Data Security Management Strategies to Mitigate Insider threats in healthcare in the United states

Kelvin Ovabor

Dr. Travis Atkison

March,2023

ABSTRACT

Insider threats have increasingly become an emerging issue of concern in the United States of America. Insider threat incidents consist of occurrences such as accessing confidential patient records without authorization, sharing protected health information (PHI) outside of the organization, or unintentionally exposing PHI due to a lack of cybersecurity knowledge. The consequences of insider threats can be far-reaching and costly for healthcare organizations. Not only do they jeopardize patients' right to privacy and confidentiality in their medical care, but they can also lead to financial losses. In addition, these incidents can create reputational damage, which could ultimately affect an organization's bottom line. The research paper analyses the problem of insider threats in the healthcare industry in the United States and discusses data security management strategies that can be used to mitigate these insider threats in the healthcare industry. The research paper defines three technological approaches that are significant in mitigating insider threats which include firewall solutions, intrusion detection systems, and honeypot technologies. Furthermore, the research study highlights additional mitigation measures such as multifactor authentication, employee training, regular background checks, and proper storage and disposal of data.

Keywords—Insider threats, data mitigation strategies, honeypot technologies, intrusion detection, firewall solutions

I. INTRODUCTION

In the recent past, there has been an increase in insider threats across various sectors. Between the year 2018 and 2020, number of insider threat incidents in the United States of America have increased by 47% [1]. Industries that deal with sensitive information, critical infrastructure, or valuable assets have been most vulnerable to insider attacks. Insider threats incidents vary industry by industry. The most affected industries include financial services, healthcare, technology, government agencies, and defense and military services [2].

An insider threat is any malicious activity by an employee, contractor, or other trusted individuals with access to an organization's network or confidential data. Mostly, Insider threats can come from malicious actors who seek to damage the organization. When an individual with access to a company's confidential information uses that access for malicious or unauthorized activities, it not only has the potential to put customer data at risk but can also lead to lost revenue, legal costs, and brand damage [3]. The finance and healthcare industry have been affected the most by incidents of insider threats. The increased number of incidents can be credited to privilege misuse by employees. Figure 1 shows incident distributions of insider threats caused by privilege abuse by employees.

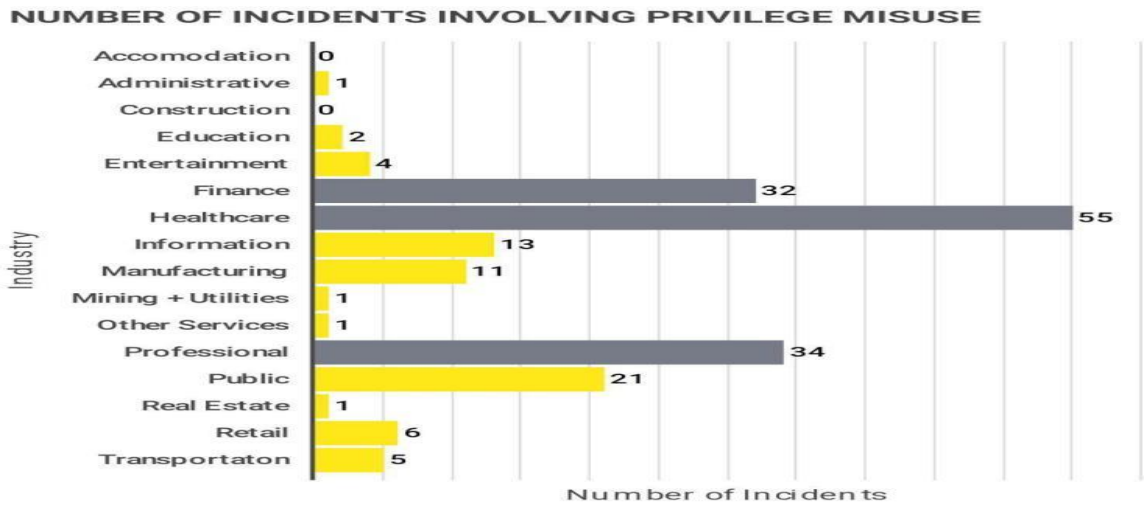

Fig1: incident distributions of insider threats (Rosenthal, 2022) [4]

A. Statement of the problem

According to the visual representation in figure 1, the healthcare industry is mostly affected by insider threats. The high number of insider threats in the healthcare sector is due to the high value of medical data, consisting of sensitive and confidential patient data, which is a prime target for malicious

[1] Maddie Rosenthal, "Insider Threat Statistics You Should Know: Updated 2022," *Tessian* , Accessed January 13, 2022, https://www.tessian.com/insider-threat-statistics/.
[2] Costa, "Patterns and Trends in Insider Threats Across Industry Sectors (Part 9 of 9: Insider Threats Across Industry Sectors)," SEI , August 22, 2019, https://insights.sei.cmu.edu//patterns-and-trends-in-insider-threats-across-industry-sectors-part-9-of-9-insider-threats-across-industry-sectors/.
[3] Dimitrios Tsiostas et al., "The Insider Threat: Reasons, Effects and Mitigation Techniques," in *24th Pan-Hellenic Conference on Informatics*, 2020, 340–45.
[4] Rosenthal, "Insider Threat Statistics You Should Know."

actors [5]. Some of the entities that target health information include Cybercrime groups consisting of well-organized and well-funded criminal organizations that specialize in hacking into healthcare systems to steal sensitive information, such as patient data or financial information. Additionally, fraudulent billing schemes engage in fraudulent billing practices, such as submitting false claims for payment or upcoding procedures to increase reimbursement. Another form of insider attack in the healthcare industry is supply chain attacks. These are criminal organizations that target the healthcare supply chain to steal medical equipment or compromise medical devices with the goal of extracting ransom or causing harm to patients.

As the healthcare sector evolves and is increasingly digitized, it is critical to understand efficient data security management strategies to mitigate insider threats in healthcare organizations. Therefore, this paper analyses data security management strategies to mitigate insider threats in the healthcare sector. The preliminary sections of this paper will contain the various forms of insider threats. Thereafter the research article will evaluate insider threats in the healthcare industry and relevant mitigation strategies for insider threats.

II. FORMS OF INSIDER THREATS

Insider threats exist in many forms and can pose a significant risk to an organization's security. There are different forms of insider threats experienced in the United States of America [6]. According to the report, the most common types if insider threats include data exfiltration, privilege misuse, data aggregation, infrastructure sabotage, circumvention of IT controls, and account sharing.
Figure 2 elaborates on the percentage distribution of the various forms of insider threats in the United States of America.

