Internet Security

Lamya AL-Khuzam

lf.alkhuzam@paaet.edu.kw

The Public Authority for Applied Education and Training, Kuwait

Abstract

With the growth of the Internet and an increasing number of users globally, internet security has become a significant concern. There is also the increased use of the Internet and information online for improved decision-making, and this information is a valuable commodity that increases the threats or risks involved in Internet use. The study provides a comprehensive overview of the growth in security threats, the types of threats on the internet, and the components and measures adopted to tackle these issues. The study explores issues like denial of service, malware, and other threats while also exploring various components in hardware and software that could be used to mitigate these threats. The study focuses on antimalware, access controls, firewalls, intrusion detection and protection systems, authentication, and other governance measures and frameworks employed in organizations to improve cybersecurity and mitigate the threats identified in the paper. The paper also discusses the importance and need for awareness or training for the people with studies highlighting how training could help in developing a culture that promotes safe use and compliance with regulatory requirements. Overall, this study helps better understand the threats, mitigation, and importance of awareness and helps summarize the views on internet security based on existing knowledge.

Contents

1. Introduction

The advent of the internet has been a major advancement in technology that allowed for improved connectivity and communication across the globe. Technology has played a critical role in bringing the world closer and offering unparalleled convenience. It is mentioned that in 2023 it will be around 5.19 billion users and 4.99 billion social media users. While the number of users is increasing, the safe use of the internet or awareness regarding the threats looming or hidden in the internet platform is minimal (Alfalah, 2023). Over the years, there have been many initiatives across the globe by different countries aimed at increasing awareness, and the growth of technology and big data has increased the threat posed by the internet and highlights the need for internet security.

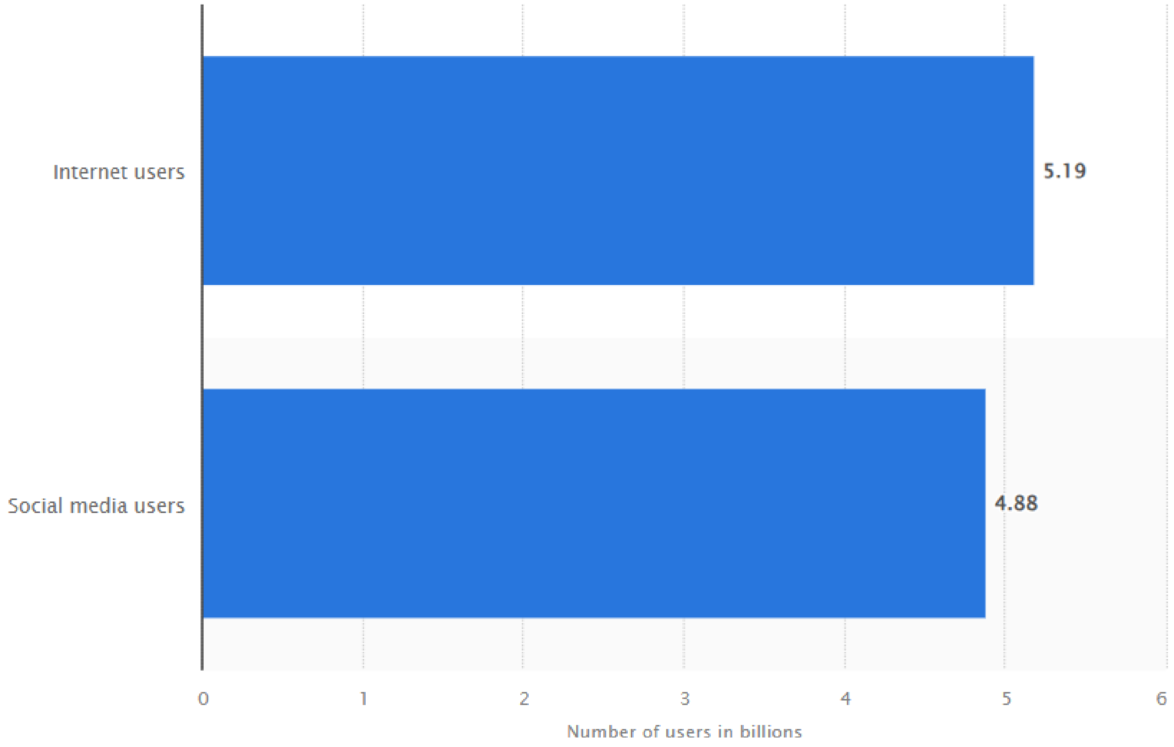


Figure 1 Internet users (Statista, 2023)

Internet security is often referred to as cybersecurity. It is said to be made of various sets of technologies, practices, and strategies to protect the individual online, digital assets, and the infrastructure that underpins the internet itself. It is the system's defense against various risks and threats that are said to lurk within the digital domain. Cybersecurity is said to be important for the following reasons (Dalal *et al.*, 2022; Mishra *et al.*, 2022):

- The Internet is a breeding ground for various malicious agents seeking financial gain from state-sponsored hackers working on political agendas. Internet security is said to be the first line of defense from these visible and hidden threats on the internet.
- In the age of big data, information is said to be a highly valuable commodity, and internet security is responsible for safeguarding the right to privacy.
- Data is a valuable asset for organizations, too, and any loss in data could have dire consequences, making internet security measures like safe practices critical in mitigating the risks.
- Internet security is critical to legal compliance in certain industries, not just good practices.

