Zero Trust and Cybersecurity in the Industries

Suchaye Mylavarapu

Mountain House High School

ABSTRACT

This paper aims to highlight the critical importance of cybersecurity in safeguarding against the ever-evolving and sophisticated nature of cyber threats that have become the norm nowadays. It is specifically pointed out that healthcare organizations must prioritize data management and robust security measures to combat ransomware and data breaches. At the same time, the software industry faces cybersecurity challenges due to the vulnerability of interconnected systems. Organizations must take proactive steps to identify potential threats and vulnerabilities and be prepared to handle any security incidents. Additionally, companies should ensure that their employees are educated on the necessary security measures to protect their data and systems. Consequently, security and development practices, software delivery, threat management, and incident management are vital for defense against cyberattacks. To protect digital assets and data, the analysis delves into firewalls, encryption, access controls, and other cybersecurity measures. Companies should also provide training to their employees on best security practices and regularly update their systems with the latest security patches. Additionally, they should develop a security policy to ensure safe access and use of the company's digital assets. Moreover, the zero-trust concept has been introduced as an advanced cybersecurity framework that challenges traditional security frameworks. Overall, this paper hopes to emphasize the importance of cybersecurity in various industries, specifically in the. healthcare, software, and the film industries are very important in safeguarding individuals, organizations, systems, assets, and information from threats.

Introduction

The consequences of a cyber attack can be devastating, ranging from financial loss and reputational damage to personal information and infrastructure. As cyber threats continue to evolve and become increasingly sophisticated, the need for skilled cybersecurity experts grows exponentially. The term security refers to a state of protection from danger or threat. This includes a variety of measures related to protecting individuals, organizations, systems, property, and information from unauthorized access, damage, disruption, or loss. Security measures are put in place to mitigate risks by ensuring authenticity, confidentiality, availability, and reliability. For computer systems and networks, security includes protecting digital assets and data from unauthorized access, theft, or destruction. This includes implementing measures such as firewalls, encryption, access control, intrusion detection systems, and regular security updates to prevent unauthorized access, data breaches, and malware. Cybersecurity can have the potential to stop a recession, terrorist identity faking, and government system hacking.

According to Gilad David Maayan (2022), the most used cybersecurity software include IPS (Intrusion Prevent Systems), NGAV (Next Gen Antivirus), and Sandboxing. These are used for the most common threats such as viruses, malware, and data breaches. Furthermore, in common network security, SOAR (Security Orchestration and Response) technologies are used. According to Cobalt Security Magazine (2022), there are over 2,200 cyberattacks each day, which breaks down to nearly 1 cyberattack every 39 seconds. With the increasing sophistication of cyberattacks, organizations must take proactive measures to protect their systems. Business states that “Cybersecurity is no longer a “nice to have” – it’s a “need to have” for business, and it needs to be a part of your business’s budget. However, it’s important to note that cybersecurity protection isn’t purely a function of money spent.” IPS, NGAV, and Sandboxing technologies can detect and stop malicious activity before it can cause any damage. SOAR technologies can also automate the process of responding to threats, making it easier to quickly identify and mitigate any threats that may arise. We need to conduct research on cybersecurity so we can stay ahead of the evolving threats, develop more secure and safer technologies for future generations, and improve our understanding of human behaviors on the internet. Additionally, it is important to ensure that cybersecurity technologies are properly implemented and used. Regular training and testing should be conducted to ensure that all staff are aware of the latest threats and how to respond. Finally, regular audits should be conducted to ensure that the security infrastructure is up-to-date and functioning properly.

This paper helps industries find better approaches to avoid ongoing cyber threats and supports the government sector in implementing and strengthening the policies and regulations, using the necessary tools and resources to protect various industries from cyber-attacks and data breaches. Furthermore, providing a comprehensive understanding of the current cyber threats will aid and equip industries with the latest tools and techniques to stay ahead of emerging threats. This will create a more secure online environment for everyone, as well as develop a security plan to ensure that everyone is protected.