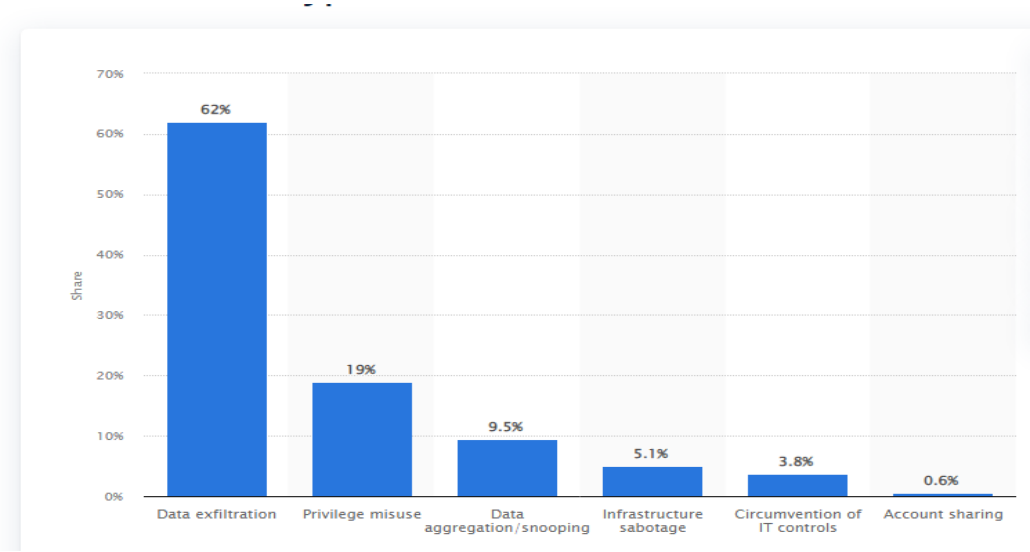

Fig 2: percentage distribution of the various forms of insider threats in the United States of America (Statista,2020) [7]

According to the report, data exfiltration is the most common type of insider threats in the United States. It involves the unauthorized extraction of sensitive data from an internal network or system by

[5] Weizhi Meng et al., "Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks," *IEEE Transactions on Network and Service Management* 15, no. 2 (2018): 761–73.
[6] Statista, "U.S. Common Insider Threat Types 2020," Statista, 2020, https://www.statista.com/statistics/1155585/most-common-insider-threat-types-united-states/.

either an insider employee or an external hacker. The most common form of data exfiltration takes place when malicious actors gain access to a company's databases, web servers or other systems in order to steal confidential information such as customer records, trade secrets, intellectual property and financial information. This type of attack is often perpetrated by insiders who are familiar with the IT environment and know how to exploit it for their own gain. Alternatively, hackers may use malware or social engineering techniques in order to extract data from target networks without authorization.

Figure 3 shows the most common forms of data exfiltration behaviors in the United States in the year 2020.

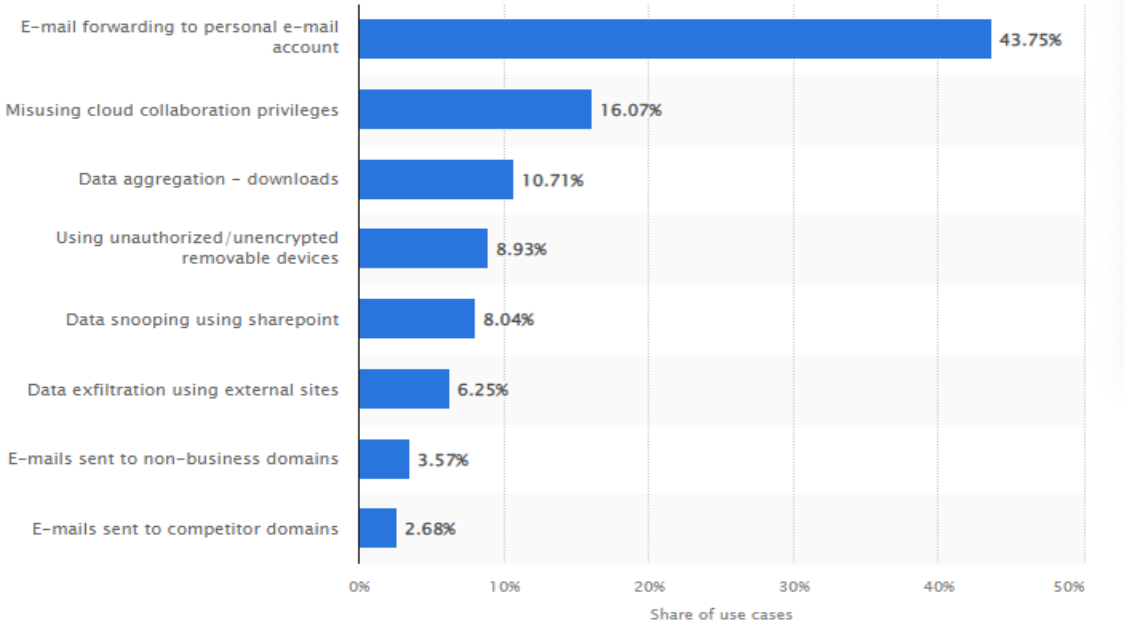

Fig 3: forms of data exfiltration behaviors in the United States by the year 2020 (Statista1,2020)[8]

A. Insider threats in the United States of America

One of the significant negative impacts of insider threats is the financial impact. As incidences of insider threats continue to increase in the United States of America, the financial damages coming from insider breaches continue to increase, exceeding those of previous years [7]. The research study highlights that the steady growth of insider threats in the United States is attributed to employee or contractor negligence, criminal and malicious insiders, and credential theft. Figure 4 highlights the financial impact of these three insider threat profiles in the United States of America.

[7] Larry, "Gaining Insight Into the Ponemon Institute's 2020 Cost of Insider Threats Report," *Security Intelligence* (), January 27, 2020, https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/.