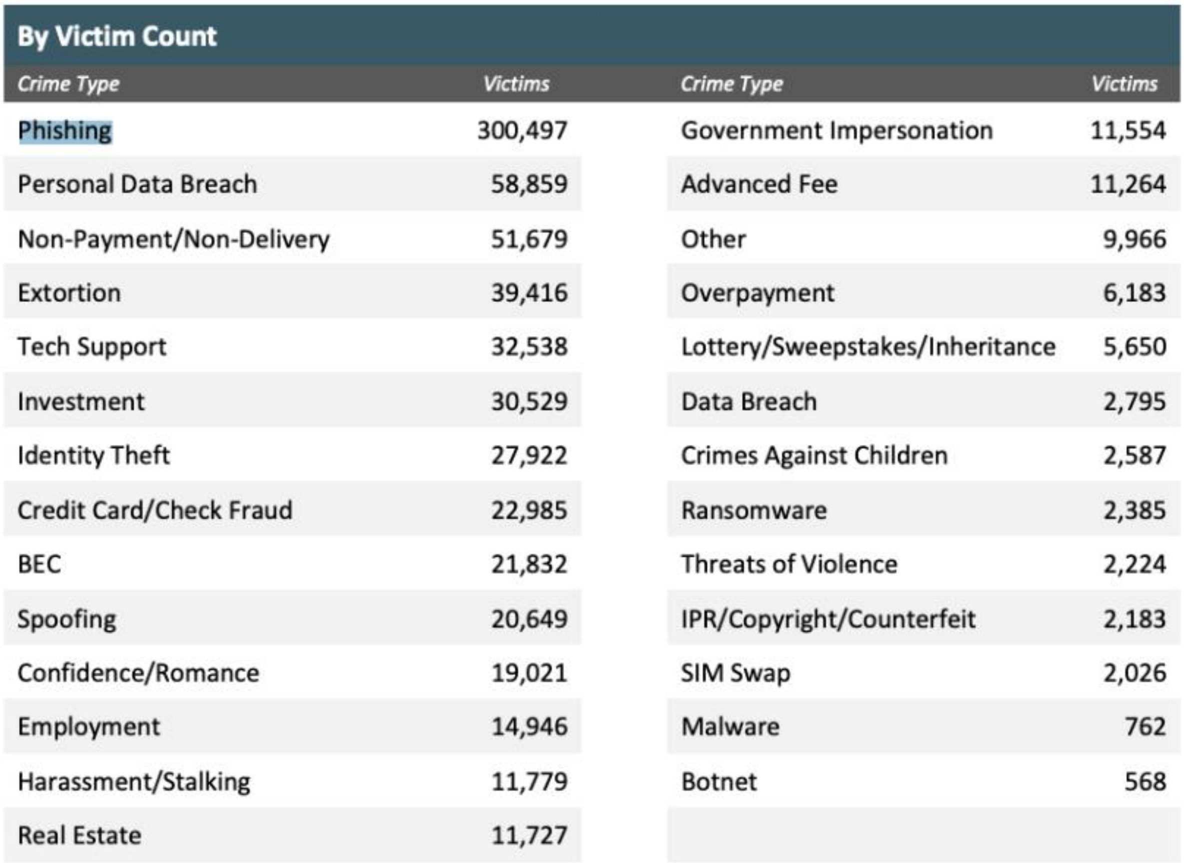
As per the CISCO report, 86% of the organization has had at least one user connect to a phishing site, and 70% reported users served with malicious browser ads (Cisco Systems, 2021). This highlights the need for awareness regarding the different threats and an understanding of best practices to avoid the issue in the long run. This research paper aims to explore the different threats under internet security while also exploring the best practices to counter and mitigate these threats with the growing digital footprint.

2. Type of Internet Security threats

Before going into the different types of internet security threats, it is critical to understand the common sources of these Cyber Threats. One of the main threats comes from hostile countries that are known to launch cyber attacks against companies or institutions to cause disorder and inflict damage (Thornton-Trump, 2019; CISA, 2020). The same techniques and tools are also used by terrorist organizations to destroy or abuse critical infrastructure, disrupt economies, or cause harm to the citizens of a country, along with criminal groups known to break into this system for their economic gains (CISA, 2020; Lehto, 2022). The threats could also come from hackers who are not within groups but individuals motivated by personal goals. These people are dangerous as they often develop new threats focusing on advancing their criminal ability and improving their notoriety in the community. Last but not least are the malicious insiders who work in the company and abuse the privileges to steal information and damage the computing system that provides them with economic or personal gain (Machado de Sousa and Shahzad, 2022; Asha, Shanmugapriya and Padmavathi. G., 2023). All these actors are known to use different techniques or tools to attack users online, which are security threats. We look at these different types of threats in this section.