Defining Zero-Trust in Cybersecurity

The zero trust security model is a further improved model over the traditional range-based security model as it does not trust anyone within or out of the network. Typically, organizations rely on traditional perimeter defenses such as firewalls, antivirus, and secure VPNs to protect their network and data. As new threats emerge and develop, these methods are less effective. Hackers are constantly looking for new ways to penetrate these defenses, and organizations need to be able to respond quickly to new threats. To do this, they need to invest in technologies such as artificial intelligence and machine learning, which can detect and respond to threats in real time. According to the article by CrowdStrike (2023), Zero Trust always follows the principle of “never trust you, always prove it”. This means that organizations must take extra precautions to prevent any unauthorized person from gaining access to their systems, such as implementing multifactor authentication and other security measures using AI and machine learning can help organizations provide for regular monitoring of potential threats and prompt response if detected.

Jack Flynn (2022) asserted that at the end of 2022, there will be 4,145 publicly disclosed data breaches worldwide, and it takes an average of 287 days to detect and contain a major data breach. Seriously there data breaches across industries have become more apparent and the need for such effective security measures has never been greater. It turns out that AI and machine learning have the potential to detect and respond to data breaches quickly and efficiently cleaned up, reducing the impact and cost of these incidents AI and machine learning can identify patterns and anomalies in data that could indicate a data breach in progress. This allows organizations to be alerted to potential breaches and respond quickly, reducing the time it takes to detect and prevent a breach. Below is a model that shows the prioritization of how zero-trust models are used in each company for the purposes listed in the diagram. The model is designed to help organizations identify the best security measures for their needs. It also helps to prioritize resources to ensure the most effective security posture. Finally, it enables organizations to understand the impact of a security incident and take proactive measures to minimize its effects.

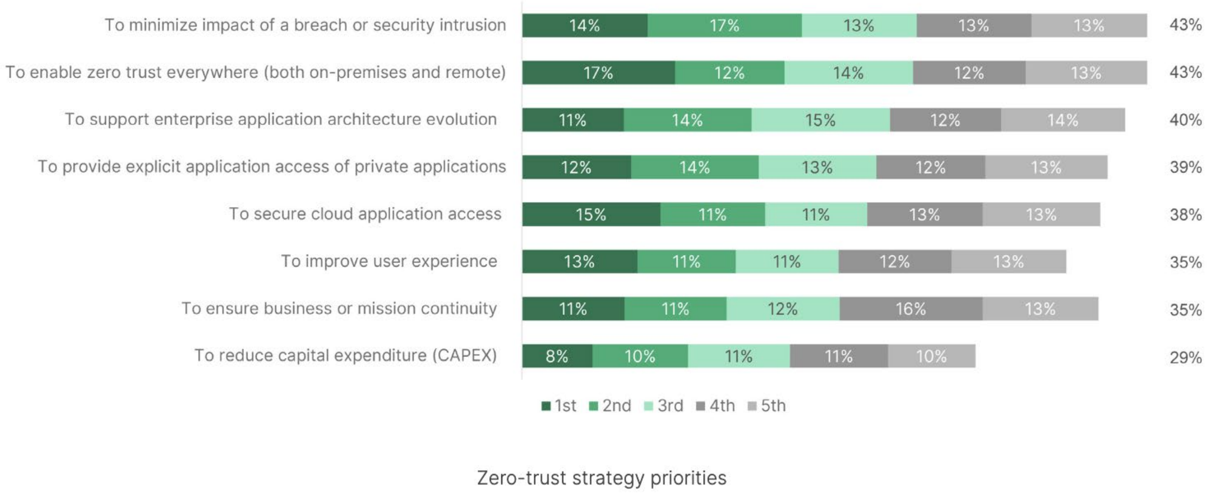

Figure 1. Zero Trust Strategy Priorities by Company Statistics (2023).

AI and machine learning can analyze data and detect anomalies that indicate a potential breach. With this information, organizations can take proactive measures to protect their data before the breach occurs. Additionally, automation can help reduce the time and effort required to respond to the breach, which can help minimize the impact and cost associated with it. AI and machine learning can analyze large amounts of data quickly and accurately, allowing organizations to identify any suspicious activities or patterns. Automation can then be used to quickly respond to any suspicious activity, such as shutting down accounts or systems or alerting the appropriate personnel. This can be done with minimal manual input, helping to reduce the cost and effort associated with responding to the breach. AI can also be used to detect potential breaches before they become a problem, allowing organizations to take preventative measures. Additionally, AI can be used to monitor networks and systems for potential threats in real-time, providing even more protection against data breaches. For example, AI-powered security tools can be used to monitor for suspicious behavior patterns that may indicate a potential data breach, such as a sudden spike in access requests to certain data or an unusual pattern of user behavior. AI-based security tools provide an invaluable layer of protection for networks and systems, helping to keep them secure from hackers and malicious software.

