Healthcare and Cybersecurity: Taking a Zero Trust Approach

George Vukotich

Medical Education - Patient Safety Leadership, University of Illinois Chicago, Chicago, IL, USA.

Health Services Insights
Volume 16: 1–5

DOI: 10.1177/11786329231187826

ABSTRACT: This article looks at Healthcare and the issues that exist with current cybersecurity measures. As hacks including ransomware attacks become more commonplace it is important to provide safeguards to protect the data of the patients and the healthcare organization. Examples of breaches are looked at with insights on how they happened and what could have been done to prevent them. A newer approach known as Zero-Trust which addresses 7 key areas to protect is reviewed and shown how its applicability to healthcare can make a difference in protecting individuals and organizations.

KEYWORDS: Cybersecurity, Zero Trust, healthcare risk, security, data protection

RECEIVED: April 8, 2023. **ACCEPTED:** June 26, 2023.

TYPE: Methodology

FUNDING: The author received no financial support for the research, authorship, and/or publication of this article.

DECLARATION OF CONFLICTING INTERESTS: The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

CORRESPONDING AUTHOR: George Vukotich, Medical Education - Patient Safety Leadership, University of Illinois Chicago, 7765 W. North Avenue, Chicago, IL 60305, USA.
Emails: gvukotich@gmail.com, vukotich@uic.edu

Introduction

The American Hospital Association[1] advises senior hospital leaders not to view cybersecurity as purely a technical issue falling solely under the domain of IT departments. Rather it states that it is critical to view cybersecurity as a patient safety, enterprise risk and strategic priority, and to instill protection into the hospital's overall enterprise, risk-management, governance, and business-continuity framework.

According to the National Library of Medicine[2] one challenge that healthcare organizations have is that many of them lack the type of cybersecurity capability that is needed to defend against hackers and others looking to gain access to healthcare systems due to the complexity, cost, and knowledge required to deal with the continuing changes and approaches those hackers use.

Health care organizations are particularly vulnerable to cyberattacks due to their high propensity to pay a ransom. Patient records possess information of high monetary value to cyber thieves and nation-state actors. The targeted data includes patients' protected health information (PHI), financial information like credit card and bank account numbers, personally identifying information (PII) such as Social Security numbers, and intellectual property related to medical research and innovation. Because healthcare providers can't fully serve patients without access to records and monitoring digital medical tools connected to health networks, they often yield to demands to put patients first. It is important to note, however, that not all organizations that pay a ransom get their data back. According to Info-Tech[3] today "Most healthcare security architectures are perimeter-based and complex to manage." This leaves only the point of entry as the barrier to be breached. Often attacks (0-day) are already in a system waiting for a trigger to set them off.

As the healthcare world becomes more global and as hackers attack from more parts of the globe protecting data and systems is becoming a more complicated process. Patients traveling and relocating to other parts of the world require their data be made available to local providers. Researchers working on medical breakthroughs collaborating with partners globally need to share data. Various governments have created their own privacy laws making data access a more complicated process as well.[4]

Issues

Stolen health records may sell for up to 10 times more than stolen credit card numbers on the dark web.[1] Unfortunately, the bad news does not stop there for health care organizations—the cost to remediate a breach in health care is almost 3 times that of other industries—averaging $408 per stolen health care record versus $148 per stolen non-health record.

Currently many organizations take a network perimeter approach to cybersecurity. This approach basically looks to stop intruders before they get into a network, but as more ways to penetrate a network have come about this strategy alone has become outdated. Today a new approach known as zero-trust is becoming the key to minimizing the impact hackers can have. Zero-trust not only looks at the perimeter of a network but also looks at the components; systems, users, data, etc. as points to protect.

As healthcare organizations look to take advantage of technology to become more effective in how they do business more avenues of attack are open to those looking to penetrate healthcare systems. There are many examples where third parties have been penetrated with the end goal to not access the system of the small business but to hack into the larger organization they are connected to and work with. As a well-documented case from the commercial space shows, Target Stores[5] became compromised by hackers using the login credentials of a HVAC company that did work for Target. The hackers originally used their connection to download customer data. This was the starting point but once the hackers were in, they were able to access more data and to expand into other systems.