One of the most common forms of attack known is the Malware attack. Malware is an abbreviation for malicious software that could be viruses, trojans, ransomware, and spyware that are used to hide within software within the coding or the files that are activated later. These threats are said to enter the system through a link to an untrusted website or email or through unsupported or unverified software downloads (Gibert, Mateu and Planes, 2020; Sudhakar and Kumar, 2020). The malware is said to deploy on the target system and stay hidden, collect sensitive data, manipulate or block access to certain network components, destroy data, or shut down the entire system. In this, viruses are said to be pieces of code injected into the application, and when the application is run, these codes are executed. Worms are the other type of malware exploiting the vulnerabilities and trying to gain access to the operating system through backdoor channels. Once installed in the network, these could initiate attacks like distributed denial of service (DDoS).

The digital environment faces a substantial and dynamic danger from Distributed Denial of Service (DDoS) assaults. These assaults entail using a hostile network of hacked computers, commonly known as a botnet, to inundate a target server or network with excessive traffic, rendering it unreachable to authorized users. The ramifications of Distributed Denial of Service (DDoS) incidents are extensive and can result in severe outcomes. Cyber attackers cause disturbances to various online services, e-commerce platforms, government websites, and vital infrastructure systems, leading to financial ramifications, harm to reputation, and occasionally posing public safety risks. Distributed Denial of Service (DDoS) assaults use the inherent openness of the internet and the extensive network of interconnected devices, posing significant challenges in prevention and mitigation strategies. The complexity of Distributed Denial of Service (DDoS) assaults has escalated, encompassing strategies such as amplification and reflection methodologies, posing greater prevention challenges (Dzurenda, Martinasek and Malina, 2015; Balarezo *et al.*, 2022). The DDoS can target the entire server, network, or website with excessive traffic, rendering it inaccessible to legitimate users. These attacks also do not have data encryption or locking, and their primary purpose is to disrupt the cause of downtime and online services. On the same line but even more deadly is ransomware, which encrypts the files and locks them out of the system, which makes the data inaccessible. This tool is used to extort money from the victim where the access or decrypt for the funds locked away would be provided once the payment is made (Clancy, 2021; Humayun *et al.*, 2021). Based on reports on the cost of ransomware, it is estimated that the average cost for a breach was $4.54 million in 2022, but this is just the loss the company suffers and does not include the ransom paid (Bluvector, 2022). It is also reported that in 2022, there was a total of 493.33 million attacks that were detected by organizations (Kolesnikov, 2023). Other malware, like rootkits, are injected into applications where the attacker can use the operating system, gain complete computer control, and deliver more malware to the system to collect and transfer data.



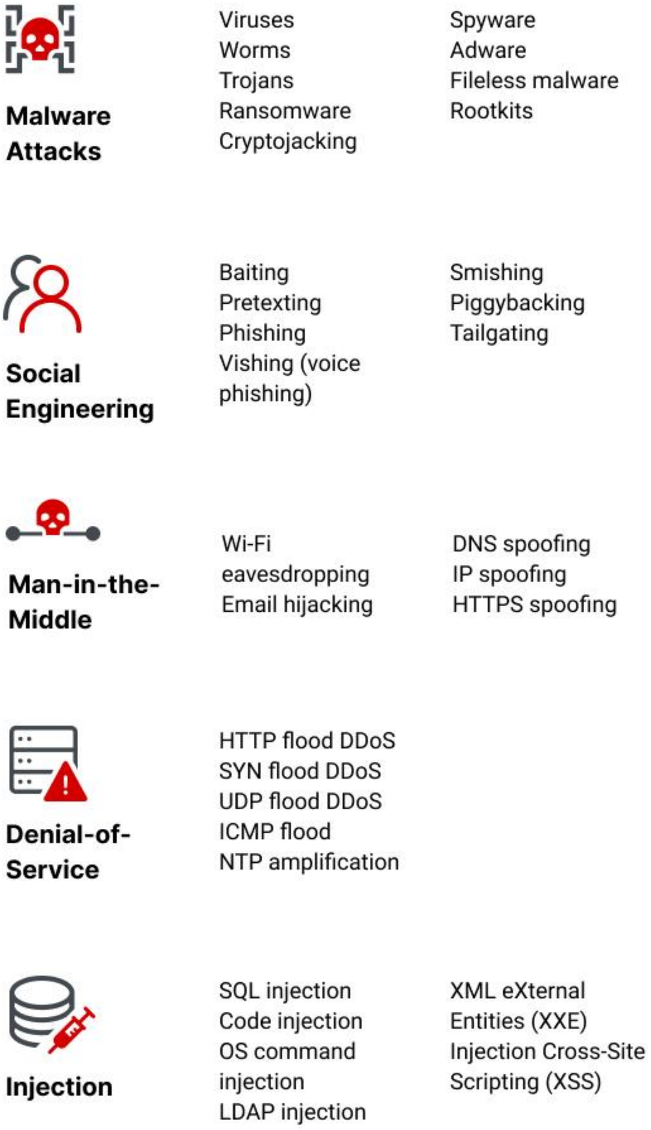
By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Figure 2 Threats by Victim Count (Kolesnikov, 2023)