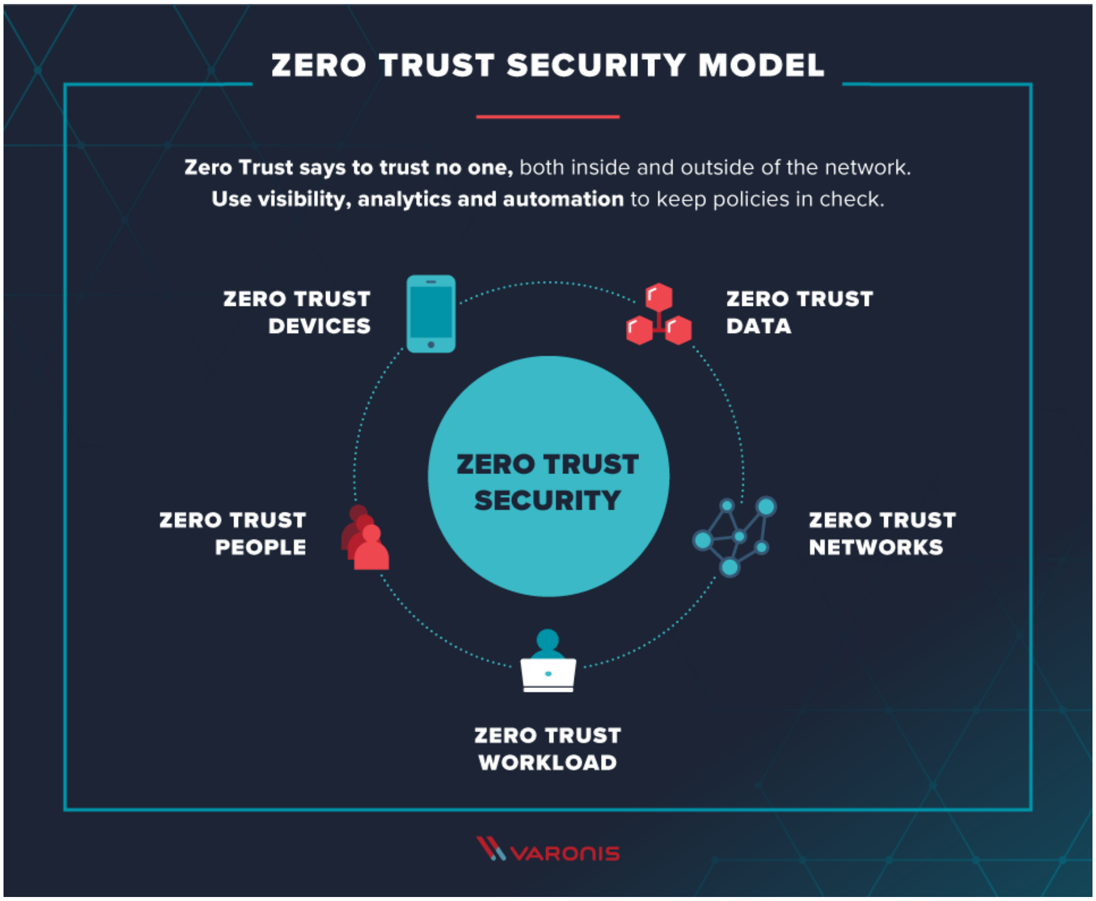
ZERO TRUST SECURITY MODEL
Zero Trust says to trust no one, both inside and outside of the network.
Use visibility, analytics and automation to keep policies in check.
ZERO TRUST DEVICES
ZERO TRUST DATA
ZERO TRUST SECURITY
ZERO TRUST PEOPLE
ZERO TRUST NETWORKS
ZERO TRUST WORKLOAD
VARONIS

Figure 2. Zero Trust Security Models (2020).