While the hackers in the Target Stores case gained access to the systems, they did not immediately cause noticeable disruption. They started out by first testing their data-stealing malware on a small number of cash registers. After determining that their software was embedded and could give them access, they uploaded their malware to most of Target Stores POS (point of sale) systems. This happened from November 27 to December 15, 2013. The hackers then used the malware to download data from about 40 million debit and credit cards.

What is interesting in this case is that Target missed several internal alerts and only discovered their systems were breached when contacted by the Department of Justice. Their monitoring software known as FireEye alerted Target staff in Bangalore, India, who in turn notified staff at headquarters in Minneapolis but no action was immediately taken. By the time Target reacted, the hackers had not only gained access to the Target system but were able to download data that would let them compromise other systems which impacted tens of thousands of individual's financial records.

More recently the largest publicly disclosed cyber-attack against U.S. infrastructure happened in the Colonial Pipeline[6] case. The attack has been identified as coming from a group known as Dark Side which accessed and stole 100 gigabytes of data within a 2-hour window. While the actual pipelines were not compromised, the hackers infected the Colonial Pipeline IT network with ransomware that affected many of the company's business systems.

What is interesting in the Colonial Pipeline case is that even though secure measures such as using a VPN (Virtual Private Network—which extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network) an employee used a common password they had used to connect to other programs and in an attack on a different network that password was found. The hackers used it to crack into the Colonial Pipeline network even though it had a higher level of security. User error, mistakes, and carelessness are still the number 1 cause allowing systems to be breached.

While many U.S. government agencies including the DoD have been hacked information related to the hacks is generally not openly shared. Possibly for fear that describing how one hack worked could lead to similar attacks. One software company known as SolarWinds that claims 498 of the Fortune 500 companies in addition to all branches of the military as clients was itself the channel that led to a number of breaches.[7] Since its software is used by all these organizations the hackers were able to gain access to all its software customers.

Once hackers have penetrated a system it is often harder to detect and eliminate them from the system than if they were denied access to start with. There are many ways hackers can get into a system.

Healthcare organizations with all they have to focus on to do their business often do not have the time, money, or resources to keep hackers from attacking their systems and if they do it is usually only to prevent the less sophisticated hacker. In the past many attempts at hacking were tied to crypto kiddies or those that were unskilled and simply wanted to see what they could get access to an organization's systems. In some cases, they would cause damage but much of what were amateurish pranks have today been replaced with cyber-attacks that are more financially motivated with the ransomware type.

Ransomware[8] is where hackers access the data on an organization's computer systems and encrypt it so that the organization cannot access it without an encryption key. In order to get access to the data again the hackers require the organization to pay a ransom, usually in a cryptocurrency such as bitcoin so that it cannot easily be found. Often these attacks can come from anywhere in the world by connecting through the internet. Often hackers based in other countries and are hard to track and even if they can be tracked there is not much that can be done if the attacks come from places like Russia, China, or Iran. The ransom money is also requested in cryptocurrency like bitcoin, so the normal banking system is bypassed. Some organizations can try to recover from the attack by bringing backed up data but even here the systems have been infected and bringing back data alone does not solve the problem. The code that spread the ransomware must be found and eliminated. In some cases, the software is what is known as a worm virus, and it quickly replicates throughout the organization's network disabling all applications.

As of today, the current level of preparedness to deal with cyberattacks is not very strong within most Healthcare organizations and the number of ways or attack vectors that can be used to access systems to plant bugs is increasing. When you consider how access is gained, often through third-party business partners such as small businesses, many of which are not well prepared should a breach happen. As more applications come online, the challenges become even greater. Infrastructure and systems are only getting more interconnected and interdependent which increases the ways a hacker can get access. This is known as an increasingly less protected attack surface. As new technologies come into play, the risks become greater. One area in particular, is what is known as the Internet of Things (IoT) where sensors and other devices like video cameras are added to a communication network. While effective in transmitting data most of these devices have not been designed to resist attempts to breach their security. In addition to the financial loss, public safety, and negative consequences to our supply chain it can put many lives at risk.