Figure 2 shows that Ransomware victims much less than other threats like personal data breaches and Phishing. This is another type of threat, which is said to be social engineering attacks, which focus on tricking the users into providing an entry point for the malware to enter the system. Here, the victims often provide sensitive information or unknowingly install malware on their devices because the attacker would pose as a legitimate actor. This would include baiting, where the attacker would lure users into social engineering traps based on promises like gift cards, pretexts, or impersonation of an authority or organization whose position would compel the victim to comply. That said, Phishing, the biggest threat with the highest victim count, is a significant challenge in internet security. Phishing is a pervasive and deceitful hack that exploits human psychology, uses social engineering strategies to get sensitive data, and illicitly undermines digital security. The process commonly entails malevolent persons assuming the guise of reliable companies, such as financial institutions, email service providers, or governmental organizations, to deceive users into revealing sensitive information, such as login passwords, financial data, or personal particulars. Phishing assaults encompass a range of manifestations, such as email phishing, characterized by disseminating deceptive emails with hyperlinks to counterfeit websites that closely mimic authentic ones (Chaudhry, Chaudhry and Rittenhouse, 2016; Thomas *et al.*, 2017; Cisco Systems, 2021). Additionally, spear-phishing tactics are employed to target individuals or organizations through customized and persuasive messaging. The potential ramifications of succumbing to phishing attacks can be substantial, encompassing the theft of one's identity, monetary detriment, or unlawful infiltration into personal or organizational accounts. Phishing perpetrators are consistently enhancing their methods, underscoring the importance for individuals and organizations to acquire knowledge about phishing risks, exercise caution when engaging with digital communications, and adopt strong security measures, including email filtering, two-factor authentication, and employee training, to mitigate the hazards associated with this perpetually evolving cyber threat.

A new threat or attack seen with software developers and vendors is the supply chain attacks that infect legitimate applications and distribute the malware through the main source code, build the processes, or from the updates. Attackers often seek non-secure network protocols and coding techniques that they could compromise on and modify their codes to hide themselves. The supply chain attacks would compromise the building tool, the code signing procedure, and malicious code sent as automated updates and pre-installed on devices (Lella *et al.*, 2021; Martínez and Durán, 2021). Supply chain attacks are more severe as the applications are often certified by trusted vendors. The software vendors would not be aware of the infection, and malicious codes would run with the same privileges as the application. A Man-in-the-Middle (MitM) attack is a complex cybersecurity threat characterized by the covert interception or eavesdropping on communication between two entities, typically without their awareness or explicit permission. An unauthorized intermediary in the communication process allows for potential manipulation, interception, or theft of sensitive information being transmitted since they place themselves between the source and recipient of data. The principal objective of a Man-in-the-Middle (MitM) assault is to undermine the security and integrity of the data being communicated. This can result in significant ramifications, such as identity theft, financial detriment, or illegal entry into sensitive systems (Conti, Dragoni and Lesyk, 2016; Mallik *et al.*, 2019; DİCLE, 2022). Eavesdropping is a prevalent strategy employed by attackers to surreptitiously intercept conversations, specifically targeting unprotected public Wi-Fi networks, to capture data transferred by unsuspecting users. Data tampering is another aspect in which malicious actors manipulate the information transmitted between entities, modifying financial transaction particulars or distorting communications to deceive receivers. Session hijacking is an additional method employed by attackers to compromise active sessions, particularly web sessions, to assume the identity of legitimate users and obtain illegal entry into their accounts. This type of attack is frequently observed in the context of online banking and email services.



Malware Attacks	Viruses Worms Trojans Ransomware Cryptojacking	Spyware Adware Fileless malware Rootkits
Social Engineering	Baiting Pretexting Phishing Vishing (voice phishing)	Smishing Piggybacking Tailgating
Man-in-the-Middle	Wi-Fi eavesdropping Email hijacking	DNS spoofing IP spoofing HTTPS spoofing
Denial-of-Service	HTTP flood DDoS SYN flood DDoS UDP flood DDoS ICMP flood NTP amplification	
Injection	SQL injection Code injection OS command injection LDAP injection	XML eXternal Entities (XXE) Injection Cross-Site Scripting (XSS)

Figure 3 Different threats

Last but not least, injection attacks are said to exploit various vulnerabilities by inserting malicious codes into web applications. The successful attack is said to expose sensitive information and execute a denial of service attack or compromise the entire system. The most common is SQL injection, where the attacker would enter an SQL query into the end user input channel like web form or content field. The vulnerable application would then end the attacker's data to the database and execute the SQL commands. Most web applications are known to use a database that runs on SQL, making them vulnerable to this attack. Other variants can target another database that does not use any relational data structure. From this, it is quite clear that a lot of cyber security threats are said to work on the lack of awareness of the individuals, while some take a more vicious approach that can cause significant losses for an individual and organization. In the next section, we explore security measures taken to mitigate these threats.