Cybersecurity in the Health Industry

One crucial industry where cybersecurity is very critical is the healthcare industry because it holds patient's sensitive information, patient's safety, and health organization's reputation, and also for health government regulatory purposes. Healthcare organizations must ensure that their data is secure and that there are measures in place to protect against cyberattacks. This includes developing secure systems, technologies, and processes that protect patient data, and implementing robust security protocols to protect against malicious actors. According to a PricewaterhouseCoopers (PWC) 2021 report, the healthcare industry is valued at 5 trillion dollars. As such, the healthcare industry is a prime target for cybercriminals looking to breach patient data and steal valuable information. With the increasing amount of healthcare data stored in digital databases, the risk of a data breach is even greater. Therefore, healthcare organizations must prioritize data security and ensure that their systems, technologies, and processes are up-to-date and secure. The most common types of attacks that occur in the healthcare industry include ransomware attacks, phishing attacks, data breaches, and supply chain attacks. Ransomware attacks are one of the common attacks because an attacker encrypts the victim's data and demands a ransom payment to decrypt it. Healthcare organizations are particularly vulnerable to ransomware attacks because they often store large amounts of sensitive data relating to the patient or the organization itself. The first ransomware attack occurred in 1989 at the World Health Organization AIDS conference in Stockholm, Sweden. Biologist Joseph Popp distributed 20,000 trojanized floppy disks at the conference (McKeon, 2022). This data is incredibly valuable for attackers and can be used to extort the organization for a ransom payment or even be sold to other attackers. Healthcare organizations often lack the resources to properly protect their data, making them an easy target for these types of attacks. Healthcare Finance states that "The cost needed to find a solution to fix breaches and to settle any civil complaints are fines from the Department of Health and Human Services Office of Civil Rights. In 2018, OCR issued 10 resolutions that totaled $28 million"(Morse, 2019).

Healthcare organizations have limited budgets and often don't have the resources to invest in IT security to prevent these types of attacks. Additionally, the cost of a data breach can be immense, as it can cause reputational damage and financial losses that can be difficult to recover from. Currently, healthcare systems are encrypting their data as much as possible so that only the data receivers will be able to view or edit the data. Below is an image of a sample privacy encryption method that is used by most healthcare providers. Encryption is the process of encoding data so that it can only be accessed by the intended recipient. Most healthcare providers use advanced encryption technologies such as AES (Advanced Encryption Standard) or RSA (Rivest–Shamir–Adleman) to protect data. By using these encryption technologies, healthcare providers can ensure that data is secure and can only be accessed by the intended recipient. Additionally, healthcare providers can also use two-factor authentication to further protect data. Two-factor authentication requires users to provide two pieces of information, such as a username and password, to access a system. This helps to ensure that only authorized users can access the data. Below is a flowchart that shows a step-by-step encryption process.

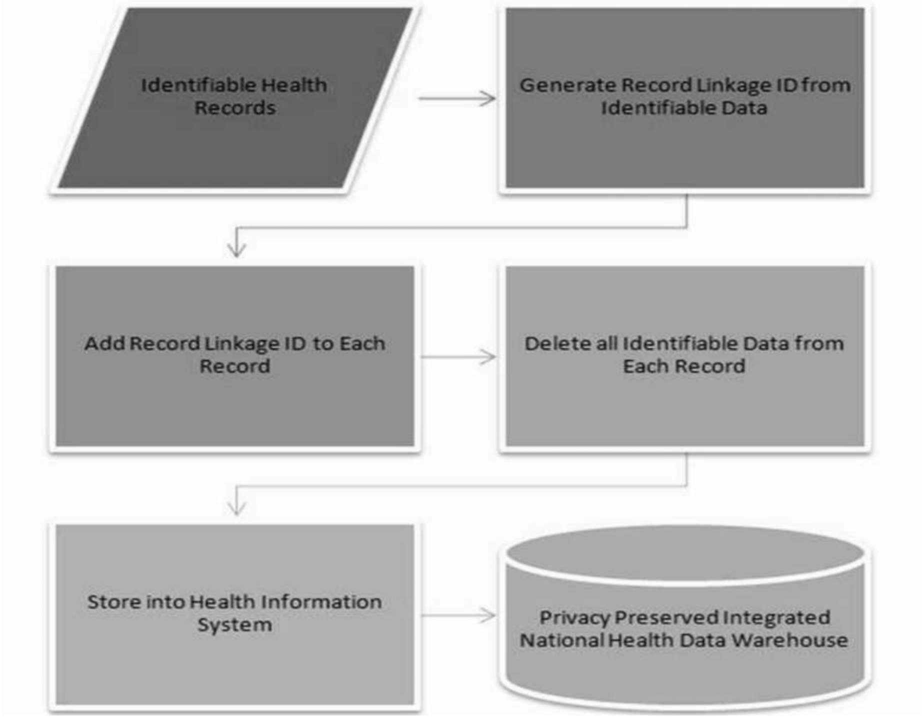
Identifiable Health Records
Generate Record Linkage ID from Identifiable Data
Add Record Linkage ID to Each Record
Delete all Identifiable Data from Each Record
Store into Health Information System
Privacy Preserved Integrated National Health Data Warehouse