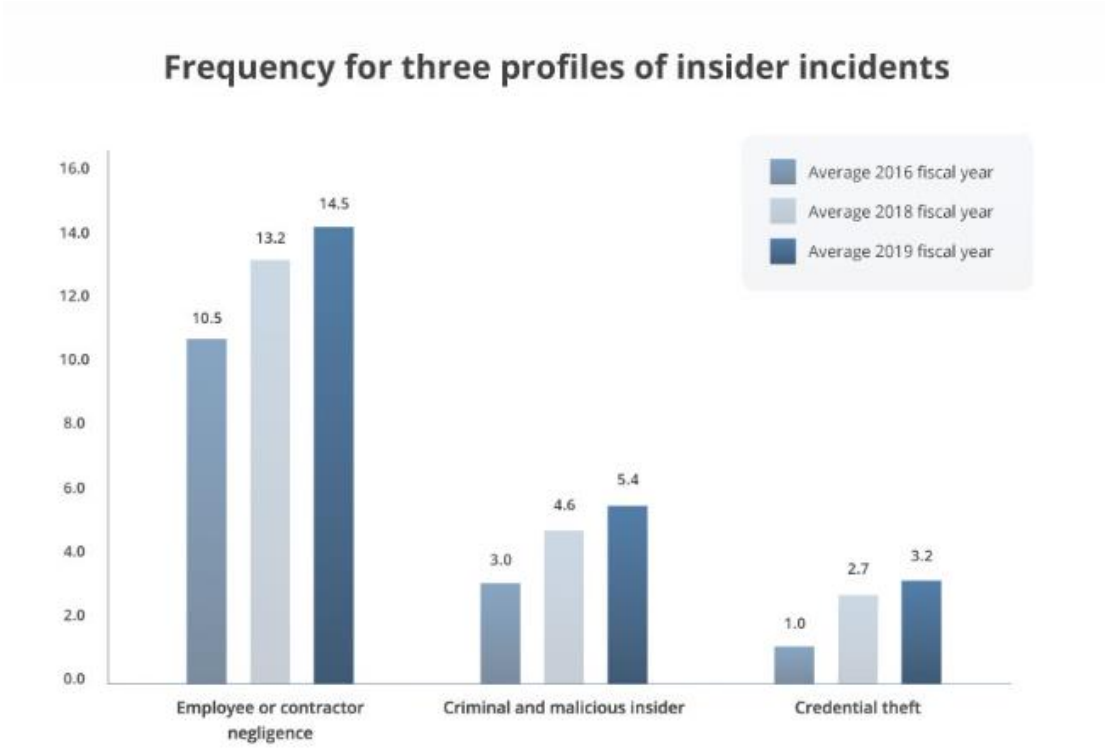

Fig 4 financial impact of insider threat profiles in the United States of America [8]

1) *Employee and contractor Negligence*

Employee negligence occurs when an employee fails to exercise reasonable care within the scope of their job duties. Examples include failing to follow established safety procedures, careless handling of confidential information, and inadequate security practices that leave systems vulnerable to attack Contractor negligence encompasses a wide range of activities that can lead to significant damages. For example, an organization may be liable for the negligence of its contractors if they fail to meet contractual obligations or are found to have violated industry standards in their work. This could include any type of negligent behavior from failure to properly maintain equipment or failing to have sufficient safety protocols in place. Additionally, contractor negligence can also refer to inappropriate behavior such as engaging in bribery, fraud, or other illegal activities while working on behalf of the company. Detecting and remediating incidences contributed by employee and contractor negligence in the United States is extremely expensive, reaching an average of $310,000 [9]. The costs are attributed to extreme measures that organizations need to take, such as conducting regular employee training, implementing strict access controls, conducting regular risk assessments, implementing incident response plans, and monitoring employee and contractor activity.

In the healthcare industry, employee and contractor negligence may play a crucial role in causing insider attacks. Negligent employees or contractors may inadvertently share sensitive patient data with

[8] Ekran, "Insider Threat Statistics for 2022: Facts and Figures," March 9, 2022, https://www.ekransystem.com/en//insider-threat-statistics-facts-and-figures.
[9] Ekran.

unauthorized individuals or fail to properly secure patient data, potentially resulting in data breaches [10]. Additionally, employee and contractor negligence can be a significant contributor to financial loss. Negligent employees or contractors may cause financial loss to the organization by mishandling equipment, inappropriately billing patients, or making other costly errors. Moreover, employee and contractor negligence can be a key contributor to legal consequences. Negligent employees or contractors may cause the organization to violate regulatory requirements, resulting in legal consequences and fines.

Furthermore, they may damage the reputation of the healthcare organization. Insider attacks caused by negligent employees or contractors can damage the organization's reputation and erode trust among patients and stakeholders.

ii) Criminal and malicious insiders

Malicious insiders, such as those with a grudge against the organization or looking to make a financial gain, are especially dangerous because they have access to sensitive data and systems. They are individuals with authorized access to an organization's systems or networks who intentionally use their privileged access to damage the organization or steal its data [11]. These malicious insiders can be current employees, contractors, former employees, or other personnel with authorized access to a company's information. They cause harm by exploiting their knowledge of the system and its vulnerabilities through malicious activities such as stealing information, manipulating data, disabling security systems and introducing malware into the system. In the United States, mitigating the effects of malicious insider activity costs averagely $760,000 [12]. This included both the direct and indirect costs associated with the incident. It is important to note that the cost of mitigating the effects of malicious insider activity can be significantly reduced through proactive measures, such as implementing robust access controls, conducting regular security awareness training, and implementing a strong incident response plan.

Criminal and malicious insiders can have a significant cost impact on the healthcare industry. Such insiders are individuals who have authorized access to an organization's systems, networks, and data but use this access for nefarious purposes. One of the potential cost impacts of criminal and malicious insiders in the healthcare industry is legal costs [13]. Healthcare organizations may face legal costs, fines, and penalties if a criminal or malicious insider breaches patient privacy, violates healthcare laws, or engages in fraudulent activities. Additionally, the impact of a data breach or insider attack can be damaging to the reputation of healthcare organizations, especially if patients' personal and sensitive information is exposed. Such a breach can lead to a loss of trust in the healthcare organization, which can impact patient retention and acquisition.

Moreover, insider threats can be a significant contributor to loss of productivity in healthcare organizations. Insider attacks and data breaches can lead to downtime, which can result in a loss of productivity and revenue for healthcare organizations.

[10] In Lee, "Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach," *Information* 13, no. 9 (2022): 404.
[11] Larry, "Gaining Insight Into the Ponemon Institute's 2020 Cost of Insider Threats Report."
[12] Ekran, "Insider Threat Statistics for 2022."
[13] Lee, "Analysis of Insider Threats in the Healthcare Industry."

iii) Credential theft

Credential theft involves stealing logins and passwords in order to gain access to an organization's network and potentially steal information or launch other attacks. In employee or contractor negligence cases, an individual may fail to secure their access credentials adequately and provide an opportunity for unauthorized access. For example, they may leave their passwords written down in plain sight or use the same password across multiple accounts. Criminal or malicious insiders are individuals who have gained access to a company's network and then attempt to steal credentials belonging to other users. This type of behavior is difficult to detect as the attack is internal in nature. Finally, credential theft can be part of broader insider threat profiles that involve espionage or data theft. Cyber criminals may target privileged users with high-level access privileges in order to gain information from within a company's network that can be used for extortion, blackmailing, fraud or other illicit activities [14].