3. Security Measures

Over the years, many fundamental security measures have been adopted to protect computer systems and networks from different security threats. In this section, we look at the different measures adopted regarding software, policies, and hardware aimed at improving internet security.

3.1. Anit-malware or Antivirus

One of the most common and well-known measures all adopt is the Antivirus software. Over the years, the software has evolved. It is also known as anti-malware software used to detect, prevent, and remove any virus or malware that could have infected the system (Hsu *et al.*, 2012). It is reported that the software first scans the entire system, or it could run scanning for specific folders, files, or programs that would look at known patterns or signatures of the malware so that it can remove them, quarantine these files for removal, or even block their installation. Some antivirus are known to use heuristic analysis in detecting suspicious behavior and potential threats, even if these do not have any standard signature. These are installed and distributed by various companies and are said to provide real-time protection and monitoring against attacks or signs of malware and often come with the operating system or the purchase of a new system. This is a foundational security tool known to help prevent infection, maintain system integrity, and safeguard sensitive data. These systems have limited techniques to evade an attack, especially those that might include obfuscation or in-memory extraction (Pérez-sánchez and Palacios, 2022). The term "obfuscation" pertains to the purposeful act of increasing the complexity of code or data to render it more challenging to comprehend or decipher. Within the realm of cybersecurity, the practice of obfuscation serves the purpose of concealing the genuine intentions and operational characteristics of malevolent software. This makes the task of detecting and analyzing such malware considerably more arduous for security researchers, antivirus programs, and other protective measures. "in-memory malware execution" refers to executing malicious code directly in a computer's random-access memory (RAM) without storing the harmful payload on the computer's storage devices, such as the hard disk or solid-state drive. Malicious software frequently uses this technique to evade detection by conventional antivirus or endpoint protection systems that primarily concentrate on monitoring file behavior (Pérez-sánchez and Palacios, 2022). These highlight the limitations of the anti-virus and the need for more measures to protect the system.

3.2. Firewall and Intrusion Detection/Prevention System

Firewalls are another security measure that has evolved over the years and is seen to be a critical component when it comes to securing and building a trusted network environment. Firewalls are internet security systems that often act as a barrier between a trusted internal network and an untrusted external network like the Internet. This aims to control and filter incoming and outgoing traffic based on established security rules (Kim *et al.*, 2020; Alicea and Alsmadi, 2021; Anwar, Abdullah and Pastore, 2021). The firewall performs Several functions, including packet filtering, stateful inspection, and application layer filtering. Packet filtering is the function where the firewall examines network packets. It applies the administrator's rules that let them decide whether the packets need to be allowed or blocked. The decision could be based on the destination, port, source, and protocol (Kim *et al.*, 2020). Network packers are often fundamental units within which the data is transmitted. They are structured pieces of data that contain information necessary for data transmission and reception between the devices connected within the network. These are considered to be the main way of data communication between networks. When the data is sent from one device to another over a network, it is often broken down into smaller packets, allowing efficient transmission. These packets would then be reassembled in the correct order, which would help reconstruct the original data (Alicea and Alsmadi, 2021). Modern firewalls are known to perform a stateful inspection that helps keep track of the active connection and allow or deny traffic based on the state. Next-generation firewalls could also inspect and filter traffic at the application layer, which is said to provide deeper visibility. Firewalls are also part of the first line of defense against unauthorized access and malicious network traffic.

With the growth in technology, the systems have become more complex and challenging, and this evolution has required new advanced features and capabilities that would help to tackle the dynamic nature of the complex environment that exists at present. The newer or modern firewalls are said to go beyond the traditional firewall. One key feature is their ability to understand and control specific applications or services that traverse the network, allowing for more granular control based on the application type. In addition, the new firewall design and policies support AI system that allows for faster data analysis and scan for threats more effectively based on self-learning patterns, making them more adept at protecting the systems (Reznik, 2021; Tassiulas, 2021). The new network architectures have given rise to the need for additional systems in the network architecture that would support improved security. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) serve different functions from the firewall. While the firewalls block or allow traffic based on certain policy controls established, IDS and IPS are said to look at the content of the message (Kuwatly *et al.*, 2004; Liao *et al.*, 2013; Kim, Lee and Kim, 2014). These systems have two functions: identifying potentially harmful behaviors and implementing proactive measures to avoid or minimize security risks. The intrusion detection process is the ongoing surveillance of network traffic, system logs, and event data to detect trends or behaviors that might indicate unauthorized access or breaches of security policies. If suspicious behavior is identified, IDS alerts security personnel or a Security Operations Center (SOC). There exist two primary classifications of Intrusion Detection Systems (IDS) known as Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). NIDS primarily concentrates on surveilling network traffic, while HIDS oversees actions on particular systems or hosts (Scarfone and Mell, 2007; Alazab *et al.*, 2012).