Figure 3. Protection of Health Records (2016).

This encryption method ensures that the data is securely transmitted, and no one can access it without the correct key. It also ensures that any data that is stored is done in an encrypted form, making it impossible for an unauthorized user to view or edit the data. For healthcare systems to prevent future attacks, they will need to use a zero-trust network which ensures that no device is trusted and that access to resources/databases is granted on a per-request basis even if the device is running on the authorized healthcare network. For example, if a user attempts to access a healthcare database, the zero trust network would first verify the identity of the user and that the user has no malicious or virus software before providing them with access to the database even if it is a work-authorized device.

In conclusion, the healthcare industry will need to be more conscious about their online security by making sure their systems are frequently monitored and they should implement a zero-trust network.

Cybersecurity in the Software Industry

Another important industry where cybersecurity is crucial is the software industry because it is essential for protecting the data, software, and reputation of software companies. By taking steps to improve their cybersecurity posture, software companies can help mitigate the risks of cyberattacks and protect their business. This includes implementing strong authentication and access control measures, employing encryption for data security, and regularly backing up data to ensure that it is not lost in the event of an attack. Additionally, investing in cybersecurity training for employees can help to ensure that they are aware of the latest threats and how to best protect their company. According to a study conducted by Kaspersky, 52% of companies report that employees constitute the most significant weakness in terms of cybersecurity (Kaspersky Lab, 2018). The software industry is particularly vulnerable to cyber threats due to the sheer number of applications and systems that are interconnected. As such, investing in comprehensive and up-to-date cybersecurity training is a crucial step in protecting companies from the latest cyber threats. With the increasing prevalence of cyber attacks, most of which are enabled by employee negligence or mistakes, organizations must provide their employees with the knowledge and training they need to identify and protect against potential threats. Unfortunately, the prediction of cybersecurity threats in the industry is predicted to increase in the next decade as shown below in the graph.