In the United States, incidences that involve credential theft are most expensive to deal with at $870,000 on average [15]. The cost of mitigating the effects of credential theft can include a range of direct and indirect costs, such as forensic investigations, legal fees, reputational damage, and lost productivity. In addition to the immediate costs of mitigating the incident, there may also be long-term costs associated with implementing measures to prevent future incidents and improve overall security posture. To reduce the risk and cost of incidents involving credential theft, organizations should implement a range of security measures, such as multifactor authentication, strong password policies, and access controls. Regular security awareness training can also help employees and contractors understand the importance of protecting their credentials and recognize potential threats, such as phishing attacks. By taking a proactive approach to security, organizations can reduce the likelihood and impact of credential theft incidents and minimize the associated costs of mitigation.

In the healthcare industry, when cybercriminals steal the login credentials of healthcare employees, they can use these credentials to gain unauthorized access to patient records and other confidential information, leading to several potential cost impacts, including legal costs, reputational damage, cost of remediation and regulatory compliance [16]. Legal costs, fines and penalties may arise when cybercriminal uses stolen credentials to breach patient privacy or violates healthcare laws. Additionally, reputational damage may occur especially if patients' personal and sensitive information is exposed. Such a breach can lead to a loss of trust in the healthcare organization, which can impact patient retention and acquisition. On the other hand, the cost of remediation entails the cost of investigating the breach, implementing security measures to prevent future attacks, and providing credit monitoring and identity theft protection for affected patients. Furthermore, Healthcare organizations are subject to various regulatory requirements, and a data breach or unauthorized access incident can lead to additional regulatory scrutiny and compliance costs.

[14] Larry, “Gaining Insight Into the Ponemon Institute’s 2020 Cost of Insider Threats Report.”
[15] Ekran, “Insider Threat Statistics for 2022.”
[16] Lee, “Analysis of Insider Threats in the Healthcare Industry.”

B. Categories of insiders

Other research studies define two basic categories of insiders: adversarial insiders and unintentional insiders.

a.) Adverserial insiders

Adversarial Insiders are individuals who intentionally use their access to sensitive information, such as company information systems, company financial data, and employee information, for malicious or unauthorized purposes [17]. In this case, adversarial insiders do not have to be current employees of the organization but can also be previous employees with relevant knowledge of the company's operational and security systems. Adversarial insiders are categorized into five groups: Class 1 Terrorists, Class 5 Terrorists, Sophisticated Economic Criminals, Unsophisticated Criminals, and Lone Criminals [18].

Class 1 terrorists consist of professional and government-trained individuals who use advanced knowledge and skills to gain access to sensitive information, communications networks, financial resources, and physical infrastructure that can be used to commit acts of terror or espionage. Furthermore, they can manipulate systems, databases, and networks for a long period without detection. Class 5 terrorists are amateur civilians who engage in activities such as data theft and sabotage of computer systems with malicious intent. They may also spread false information with malicious intent to cause harm or disruption. The goal of these terrorists is often financial gain through ransom demands or exploiting sensitive data for their personal benefit.

The third category of adversarial insiders is the sophisticated economy criminals with expert-level knowledge and technical ability to manipulate systems to gain access to data specifically for financial gain. On the other hand, unsophisticated criminals have less expertise in gaining unauthorized access. These criminals often lack the resources or capability to execute large-scale attacks, but they can still cause significant damage with small-scale actions. Lone criminals refer to adversarial insiders who work independently to commit a crime for personal gain or to exact revenge on a particular target. These criminal acts are often carried out without any direct assistance from outside parties. Lone criminals usually lack extensive criminal networks, making them difficult to identify or track down. This also means that their actions are often seen as more unpredictable and, therefore, more dangerous than other forms of insider threats due to their individual motivations.

A good example of adversarial insiders in the health industry is disgruntled employees who use their access to patient data to steal identities or other sensitive information. This includes employees who feel mistreated by their employer or fellow employees and may use their privileged access to exercise revenge on people who have wronged them. Moreover, another example of adversarial insiders in the healthcare industry includes contractors or vendors who use their access to sensitive information for unauthorized purposes. Additionally, adversarial insiders consist of healthcare providers who engage in fraud or theft, such as billing for services not provided or falsifying records for personal or financial gain.

---

[17] Duc C. Le and A. Nur Zincir-Heywood, "Evaluating Insider Threat Detection Workflow Using Supervised and Unsupervised Learning," in *2018 IEEE Security and Privacy Workshops (SPW)* (IEEE, 2018), 270–75.

[18] Chaitanya Joshi, Jesus Rios Aliaga, and David Rios Insua, "Insider Threat Modeling: An Adversarial Risk Analysis Approach," *IEEE Transactions on Information Forensics and Security* 16 (2020): 1131–42.

b.) Unintentional insiders

As organizations become more decentralized and digital, there's an increased risk of employees becoming unintentionally privy to corporate secrets and confidential information. Individuals with access to sensitive data, either in person or electronically, can sometimes cause damage without realizing it. Such individuals are referred to as unintentional insiders. Unintentional Insiders are individuals who may have access to sensitive data without any malicious intent, yet their actions can cause damage when they expose such information [19]. An unintentional insider threat is a security risk that arises when an employee or contractor unknowingly introduces malicious content, causes damage to an organization's computer systems, or shares sensitive information with unauthorized parties.

One of the most common causes of unintentional insider threats is human error [20]. Data breaches caused by employee mistakes can have detrimental effects on the organization, often leading to financial losses or reputational damage. Examples of such errors include leaving confidential information exposed online, mismanaging passwords, or failing to update software on time. Such scenarios increase the likelihood of data falling into the wrong hands if left unchecked. Human errors occur as a result of a lack of proper training or even negligence [21]. Lack of proper training of employees on data security protocols, such as access rights management, software updates, and secure password usage, puts the employees at risk of undertaking an unintentional breach which may cause substantial losses and may be as damaging as intentional breaches. Additionally, one of the significant causes of human error in the workplace is employee fatigue. Employee fatigue happens when employees become overworked due to long hours and a heavy workload, leading them to make careless errors, where one mistake could lead to a significant breach of data and confidential information.

A good example of an unintentional insider threat in the healthcare industry is accidentally sending sensitive information to the wrong recipient, such as sending an email containing patient data to an unintended recipient. Such an occurrence is likely to cause data to get to unauthorized people who may manipulate data and use it for unauthorized purposes. In addition, another example of an unintentional insider threat incident in the healthcare industry is losing a device that contains sensitive patient information, such as a laptop or mobile device that has not been properly secured. Such data contained in these devices may also fall into unauthorized hands, who may manipulate the data for personal or financial gain. Moreover, another example of an unintentional insider threat in the healthcare industry is falling for phishing scams, where an attacker tricks the employee into providing sensitive information, such as login credentials or financial information. Additionally, a healthcare institution may fall victim to an insider threat attack by neglecting to properly secure sensitive information, such as leaving patient records on a shared drive or failing to encrypt a device.