Information about many attacks is never shared but we can learn from some of the more publicized events like the one that happened in Atlanta, Georgia in 2018.[9] The attack there shut down many of the city's agencies including the court system,

water department, and traffic department. Keep in mind cities often have 30 to 40 different agencies that can be impacted by a single attack. In this case the Iranian hackers behind the attack demanded $51,000 in Bitcoin which the city indicated they did not pay. The city spent $17M in costs related to the hack to get back to up and running. Clearly deterring and preventing hacks is much cheaper than paying the costs to recover from them. Some might say why not just pay the ransom, but there is no guarantee that doing so will prevent further attacks and may even encourage others.

In Healthcare, payment systems add to the complexity of protecting data.[10] Not just in the U.S. but with each country having its own approach to billing, reimbursement, and payments. Reimbursement methods alone include everything from salary reimbursement, fee-for-service, capitation, nationalization, pay-for-performance, health-savings-accounts, and a number of alternative systems which can not only be confusing to the public but open the number of areas hackers can attack. Most countries have mixed systems that require greater amounts of payment transfer between systems. Social, political, and economic factors drive political decisions and often add to the complexity to meet legal requirements. All these requirements cause more data to be transferred to more systems in more places. Application programming interfaces which link systems to each other are also being compromised more often.

While there have been questions related to understanding and making sense of fairness in using algorithms[11] as users become more familiar with how the algorithms work the level of trust in the tools they use becomes greater as well. Shin[12] noted that when users get the sense that algorithmic recommendations are optimized to a user's preferences, they consider the service more valuable and feel more trusting of the content. Users perceive the algorithms as credible and reliable as long as they perceive the recommended items or content as high-quality choices for their specific needs.

While not new, there is an increased focus on taking a "zero trust" approach to data and information and how it is accessed and by who. The Department of Defense (DoD) is taking a lead in developing this strategy and can be a model for healthcare as well.

User Perspective

As cybersecurity tools continue to rely more on artificial intelligence, tools from a user's perspective themselves determine to what degree they will implement them. Areas related to privacy of data monitored, the security around data in the various states of; rest, use, and transport, along with the risk of data theft are often considered in the protection approaches. User awareness shapes user behavior.

The use of artificial intelligence has also led to concerns about data privacy and information disclosure from the perspective of data which needs to be uses to train the machine learning algorithms.[13] Misinformation used in the training of algorithms can often cause more problems than it solves. Focusing on data alone provided the impetus to go beyond monitoring only data files in the security process.

Alternatives

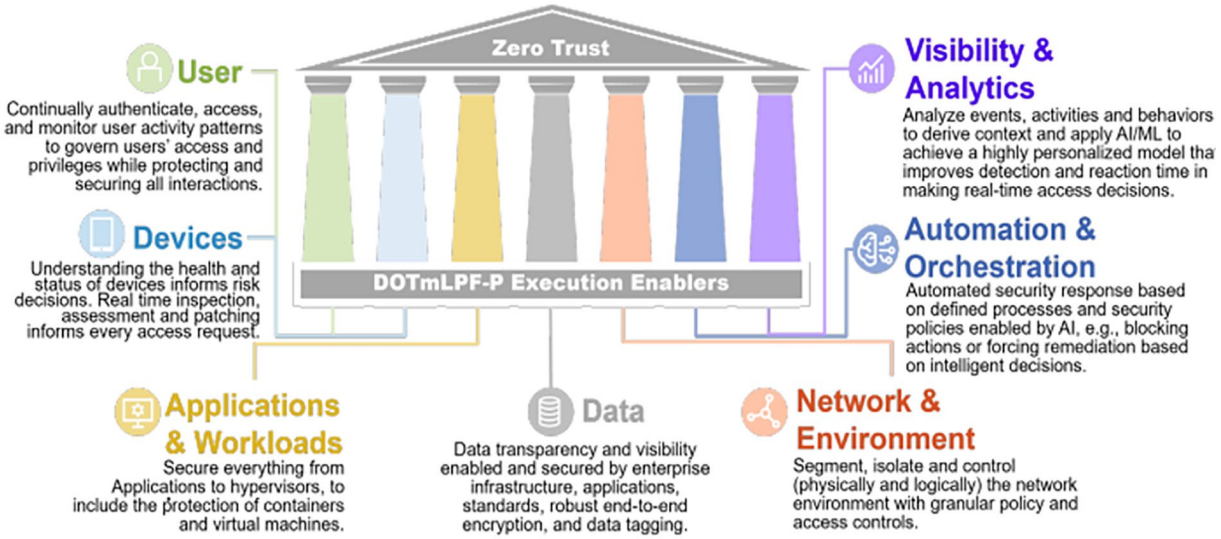
While the increasing number of attacks continues to grow at an exponential rate many new technologies offer promise as well as the potential for greater risk. Blockchain technology which itself is experiencing exponential growth, and in particular the aspects of blockchain technology related to cryptocurrency provides us with areas to consider as well. Blockchains provide decentralize, peer-to-peer security for all transactions, yet many blockchain security vulnerabilities remain. How to ensure privacy and security of data is again the focus.[14] This uncertainty is the most critical challenge for the sustainable development.