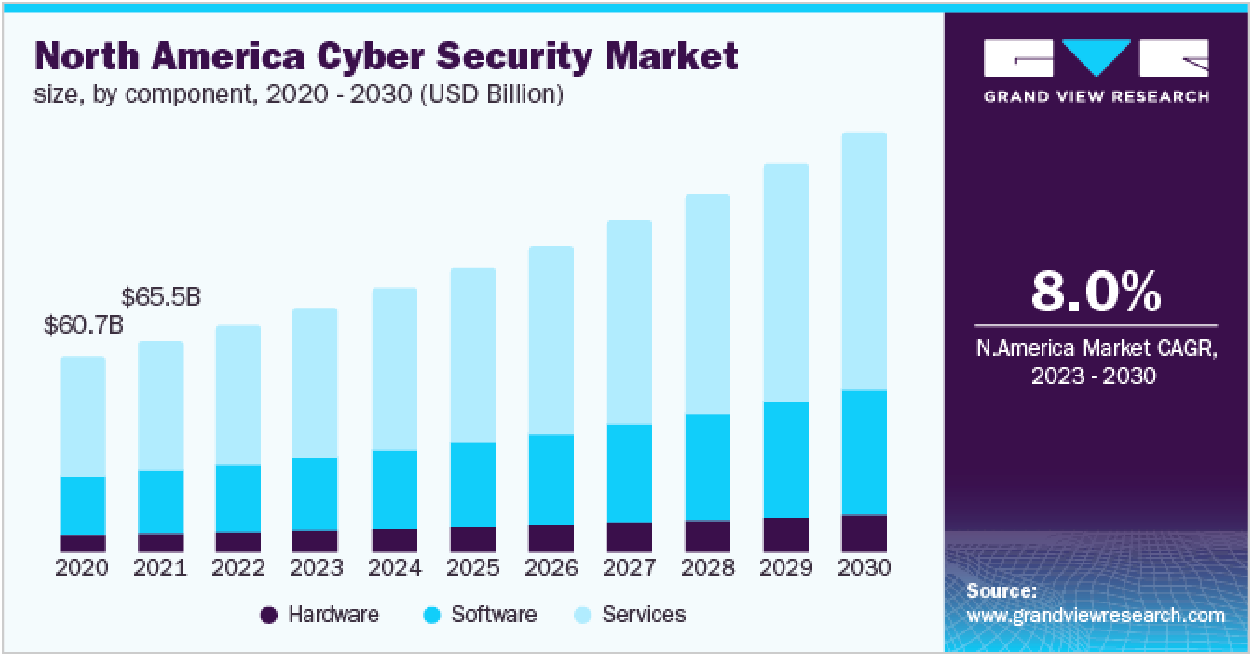

Figure 4. North America Cyber Security Market (2021).

This is due to cyberattacks becoming more sophisticated, and attackers are finding new ways to exploit weaknesses in systems. Additionally, with the ever-increasing use of digital technologies, the number of potential targets for attackers is growing exponentially. Ponemon reports that, globally, the cost of insider threat incidents has risen 44% over the past two years, and the average cost per incident is now $15.38 million. As a result, organizations must stay ahead of the curve and ensure their employees have the knowledge and training they need to prevent and mitigate cyberattacks. This shows the need for organizations to proactively invest in cyber security and employee training.

With the right tools and training, organizations can reduce the risk of cyberattacks and minimize the costs associated with them. According to CISA (2022), here are some additional tips for software companies to prevent cyberattacks:

- Use secure development practices: When developing software, it is important to use secure development practices. This includes using secure coding practices, as well as implementing security testing throughout the development lifecycle.
- Use secure software supply chains: Software companies should use secure software supply chains. This means ensuring that the software they use is from trusted sources and that it has been properly vetted for security vulnerabilities.
- Monitor for threats. Software companies should monitor their networks and systems for signs of threats. This includes using intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).
- Have a security incident response plan. Software companies should have a security incident response plan in place. This plan should detail how the company will respond to a cyberattack, including steps to identify and contain the attack, as well as steps to recover from the attack.

For instance, the plan should include procedures for communicating with customers and partners about the attack, as well as procedures for logging and reporting the incident to relevant authorities. If we start implementing these procedures, then we can have a much safer software work experience and many losses such as identity theft, company product theft, money loss, etc. will be prevented.

Cybersecurity in the Film Industry

The film industry is also one of the main industries with the most impact due to the use of filmmaking software such as Adobe, Final Cut Pro, Logic Pro, Filmora, etc. With the increased use of this type of software, the industry needs to implement cybersecurity measures such as proper authentication protocols, data encryption, and regular security updates to protect the data and intellectual property of the companies and individuals in the industry. A recent study by Business found that a small business's average cost of a data breach can be anywhere from $120,000 to $1.24 million (Rinaldi, 2023). This is why it is so important for the industry to take these measures, as the financial and reputational damage caused by a data breach can be devastating. TBG Security states that “Similar to the Sony hack of 2014, 1.5 terabytes of HBO data were stolen, including full episodes of unreleased shows and sensitive internal documents. New programs were leaked online before release dates. A ransom note said that HBO would need to pay millions of dollars to stop the episodes from leaking.” This attack was carried out by a collection of hackers who stole episodes of the imminent season of the hit display &quot; Game of Thrones; and released them online. The hackers also stole private data about HBO employees, which includes Social Security numbers and credit score card numbers. The hack caused vast disruption to HBO's operations and valued the corporation thousands and thousands of bucks. The hackers were able to gain access to HBO's systems which allowed them to steal confidential data that had the potential to be used for identity theft, financial fraud, and other malicious activities. This caused significant financial damage to HBO as they had to spend money to repair their systems and protect their customers. The Washington Post states that “Over the coming week's multiple statements purported to be from GOP, short for "Guardians of Peace," were posted online -- many to a text-sharing site called PasteBin, which is also used by some hacktivist groups.”