[19] Neeshe Khan, Robert J Houghton, and Sarah Sharples, "Understanding Factors That Influence Unintentional Insider Threat: A Framework to Counteract Unintentional Risks," *Cognition, Technology & Work*, 2021, 1–29.
[20] Khan, J Houghton, and Sharples.
[21] Khan, J Houghton, and Sharples.

III. Mitigation strategies

As insider threats are increasingly becoming a rising concern for healthcare organizations, they are also increasingly turning to technology to detect and mitigate data security threats [22]. Many organizations have implemented solutions that monitor employee behavior, such as access logs and audit trails. This type of surveillance allows security personnel to identify anomalous activity that could suggest malicious intent or negligence by employees. In addition, many organizations are configuring systems to automatically flag suspicious activity for review by security experts, who then can therefore respond accordingly. Other technologies allow companies to control privileged user accounts and protect sensitive data from unapproved access, reducing the risk of an insider threat event. Organizations are taking advantage of technology to implement layers of technological security that can reduce the number of accessible vulnerabilities by insiders. Some of the measures of technological security recommended by researchers include intrusion detection technologies, honeypot technologies, and firewall solutions.

.

A. Firewall solutions

Firewalls are one of the most effective tools for protecting organizational data from insider threats in the form of data theft, system sabotage, or cyber criminals [23]. A firewall is a barrier that blocks certain traffic from entering or leaving a network. It is designed to inspect incoming and outgoing data packets, analyzing each packet for malicious content before allowing it through the firewall or discarding it entirely. Firewalls also allow administrators to control user access to certain applications or websites, preventing malware or viruses from entering their networks through unsecured sites or programs. For example, a firewall can be set up to allow access to sensitive data only from a trusted IP address range or to block traffic from certain IP addresses or regions that are known to be associated with malicious activity.

Additionally, firewalls can be configured to log and alert on suspicious activity, such as repeated login failures or attempts to access prohibited resources. This information can be used to detect and respond to insider threats in real-time and to improve the organization's security posture over time. Generally, firewalls are designed to monitor traffic that enters or leaves an organization's network and detect suspicious activity. By implementing a multi-level firewall system with sophisticated access control policies and monitoring capabilities, organizations can limit the risk posed by insiders who may have malicious intent or unintentionally create security vulnerabilities within their networks.

The most common firewall solution used to deal with insider threats in the healthcare sector is the traditional firewall systems. Traditional firewalls are designed to control traffic between networks based on packet headers and ports. They often provide features such as stateful inspection and deep packet inspection (DPI) to ensure all data is secure. These are additional tools for monitoring and managing network traffic in hospitals that can be used to detect applications or protocols that are used for malicious practices such as data exfiltration. Utilizing DPI as a firewall can help healthcare organizations guard against insider threats and other malicious activity. It offers numerous benefits that make it a viable solution for protecting valuable patient data and assets. DPI works by analyzing the contents of all packets sent over a network. Instead of simply blocking traffic based on port numbers or IP addresses, this type of

[22] Tsiostas et al., "The Insider Threat."

[23] Padma Priya Mukkamala and Sindhu Rajendran, "A Survey on the Different Firewall Technologies," *International Journal of Engineering Applied Sciences and Technology* 5, no. 1 (2020): 363–65.

firewall examines each packet in detail to detect potentially malicious activity. This allows administrators to quickly identify any suspicious activity within their networks, making it easier to take appropriate action and prevent damage before it occurs. Additionally, DPI firewalls are often able to recognize patterns in traffic that may indicate malicious behavior, allowing administrators to respond more effectively when an attack does occur.

B. Intrusion Detection Systems

One of the most effective solutions for defending against insider threats is an intrusion detection system (IDS). An IDS is a type of security tool specifically designed for detecting, preventing, and responding to live (in real-time) malicious activity within a network or system environment [24]. It uses advanced analytics and machine learning algorithms to detect suspicious behavior by analyzing user actions such as file access or downloads from the network. . The system can then alert IT administrators so that appropriate action can be taken in response. Not only can it help identify malicious activity before it becomes a problem, but it also helps reduce false positives and provide more accurate threat intelligence. There are two types of intrusion detection systems which include anomaly-based IDSs and signature-based IDSs [25]. Anomaly detection is a type of security system that uses machine learning algorithms to detect suspicious activity on a network [26]. It works by monitoring user behavior, identifying any anomalies in the data, and issuing an alert if any suspicious activity is detected. An anomaly detection system can be applied to many networks, such as computer networks, manufacturing systems, and financial transactions. The system will analyze historical data from the network to create a baseline of normal behavior patterns that can detect any unusual activity. This makes it possible for the system to identify malicious activities like malware or unauthorized access attempts much more quickly than traditional security solutions. Furthermore, anomaly detection systems are highly customizable and can be tailored for specific environments or use cases. The main advantage of using an Anomaly IDS is its ability to quickly recognize new types of attacks that have yet to be documented or identified. It can also identify the source of the attack, allowing administrators to take proactive steps to prevent future attacks on their networks [27]. One limitation of anomaly-based IDS is that it relies heavily on accurate data profiles, which can be difficult to create due to the dynamic nature of networks. The system must be trained with existing network traffic to detect any anomalies, which means that if the profile changes due to new applications or user behaviors, the system may not be able to distinguish between normal and suspicious activity. In addition, false positives are common in anomaly-based IDS due to errors in training or because legitimate activities may also trigger alerts.

On the other hand, signature-based intrusion detection systems look for predefined patterns or templates known as "signatures" based on attack patterns that indicate malicious behavior or potential

---

[24] Ansam Khraisat et al., "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges," *Cybersecurity* 2, no. 1 (2019): 1–22.

[25] Sajad Einy, Cemil Oz, and Yahya Dorostkar Navaei, "The Anomaly-and Signature-Based IDS for Network Security Using Hybrid Inference Systems," *Mathematical Problems in Engineering* 2021 (2021): 1–10.

[26] K. N. Ambili and Jimmy Jose, "Trust Based Intrusion Detection System to Detect Insider Attacks in IoT Systems," in *Information Science and Applications: ICISA 2019* (Springer, 2019), 631–38.

[27] Liu Liu et al., "Anomaly-Based Insider Threat Detection Using Deep Autoencoders," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)* (IEEE, 2018), 39–48.

threats [28]. These signatures can be in the form of specific patterns of packets transmitted over a network, data payloads associated with known malware, or even particular types of user behavior. By using signature-based detection methods, SIDS can quickly identify and alert administrators to any suspicious activities occurring within their environment. The main advantage of using a signature-based intrusion detection system is its accuracy in detecting known attacks and vulnerabilities. Since these attack signatures are already defined in the database, the system can quickly detect them even before they cause any damage to the network.