Intrusion prevention serves as a valuable supplement to detection mechanisms by actively acting to avoid or reduce security problems. IPS can react autonomously to identified threats by IDS, thwarting their progression. IPS possesses the capability to promptly execute various measures, such as the interception of harmful packets, imposition of limitations on IP addresses, or modification of firewall regulations (Scarfone and Mell, 2007). The methods above are designed to mitigate the effects of assaults and preserve the integrity of the network. The deployment of Intrusion Detection and Prevention (IDP) systems may be categorized into two main approaches: network-based and host-based. In the network-based approach, strategically positioned Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS) are employed to evaluate the traffic traverses the network. On the other hand, the host-based approach involves the utilization of Host Intrusion Detection Systems (HIDS) and Host Intrusion Prevention Systems (HIPS) to protect particular hosts or devices (Scarfone and Mell, 2007). These systems are of utmost importance in a complete cybersecurity strategy, operating in conjunction with other security measures to offer a strong defense against various security threats and possible breaches. The maintenance of network security and safeguarding of sensitive data necessitates the implementation of efficient configuration, monitoring, and response measures.

3.3. Access Control and Cybersecurity Governance

With the threats and the environment being as challenging, many organizations find it difficult to develop and implement an effective strategy to counter or mitigate eth said threats. Cybersecurity governance is the framework, policies, practices, and processes put in place by the government to manage and oversee cybersecurity efforts effectively and efficiently. The process focuses on defining the structure, responsibilities of the stakeholders, roles, and decision-making process linked to cybersecurity within the organization (Zukis, 2022; Melaku, 2023). This is critical as it helps ensure the cybersecurity strategy aligns with the business's objectives or goals and meets compliance requirements. Most industries and organizations, for example, the healthcare sector, have specific requirements for identifying, assessing, and mitigating cybersecurity risks. Effective governance is said to help the organization make these informed decisions regarding how to allocate resources best and reduce the associated risks. One of the most well-known is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. It provides the organization with a structured approach to managing and enhancing its cybersecurity posture and ensuring that the practices align with the best practices and can adapt to evolving threats. The framework is designed to be flexible and easy to adapt across industries and organizations of different sizes. This provides a structured and systematic approach to governance and helps prioritize the cybersecurity risk while highlighting the governance policies that need to be introduced to ensure the safe use of information within the organization and in storage (Frayssinet Delgado *et al.*, 2021; NIST, 2021). Thus, the framework helps continuously improve and enhance the overall cybersecurity resilience.

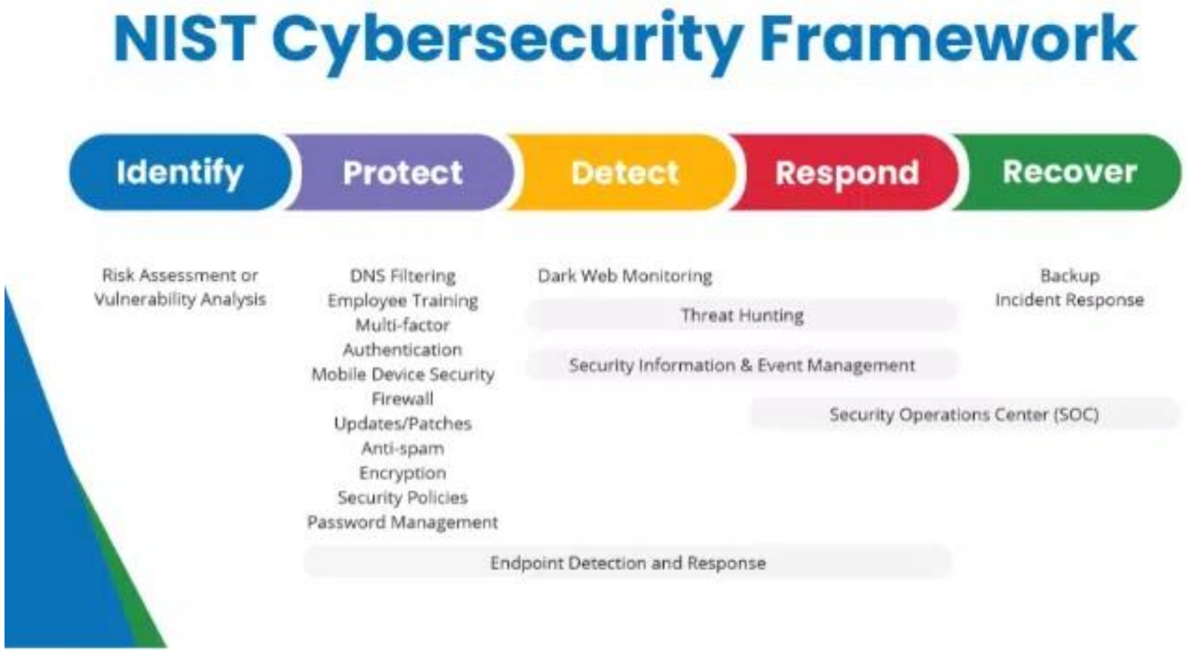


Figure 4 NIST Framework (Bocchino, 2022)