Artificial Intelligence (AI) is another area that is currently being utilized to identify patterns and trends and will continue to grow in importance to supporting cybersecurity measures.[15] AI can help by curating threat intelligence from millions of research papers, blogs, and news stories. The machine learning and natural language processing areas of AI can provide increasingly rapid insights to identify actual threats as compared to hoaxes and can allow for drastically reduce response times in responding to identified threats.

A number of other technologies have also been addressed, but there is one that goes beyond just trying to protect data and perimeter security. Known as Zero Trust it takes a comprehensive approach to protecting an organization. While the tools related to AI and blockchain can be used in cybersecurity it goes beyond just checking perimeter entry or data analysis.

Zero Trust[16] is the term for an "evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." At its core, ZT assumes no implicit trust is granted to assets or users based solely on their physical or network location (ie, local area networks vs the Internet) or asset ownership (enterprise or personally owned).[17] This shift in philosophy is a significant change in legacy authentication and security mechanisms. It also represents a major cultural change that stakeholders throughout the DoD ZT Ecosystem, including the Defense Industrial Base (DIB), will need to embrace and execute beginning with FY2023 through FY2027 and in the future.

From the DoD Zero Trust Strategy document created November 7, 2022, it looks at the Seven Pillars of Zero Trust. Further detail can be found in the 7 tenets of zero trust outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207.



User: At the user level the focus is on continual authentication, access, and monitoring of user activity patterns to govern access and privileges. Parameters include password authentication and multi-factor authentication which can include dialing a user's cell phone, using some type biometric such as a fingerprint, or even monitoring where a person is at when trying to access the system.

Devices: The physical device a person would use to access the system. It could have built in memory, where the device is located (GPS), or access management software. Tracking is done real-time and software patches can be applied as they become available.

Applications & Workloads: The actual applications that are used in accessing the data. Taking care that only certain users have login access at the application level. It may also have differing levels of access depending on the need of the specific user. Keep in mind user IDs should be for individual users not groups of users. Group access can cause issues in identifying specific users and what they accessed. This includes monitoring and protection of containers and virtual machines.

Data: The data itself is where the value is and is generally in 1 of 3 stages where it could possibly be accessed. Data at rest or in storage. Here the key is to ensure that no one can access and take or manipulate the data. Data in transit through a network. Here the key is to ensure that that the data cannot be read or interpreted. A strong encryption set can help protect the data. The third area is data in use in an actual application. Here the key is to make sure the data has integrity.

Network & Environment: Also known as the transport level. The focus here is on protecting data in motion and can include approaches that include encryption and protect the data from being accessed while it is moving through networks.

Automation & Orchestration: Automated security response based on defined processes and security policies. Often enable by artificial intelligence that could block or force remediation based on intelligent algorithms in the decision process.

Visibility & Analytics: Monitor and analyze events, activities, and behaviors to derive context and apply artificial intelligence and matching learning approaches to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Limitations

While cyberattacks continue to evolve and what may be a relevant way to protect organizations and their systems today may become quickly outdated. The key is for the protectors to continue to evolve to understand what vectors are being used and how to better prevent access to systems and in those cases where access has happened preventing or stopping active attacks and recognizing and rendering harmless inactive code waiting for a trigger to launch an attack. While there is no one way to prevent attacks today. Zero Trust brings a multipronged approach to the problem.