Additionally, since new attack signatures can be added to the database as needed, it allows for an evolving security infrastructure to keep up with emerging threats. This makes it an ideal solution for organizations looking for a proactive approach to protecting their IT systems. However, as cyber attackers continue to develop new ways of infiltrating computer systems, SBIDS are often unable to keep up with the changing threat landscape. This can lead to false positives or false negatives in security alerts, hindering an organization's ability to respond quickly and appropriately. Another issue is scalability; most organizations eventually outgrow their existing signatures-based detection systems because they cannot scale up when the number of users increases. SBIDS are also vulnerable to data tampering; if attackers gain access to the signature database, they could modify or delete existing security signatures, making it easier for them to bypass detection.

C. Honeypot technologies

Honeypots are security technologies used to detect and respond to insider threats by creating a decoy network or system that mimics a valuable target for attackers to interact with. Insider threats are security incidents that originate from within an organization, such as malicious insiders or employees who unintentionally cause harm. By using a honeypot, organizations can lure potential insiders into interacting with the decoy, allowing security teams to observe and track their activities, gain insights into their tactics and techniques, and potentially prevent or mitigate a security breach [29]. An example of how a honeypot works is if an employee tries to access restricted information on the company's server, they will be diverted instead to the honeypot. The honeypot then records all activity and provides alerts so that security personnel can take the steps necessary in order to prevent any further damage from occurring. Honeypot technology works through honeytokens. Honeytokens act as a link between an actual honeypot and the attacker who is trying to access it [30]. When the attacker attempts to gain access, they will be given a false set of credentials or data which will trigger an alert and allow the organization's security team to take appropriate action if needed. Honeytokens provides organizations with an early warning system allowing them to quickly identify potential threats and take preventative measures before any damage occurs.

One of the main drawbacks of honeypot technology is that it needs to be enticing enough for attackers. For a honeypot to be effective, it must make an appealing target while still being difficult enough

---

[28] Steven Tug, Weizhi Meng, and Yu Wang, "CBSigIDS: Towards Collaborative Blockchained Signature-Based Intrusion Detection," in *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (IEEE, 2018), 1228–35.

[29] Muhammad Mudassar Yamin et al., "Implementation of Insider Threat Detection System Using Honeypot Based Sensors and Threat Analytics," in *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2* (Springer, 2020), 801–29.

[30] Yamin et al.

that it cannot easily be detected or compromised by an attacker because honeypots may be useless if the attacker does not interact with them [31]. This requires careful planning on how the honeypot will appear and what data is included within its environment so that it remains undetectable. In case an attacker identifies a honeypot, they may implement false information that can lead the security personnel in the wrong direction.

D. Other data strategies to combat internal threats

1) Employee training

The above technological approaches to combating insider threats are applicable to adversarial insiders. However, healthcare organizations need to implement mitigation measures for unintentional insiders who may put the organization at risk of loss of sensitive or confidential data. One of the common causes of unintentional insider threats is the lack of proper employee training programs to raise awareness of the problem of insider threats in organizations. Employee training is an essential component of an insider threat awareness program, as it helps to educate employees about the risks associated with insider threats and provides them with the knowledge and skills they need to recognize and respond to potential security incidents. Employee training aims to raise awareness of the importance of information security and encourage employees to take a proactive role in protecting the organization's data and resources [32].

The employee training program should clearly define what constitutes an insider threat and the potential harm it can cause to the organization. Secondly, the training should provide employees with real-world examples of insider threats and their impact on an organization. Additionally, employees should be trained on the organization's security policies, including the acceptable use of company resources, data protection, and incident reporting of insider threats. Furthermore, Employees should be trained on how to report suspected security incidents, who to report them to, and what information to include in the report.

Moreover, Employees should be trained on the technical security controls in place, such as firewalls, intrusion detection systems, and encryption, and how they help to protect the organization's data and resources. In addition, employees should be trained on best practices for information security, such as avoiding phishing scams, protecting passwords, and being vigilant about suspicious activity. It is important to note that by providing employees with information that raises their awareness of insider threat security, organizations will be able to reduce the risk of security breaches and improve overall security for the organization.

2) Multifactor authentication

Multifactor authentication is an additional layer of security that requires a user to provide two or more pieces of evidence in order to gain access. There are three most commonly used methods of multifactor authentication [33]. One of the most common types is something the user knows, like a password.

---

[31] Yamin et al.

[32] Shaun Joseph Smyth, Kevin Curran, and Nigel McKelvey, "The Role of Education and Awareness in Tackling Insider Threats," in *Cybersecurity Education for Awareness and Compliance* (IGI Global, 2019), 33–52.

[33] Siranjeevi Rajamanickam, N. Ramasubramanian, and Satyanarayana Vollala, "Insider Attack Prevention Using Multifactor Authentication Protocols-A Survey," in *Applied Information Processing Systems: Proceedings of ICCET 2021* (Springer, 2022), 331–39.

This type of MFA relies on a user knowing something specific, like a username or PIN, to authenticate. A user must present the card and then provide additional information, such as username and password, for access to the network. These tokens typically generate random codes, making it impossible for hackers to gain unauthorized access even if they have obtained the user's credentials from other sources. It can also require additional information, such as answers to security questions. Another type of MFA is something you have. This could be in the form of an ID card with a chip that contains unique information about the user or even biometric authentication using fingerprint scanners or facial recognition technology. This type of authentication requires physical possession of something and is often combined with other methods for added security. A third type of MFA is based on location or environment, which has become more popular in recent years due to technological advancements. Geofencing and IP address tracking are used to detect if someone trying to access your account is attempting it from somewhere they shouldn't be (like an IP address located halfway across the world). Additionally, some systems use behavioral analytics such as mouse movement and typing speed in order to help verify users' identities more accurately.

Modern technologies of MFA have emerged in the healthcare industry to prevent access by unauthorized users. One of the most recent common methods of MFA in the healthcare industry is the time-based one-time passwords (TOTP). This involves generating unique codes that expire after a certain amount of time; this requires users to continually update their passwords over time which adds an extra layer of security against insider criminals who may try repeatedly guessing login information until they get it right. It prevents unauthorized users from gaining access by requiring multiple credentials at different levels that are harder to replicate or steal than just one password, making it difficult for hackers to gain entry into systems. Additionally, multifactor authentication can provide an extra layer of protection if one factor fails due to lost credentials, compromised accounts, or other types of attacks, such as phishing attempts.