The security policies under the framework serve as the foundational element, help establish a clear and consistent approach to countering threats, and help create awareness among the people (Mijwil *et al.*, 2023). The first step in governance is identifying risk or risk assessment that focuses on identifying potential vulnerabilities, associated risks, and threats. Once the said risks are understood, policies would help the organization guide and implement the protective measures that would help mitigate or act proactively against the said threats on the internet. The assessment would include identifying the different information assets that could be affected by an attack and then identifying the risks that could impact these assets. Risk estimation and evaluation are usually followed by a selection of control that helps treat or find the identified risk. Monitoring and reviewing the risk environment to detect any changes is essential. The ISO 27001 provides a list of best practices for risk management. It addresses all aspects of cybersecurity, including processes, technology, and people. Some of these would include (Podrecca *et al.*, 2022; Junaid, 2023):

- Maintaining and establishing specific information risk criteria
- Ensuring repeated or continuous risk assessments are undertaken to produce consistent, comparable, and valid results.
- Identify the risk that might be linked with loss of confidentiality, availability, and integrity of information within the scope of the information security management system.
- Identify the owners of the various risks.
- Analyze and evaluate the risks based on the established criteria of threat importance and tolerance levels.
- Identify vulnerabilities that can be exploited.

Another critical aspect of governance is the definition of policies around access control, which specifies who would have access to the resources and under what conditions they would have this access, which helps safeguard sensitive information, applications, and systems from avoiding unauthorized access and potential security breaches (Chatterjee, Das and Sing, 2014; Cao, Lien and Liang, 2021). These strict requirements define how the access would be restricted and handled, and it would provide the organization with control over its resources by ensuring the users are genuine with regards to their identity and have proper corporate data access with the help of permission and authentication. There are many advantages to access control. For example, when there might be a data breach, access from one of the lower tier accesses would have minimal effect compared to the administrator account. In the regular scenario, without access control and having the same level of access, one mistake from one individual could entirely corrupt the entire system and cause much damage and loss for the company. Over the years, different types of access control have been implemented (Khilar, Chaudhari and Swain, 2019; Carruthers, 2022; Planas *et al.*, 2022). These include discretionary, mandatory, role-based, and attribute-based access control. The access control could be managed and configured centrally, depending on the company's needs. Different access levels are allocated to data, physical location, or individual. This would enable users to access or use the data, information, and location they require or are permitted to use. That said, this access comes only after an authentication process for the individual has been carried out.

Authentication is a fundamental process when it comes to access control. Here, the method is used to identify the individual attempting to access the system with which the rest of the information, like the type of application they would need access to, the type of information, their role, and work, are all linked. So unless the authentication is done, the individual would not be able to access the resources, and this is often done by having a dedicated login for each user with a separate username and a password of their choice (Cao *et al.*, 2023). This method is a single-factor authentication, and it does come with its challenges as the passwords can be hacked or traced, allowing the hackers to gain access. Another reason is that passwords often developed are weak and do not satisfy the password creation guidelines. This is mostly due to the lack of awareness among the people and also to ensure the ease of use as complex passwords would be hard to remember, and if they use these complex passwords, they would often leave traces of it which can be found and could cause the access to be compromised (Stobert and Biddle, 2014; Rainey, 2017). These limitations have led to two-factor authentication (2FA). In 2FA, Users are generally required to furnish two distinct kinds of authentication, commonly including knowledge-based factors (such as a password) and possession-based factors (such as a smartphone or a security token). This strategy offers a substantial improvement in security compared to single-factor authentication, which relies solely on a single type of verification (Pomputius, 2018; Zhang *et al.*, 2018). The principal advantage of 2FA is its efficacy in preventing unwanted access, even if an attacker successfully acquires a user's password. In the event of a compromised password, the attacker would still require the second factor to obtain access, significantly increasing the difficulty level for their success. The additional level of security is particularly advantageous in safeguarding confidential data, online accounts, and systems susceptible to illegal intrusion. The approach is extensively used and endorsed for many applications, such as email, banking, social media, and business networks, due to its substantial effectiveness in mitigating the likelihood of unauthorized access to user accounts (Zhang *et al.*, 2018).

