/sites/forbesbusinesscouncil/2020/11/12/how-technology-can-help-nonprofits-prove-their-value-to-donors/?sh=750179bc21d8.