One of the significant benefits of utilizing MFA is that it can greatly reduce the risk of a successful cyberattack. By requiring users to go through multiple levels of verification before gaining access, insiders intending to use access privilege to cause harm are much less likely to be able to breach a system successfully. Additionally, if any one factor were compromised, other credentials still remain intact and secure due to the layered approach provided by MFA. Another advantage of implementing an MFA system is that it can help increase user convenience and efficiency. By reducing the number of steps required for user authentication, users can gain quicker access with fewer complications or delays while still maintaining a high level of security. In addition, some systems provide additional features, such as two-step verification codes or biometric scans, which can further simplify the login process for users while providing enhanced protection against attackers. Additionally, using an MFA system often reduces costs associated with dealing with insider threats or identity theft since fewer successful breaches occur when multiple layers of authentication are required for access. This helps organizations save money on repairs and recovery, which would be necessary after a breach without strong security measures in place, like those offered by multifactor authentication systems.

MFA has its significant share of limitations. It is important to note that MFA can be difficult to set up initially, especially for users who are not tech-savvy. It can require multiple steps and the user may need assistance in order to complete the setup process. This can be time-consuming and costly for companies who may have to hire IT support or outsource the setup. Another downside of MFA is that it is not foolproof. While it does help reduce the risk of unauthorized access, it does not guarantee that a hacker will not gain access to an account if they gain access to a user's credentials, such as their username

and password. Additionally, some methods of authentication, such as SMS verification codes, can be vulnerable to interception by malicious actors. Moreover, MFA can lead to decreased usability for users since they must go through extra steps in order to log into their accounts or perform certain actions within them. This can increase frustration which could ultimately lead users away from using the service altogether if they view the security measures as too cumbersome or intrusive.

3) Physical security measures

Physical security measures can play an important role in preventing insider threats, as they can help restrict physical access to sensitive areas and resources within an organization [34]. One of the most commonly used physical security measures in healthcare organizations is the use of video surveillance. Video surveillance is a physical security measure used to monitor an area for suspicious activity and deter insider threats. It involves installing cameras in strategic locations such as entrances, exits, and around vulnerable areas. This footage can be viewed in real-time or later reviewed if an incident occurs. Video surveillance has become increasingly popular due to advances in digital technology that make the systems more sophisticated and efficient than ever before. Cameras are now able to capture images with greater clarity, enabling organizations to identify people more easily. They also feature facial recognition capabilities, which can help detect suspicious behavior quickly. Additionally, modern video surveillance systems are equipped with analytics capabilities that allow it to map out common patterns of movement or detect any abnormal activity that might point to a potential threat. Lastly, most systems offer remote access so authorized personnel can access the footage from anywhere at any time for added convenience and peace of mind.

Secure storage is essential in protecting data from insider threats. It helps prevent insider threats by restricting access to sensitive data and physical assets within an organization. By limiting access to authorized personnel only, secure storage can help prevent theft, unauthorized access, and other malicious activities that can be carried out by insiders. This includes proper storage protocols such as locking cabinets and drawers and ensuring restricted access to sensitive areas. Another layer of secure storage involves encryption protocols for both physical media (e.g., hard drives) and virtual systems (e.g., cloud services). Encryption ensures that even if a device is stolen or accessed by an unauthorized user, the data contained within remains safe from being exposed or tampered with. Additionally, companies can opt to use file-level encryption, which allows individual files to be encrypted without the need for entire disks or volumes to be encrypted each time a file is added/removed/modified – this helps reduce encryption overhead costs while protecting organizational assets at the same time

Research studies recommend some key considerations for implementing secure storage as a physical security measure to prevent insider threats in healthcare organizations. One of the key actions healthcare organizations need to establish first is to identify what needs to be secured. In a healthcare organization, patient health information is one of the most critical data. This includes any information about a patient's medical condition, treatment history, medication information, and test results. PHI is protected by the Health Insurance Portability and Accountability Act (HIPAA) and should only be accessed by authorized personnel. Additionally, healthcare organizations have other critical information

[34] Myeongki Jeong and Hangjung Zo, "Preventing Insider Threats to Enhance Organizational Security: The Role of Opportunity-Reducing Techniques," *Telematics and Informatics* 63 (2021): 101670.

such as personal identification information of patients, financial information of patients, research data, and employee information.

Once the organization has identified what needs to be secured, it can select appropriate storage solutions based on the type and level of security required. One of the most commonly used storage solutions in a healthcare organization is the Electronic Health Record Systems (EHR Systems). EHR systems are secure electronic storage systems that allow healthcare providers to access and update patient records in real-time. These systems are designed to ensure patient privacy and security and are compliant with HIPAA regulations. Additionally, Cloud storage is a secure and cost-effective way to store large amounts of data. Hospitals can use cloud storage solutions that are designed specifically for healthcare, such as Amazon Web Services (AWS) or Microsoft Azure, which provide HIPAA-compliant cloud storage.

4) Regular background checks

Regular background checks can be an effective data mitigation strategy against insider threats in the health care setting. Regular background checks are a key data mitigation strategy against such threats as they help uncover any potential past criminal activity or misconduct that may have been overlooked during the initial hiring process of employees [35]. Even if no alarms are raised during the screening process, it is important to perform periodic background checks on employees with access to sensitive data and systems. This allows organizations to stay up to date with any changes in their employees' backgrounds and detect new risks before harmful insiders cause any significant harm. A good background check system should be comprehensive and include all relevant information. This includes verifying the individual's identity, criminal record, driving history, employment history, credit report, education records, and any other data that can be used to vet an applicant or employee. Additionally, organizations should confirm references from previous employers or schools to verify that the employee is who they say they are. The background check process should also include a risk assessment of the individual of interest. This helps identify potential areas for concern in their past and present activities that may present a risk to the organization if hired. It is important for organizations to take into account factors such as current location, name changes, or inconsistencies in past backgrounds when conducting background investigations. Finally, it is essential for employers to have proper procedures in place so that the results of these checks are properly stored and managed in order to maintain compliance with applicable laws and regulations.

Some of the benefits associated with regular background checks include improved safety, reduced costs, and increased compliance with regulations. Since most insider threats occur due to negligence or malicious intent on the part of employees, having an effective vetting process in place helps organizations identify any potential threat in advance. Additionally, by ensuring that personnel has been properly vetted through a comprehensive screening process, organizations can take more preemptive measures when it comes to protecting their data assets.

A good background check system is important in setting up access management policies. Access management involves controlling who can access data within an organization, as well as what type of data

[35] Rakan A. Alsowail and Taher Al-Shehari, "Techniques and Countermeasures for Preventing Insider Threats," *PeerJ Computer Science* 8 (2022): e938.

they can view and modify. Poorly implemented access management policies create opportunities for malicious insiders to gain unauthorized access and steal confidential information from the system without being detected. By implementing strong access control measures, organizations can protect their networks from potential insider threats who may have an undesirable background record.