The cyber attack on Sony Pictures was a devastating blow to the company, causing the theft of terabytes of data including unreleased movies, scripts, and employee personal information. The hackers responsible for this breach were purportedly from North Korea and issued a threat to Sony Pictures demanding the cancellation of the movie "The Interview," a comedic film about the assassination of North Korean leader Kim Jong-un. Despite the hackers' threats, Sony Pictures released the movie, but the damage was already done and the company was left to pick up the pieces of their bad reputation and financial losses. The film industry can implement the zero trust network by ensuring strong authentication processes for all users, encrypting data, monitoring access to sensitive data, and implementing multi-factor authentication. Additionally, they should ensure that all users are only granted access to the data that they need to do their job and no additional privileges. Finally, they should continuously monitor and audit user activity to detect suspicious or malicious behavior. Zero-trust policies can help the film/media industry too:

- Prevent unauthorized access to sensitive data: Zero trust systems assume that no user or device is inherently trustworthy, and systems and data must be checked by anyone keep it all thorough This can help prevent unauthorized access to sensitive data, such as movies, scripts, or personal information about employees.
- Detect and prevent back traffic: Back traffic occurs when an attacker gains access to one system and then uses that access to access other systems on the network A zero trust policy can help detect and prevent features that limit traffic by monitoring all network traffic and strictly controlling access.
- Data protection: Data extraction occurs when an attacker steals data from one system and then transfers it to another system. A zero-trust system can help protect against data extraction by encrypting data in transit and monitoring all network traffic for suspicious activity.
- Reduce the risk of ransomware attacks: Ransomware attacks are a major film/media industry threat. Zero trust systems can help reduce the risk of ransomware attacks by implementing strong authentication methods, encrypting data at rest and travel, and organizing density preservation and recovery

Here are some specific examples of how a zero-trust system can be used in the film/media industry:

- A film studio can use a zero-trust system to prevent unauthorized access to unreleased movies and scripts. The system would require all users to authenticate themselves before they could access these assets, and it would also monitor all network traffic for suspicious activity.
- A streaming service can use a zero-trust system to protect its customers' personal information. The system would require all users to authenticate themselves before they could access their accounts, and it would also monitor all network traffic for suspicious activity.
- A movie theater chain can use a zero-trust system to protect its customers' payment information. The system would require all customers to authenticate themselves before they could purchase tickets or concessions, and it would also monitor all network traffic for suspicious activity.

Overall, a zero-trust system can be a valuable tool for film/media companies that are looking to improve their cybersecurity posture. By implementing a zero trust system, companies can make it more difficult for attackers to gain access to their systems and data, which can help to protect their IP, data, and reputation from cyberattacks.