Conclusion

In addition to the various areas organizations need to track who and how data is being accessed along with having effective backup and recovery processes. In my work I often ask individuals when was the last time, they conducted a data audit? Often the answer is never or only a minor subset of what should be done to protect the data of the members of the community

they are responsible for. Too often a breach is not even known for months or years after it has happened.

With the importance of healthcare data, it seems only natural that healthcare systems should consider taking a Zero Trust approach. While an educated user is the key to preventing malware from getting into a system, the tools and processes hackers are using are also getting more sophisticated. Even requiring users to set up approaches like dual factor authentication will not stop a hacker if the user clicks on the wrong type of email or goes to the wrong type of website. By focusing on a more proactive approach and bringing the aspects of Zero Trust to the healthcare industry, a first step to reducing the potential of unauthorized access can be taken.

Author Contributions

George Vukotich is the sole researcher and author of this publication.

REFERENCES

1. Riggi J. The importance of cybersecurity in protecting patient safety. Accessed December 12, 2022. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety
2. He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. *J Med Internet Res*. 2021;23:e21747.
3. Info-Tech. Navigate Zero-Trust security in healthcare. https://www.infotech.com/research/ss/navigate-zero-trust-security-in-healthcare
4. World Health Organization. Formalizing political commitment by making effective laws for universal health coverage. 2023. https://www.who.int/publications/m/item/formalizing-political-commitment-by-making-effective-laws-for-universal-health-coverage
5. Vijayan J. Target breach happened because of a basic network segmentation error. February 6, 2014. Accessed October 17, 2022. https://www.computerworld.com/article/2487425/target-breach-happened-because-of-a-basic-network-segmentation-error.html
6. Kerner SM. Colonial pipeline hack explained: everything you need to know. April 26, 2022. Accessed October 17, 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=What%20was%20the%20root%20cause,Homeland%20Security%20on%20June%208
7. SolarWinds. IT Management Software and Observability Platform. Accessed October 17, 2022. https://www.solarwinds.com/?CMP=KNC-TAD-GGL-SW_NA_X_PP_CPC_LD_EN_BRDB_TIN-X-17919228470~138273364263_g_c_solarwinds-e~613965837273~~p72463195083&s_kwcid=AL%2111508%213%216139658372 73%21e%21%21g%21%21solarwinds&ds_cid=71700000098707479&ds_agid=58700007958078559&network=g&device=c&keyword=Solarwinds&matchtype=e&creative=613965837273&feeditemid=&gclid=CjwKCAjw-rOaBhA9EiwAUkLV4oFqSuyI3vvFZMkaemlIRn79eayZlWqYMaKSWyZpDjl_Lq48cIqfmRoCz8UQAvD_BwE&gclsrc=aw.ds
8. Malware Bytes. Ransomware. https://www.malwarebytes.com/ransomware
9. Blinder A, Perlroth N. A cyberattack hobbles Atlanta, and security experts shudder. *The New York Times*. March 27, 2018. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html. Accessed November 5, 2022.
10. Britton JR. Healthcare reimbursement and quality improvement: integration using the electronic medical record comment on "fee-for-service payment–an evil practice that must be stamped out?" *Int J Health Policy Manag*. 2015;4:549-551.
11. Shin D, Lim JS, Ahmad N, Ibahrine M. Understanding user sensemaking in fairness and transparency in algorithms: algorithmic sensemaking in over-the-top platform. *AI Soc*. Published online July 3, 2022. doi:10.1007/s00146-022-01525-9
12. Shin D. Embodying algorithms, enactive artificial intelligence and the extended cognition: you can see as much as you know about algorithm. *J Inf Sci*. 2023;49:18-31.
13. Shin D, Kee KF, Shin EY. Algorithm awareness: why user awareness is critical for personal privacy in the adoption of algorithmic platforms? *Int J Inf Manag*. 2022;65:102494.
14. Shin D, Hwang Y. The effects of security and traceability of blockchain on digital affordance. *Online Inf Rev*. 2020;44:913-932.
15. Das R, Sandhane R. Artificial intelligence in cyber security. *J Phys Conf Ser*. 2021;1964:042072.
16. Department of Defense. DoD Zero Trust Strategy. November 7, 2022. Accessed December 19, 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
17. Office of Small Business Programs Department of Defense. Home. Accessed October 17, 2022. https://business.defense.gov/Work-with-us/Cybersecurity/