5) Proper handling and disposal of data

Proper handling and disposal of data is an important data mitigation strategy against insider threats in a hospital setting. Improper handling or disposal of sensitive data can lead to data breaches, which can have severe consequences for the hospital, patients, and employees. t requires that all information stored on any device should be removed permanently so as to reduce the chances of unauthorized access. To ensure proper data disposal, organizations must have policies and procedures in place for identifying which data needs to be disposed, determining when it should be disposed, and how it should be done. Organizations must use secure methods to dispose of data they no longer need or use. This includes using certified erasure software and hardware-based solutions to completely erase any traces of the file or document from the computer's hard drive. The most secure method of disposing electronic media is degaussing; this involves exposing the media to powerful magnetic fields in order to "scramble" its contents beyond recognition. Additionally, the Physical destruction of hard drives can also help ensure that none of their information can ever be recovered by someone with malicious intent. Organizations may employ shredding services for paper documents containing sensitive information before disposing them off in an approved manner. Furthermore, health organizations should also limit the transferability of any non-public information between users so as not to reduce risk associated with insider threats that may arise due to to mishandling or sharing this sensitive information with external parties.

IV. CONCLUSION

In conclusion, data security management strategies to mitigate insider threats in the healthcare sector are essential for organizations to remain secure and compliant. The objective of this research study was to analyze some of the data security management strategies to mitigate insider threats in the healthcare sector. The research study recommended a technological approach to combatting insider threats in organizations. Effective technological solutions, such as firewall solutions, honeypot technologies, and intrusion detection systems, can play a crucial role in reducing the risk posed by adversarial insiders. On the other hand, the usage of employee training programs to raise awareness of insider threats can help reduce the risk posed by unintentional insiders. Moreover, additional mitigation measures such as multifactor authentication, regular background check and proper handling and disposal of data can play a crucial role in reducing the likelihood of insider attacks in healthcare organizations.

Reference

Alsowail, Rakan A., and Taher Al-Shehari. “Techniques and Countermeasures for Preventing Insider Threats.” *PeerJ Computer Science* 8 (2022): e938.

Ambili, K. N., and Jimmy Jose. “Trust Based Intrusion Detection System to Detect Insider Attacks in IoT Systems.” In *Information Science and Applications: ICISA 2019*, 631–38. Springer, 2019.

Costa. “Patterns and Trends in Insider Threats Across Industry Sectors (Part 9 of 9: Insider Threats Across Industry Sectors).” SEI , August 22, 2019. https://insights.sei.cmu.edu/ /patterns-and-trends-in-insider-threats-across-industry-sectors-part-9-of-9-insider-threats-across-industry-sectors/.

Einy, Sajad, Cemil Oz, and Yahya Dorostkar Navaei. “The Anomaly-and Signature-Based IDS for Network Security Using Hybrid Inference Systems.” *Mathematical Problems in Engineering* 2021 (2021): 1–10.

Ekran. “Insider Threat Statistics for 2022: Facts and Figures,” March 9, 2022. https://www.ekransystem.com/en/ /insider-threat-statistics-facts-and-figures.

Jeong, Myeongki, and Hangjung Zo. “Preventing Insider Threats to Enhance Organizational Security: The Role of Opportunity-Reducing Techniques.” *Telematics and Informatics* 63 (2021): 101670.

Joshi, Chaitanya, Jesus Rios Aliaga, and David Rios Insua. “Insider Threat Modeling: An Adversarial Risk Analysis Approach.” *IEEE Transactions on Information Forensics and Security* 16 (2020): 1131–42.

Khan, Neeshe, Robert J Houghton, and Sarah Sharples. “Understanding Factors That Influence Unintentional Insider Threat: A Framework to Counteract Unintentional Risks.” *Cognition, Technology & Work*, 2021, 1–29.

Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. “Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges.” *Cybersecurity* 2, no. 1 (2019): 1–22.

Larry. “Gaining Insight Into the Ponemon Institute’s 2020 Cost of Insider Threats Report.” *Security Intelligence* ( ), January 27, 2020. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/.

Le, Duc C., and A. Nur Zincir-Heywood. “Evaluating Insider Threat Detection Workflow Using Supervised and Unsupervised Learning.” In *2018 IEEE Security and Privacy Workshops (SPW)*, 270–75. IEEE, 2018.

Lee, In. “Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach.” *Information* 13, no. 9 (2022): 404.

Liu, Liu, Olivier De Vel, Chao Chen, Jun Zhang, and Yang Xiang. “Anomaly-Based Insider Threat Detection Using Deep Autoencoders.” In *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, 39–48. IEEE, 2018.

Meng, Weizhi, Kim-Kwang Raymond Choo, Steven Furnell, Athanasios V. Vasilakos, and Christian W. Probst. “Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks.” *IEEE Transactions on Network and Service Management* 15, no. 2 (2018): 761–73.

Mukkamala, Padma Priya, and Sindhu Rajendran. “A Survey on the Different Firewall Technologies.” *International Journal of Engineering Applied Sciences and Technology* 5, no. 1 (2020): 363–65.

Rajamanickam, Siranjeevi, N. Ramasubramanian, and Satyanarayana Vollala. “Insider Attack Prevention Using Multifactor Authentication Protocols-A Survey.” In *Applied Information Processing Systems: Proceedings of ICCET 2021*, 331–39. Springer, 2022.

Rosenthal, Maddie. “Insider Threat Statistics You Should Know: Updated 2022.” *Tessian* ( ), May 13, 2022. https://www.tessian.com/ /insider-threat-statistics/.

Smyth, Shaun Joseph, Kevin Curran, and Nigel McKelvey. “The Role of Education and Awareness in Tackling Insider Threats.” In *Cybersecurity Education for Awareness and Compliance*, 33–52. IGI Global, 2019.

Statista. “U.S. Common Insider Threat Types 2020.” Statista, 2020. https://www.statista.com/statistics/1155585/most-common-insider-threat-types-united-states/.

Statista1. “U.S. Insider Threat Data Exfiltration Behaviors 2020.” Statista, 2020. https://www.statista.com/statistics/1155846/most-common-data-exfiltration-insider-threat-types-usa/.

Tsiostas, Dimitrios, George Kittes, Nestoras Chouliaras, Ioanna Kantzavelou, Leandros Maglaras, Christos Douligeris, and Vasileios Vlachos. “The Insider Threat: Reasons, Effects and Mitigation Techniques.” In *24th Pan-Hellenic Conference on Informatics*, 340–45, 2020.

Tug, Steven, Weizhi Meng, and Yu Wang. “CBSigIDS: Towards Collaborative Blockchained Signature-Based Intrusion Detection.” In *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1228–35. IEEE, 2018.

Yamin, Muhammad Mudassar, Basel Katt, Kashif Sattar, and Maaz Bin Ahmad. “Implementation of Insider Threat Detection System Using Honeypot Based Sensors and Threat Analytics.” In *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2*, 801–29. Springer, 2020.