Conclusion

In Conclusion, Cybersecurity measures aim to mitigate risks by ensuring authenticity, confidentiality, availability, and reliability. In the digital realm, cybersecurity protects digital assets and data from unauthorized access, theft, or destruction through techniques like firewalls, encryption, access control, and regular updates. Cyber threats, such as cyberattacks, can result in severe consequences, including financial loss, reputational damage, and compromised personal information. As these threats evolve and become more sophisticated, the demand for skilled cybersecurity professionals grows exponentially. Key cybersecurity tools like Intrusion Prevent Systems (IPS), Next-Gen Antivirus (NGAV), and Sandboxing help counter common threats like viruses and malware. Security Orchestration and Response (SOAR) technologies aid in efficient threat response. Zero Trust is an advanced cybersecurity model that challenges the traditional perimeter-based security approach. Zero Trust assumes no inherent trust and requires continuous verification of users and devices before granting access to resources. This model leverages technologies like artificial intelligence and machine learning to detect and respond to threats in real-time. With over 2,200 cyberattacks daily, organizations must adopt proactive measures to protect their systems. In the healthcare industry, cybersecurity is crucial due to sensitive patient data, safety, and regulatory requirements. Healthcare organizations must ensure secure data handling and implement robust security protocols against threats like ransomware and data breaches. Data breaches can lead to significant financial and reputational damage. Advanced encryption technologies and two-factor authentication are commonly used to secure healthcare data. The software industry also faces cybersecurity challenges as interconnected systems become vulnerable to cyber threats. Secure development practices, software supply chains, threat monitoring, and incident response plans are vital for software companies to protect against cyberattacks. Proper cybersecurity training for employees is crucial, as employee negligence is a significant weakness in cybersecurity. The film industry relies heavily on filmmaking software, making it susceptible to cyberattacks. The industry must prioritize authentication protocols, data encryption, and regular updates to safeguard data and intellectual property. High-profile incidents, such as the Sony hack, underscore the need for robust cybersecurity measures. Implementing a zero-trust network can help prevent unauthorized access and data breaches, thus protecting sensitive content. Overall, cybersecurity plays a critical role in various industries, including healthcare, software, and film. Therefore, it is important for organizations to prioritize cybersecurity measures in order to protect their data and systems from potential attacks. Companies must also invest in regular security audits to ensure their systems are up-to-date and secure. Finally, organizations should educate their employees on the importance of cybersecurity and provide them with the necessary resources to protect themselves. As cyber threats evolve, organizations must adopt advanced security measures, including zero trust, encryption, and continuous monitoring, to safeguard their assets, data, and reputation.

References

Fox, J. (2023). *Top cybersecurity statistics to know for 2023*. Cobalt. https://www.cobalt.io/blog/cybersecurity-statistics-2023#:~:text=How%20many%20cyberattacks%20per%20day,1%20cyberattack%20every%2039%20seconds.

Corporation, P. (2021). *Global Top Health Industry Issues 2021*. PwC. https://www.pwc.com/gx/en/industries/healthcare/top-health-industry-issues.html

Morse, S. (2019). *Healthcare's number one financial issue is cyber security*. Healthcare Finance News. https://www.healthcarefinancenews.com/news/healthcares-number-one-financial-issue-cybersecurity

Khan, S. (2016). *Flow chart for the security system | download scientific diagram.* ResearchGate. https://www.researchgate.net/figure/Flow-chart-for-the-security-system_fig4_318787447

Kaspersky, E. (2023). *The human factor in IT security: How employees are making businesses vulnerable from within.* Daily English Global blogkasperskycom. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Flynn, J. (2023). *25 alarming data breach statistics [2023]: Frequency of exposed records*. Zippia. https://www.zippia.com/advice/data-breach-statistics/

McKeon, J. (2022). *HC3 outlines the history of healthcare cybersecurity from the 1980s to now*. HealthITSecurity. https://healthitsecurity.com/news/hc3-outlines-history-of-healthcare-cybersecurity-from-1980s-to-now#:~:text=The%20first%2Dever%20ransomware%20attack,AIDS%20conference%20in%20Stockholm%2C%20Sweden.

Rinaldi, A. (2023). *How much should your SMB budget for cybersecurity?* business.com. https://www.business.com/articles/smb-budget-for-cybersecurity/

Theriault, C. (2022). *Takeaways from 2017's Cyber Hacks, data leaks and breaches*. TBG Security. https://tbgsecurity.com/takeaways-from-2017s-worst-cyber-hacks-data-leaks-and-breaches/

Maayan, G. D. (2023). 4 cybersecurity tools to know about: NGAV, SAST, EDR, NGFW. Back4App Blog. https://blog.back4app.com/cybersecurity-tools/

Rana, K. (2023). What is Zero Trust security? principles of the zero trust model. ' CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

Mussington, D. (2023). 4 things you can do to keep yourself cyber safe: CISA. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe

PUBLICATIONS, G. (2020). *Zero trust security market size and share [2023 report]*. Zero Trust Security Market Size And Share [2023 Report]. https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report

Tucker, K. K. (2021). Pros and cons of the Zero Trust Model. Infused Innovations. https://www.infusedinnovations.com/blog/secure-intelligent-workplace/pros-and-cons-of-the-zero-trust-model