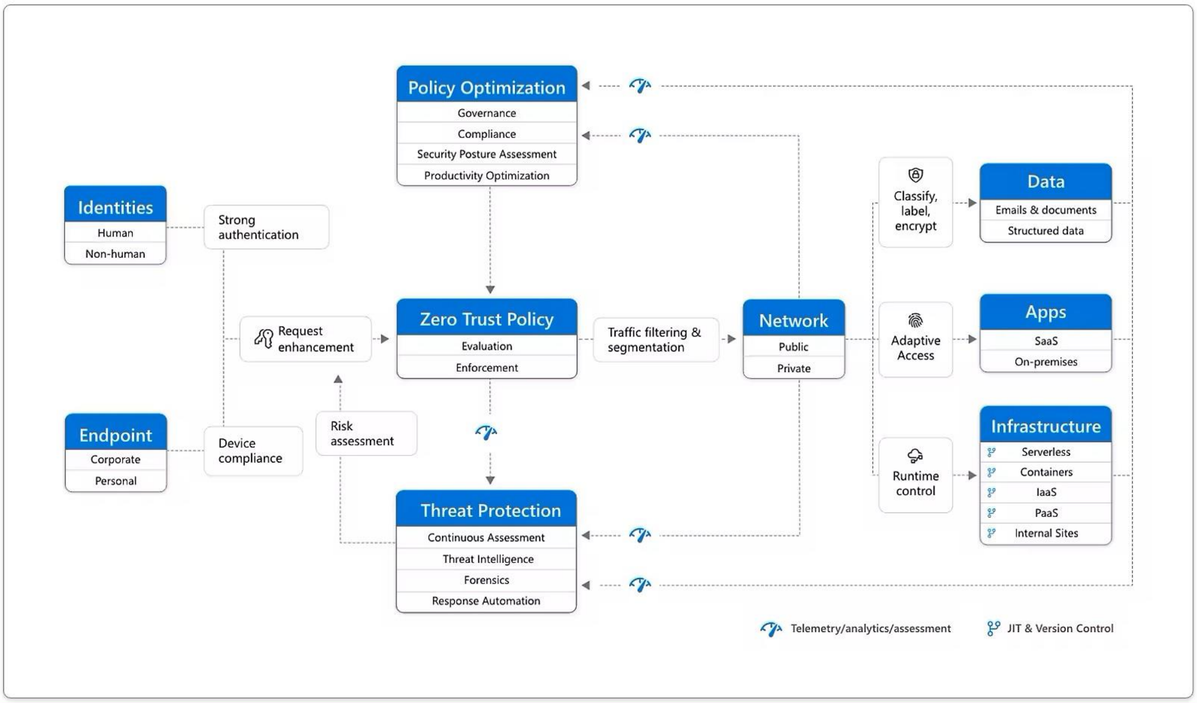


Figure 5 Zero trust architecture (Microsoft, 2022)

Over the years, there have been many concepts or frameworks that have been developed to improve access control and authentication, and one such is the Zero Trust framework. This is considered to be a high-level strategy that embraces proactive security. This approach challenges the traditional view of trust within the network and information security. The organization would assume that no user, system, or device can be trusted in the default setting, even if found within the corporate network (Delbene, Medin, and Murray, 2019; Rose et al., 2019; Mir and Ram Kumar, 2021). The trust would be evaluated continuously, and they are granted on a per-session basis or based on interaction requirements and are also controlled by different factors. The concept is based on the phrase “never trust, always verify.” A sample framework for the Zero trust is provided in Figure 5. Here, multi-factor authentication is used to ensure the users and devices are who they claim to be, and the principle of least privilege is applied to ensure that the users and devices have minimal access required to perform their tasks (Rose *et al.*, 2019). The networks are also divided into smaller segments that are said to limit the lateral movement of attackers in case of a breach. Dynamic access control is used in the system, which ensures access is granted based only on different contextual factors like identity, device health, location, and specific applications or resources requested for access. Thus, access control is critical in ensuring security and mitigating significant threats or issues.

3.4. Encryption

Another tool or technique that is used to improve overall security is encryption. It plays a fundamental role in safeguarding the security of the internet, fulfilling many essential duties that protect the secrecy, integrity, and validity of digital data. One of the principal functions of the process is to provide confidentiality by converting data into an incomprehensible form during transmission, rendering it unintelligible to unauthorized individuals who intercept it without owning the appropriate decrypt key (Xu, Qian and Hu, 2022; 'Encryption and Cybersecurity,' 2022). Protecting sensitive information, such as financial transactions, personal data, and passwords, is of utmost importance to ensure that only authorized individuals can access it. Furthermore, encryption assumes a crucial function in ensuring data integrity by validating the absence of any unauthorized alterations to information throughout its transit. The occurrence of any alterations made to data without proper authorization would lead to decryption failures, hence indicating the possibility of tampering. Furthermore, it plays a substantial role in the process of authentication and identity verification through the utilization of digital certificates and keys to validate the authenticity of websites, services, or individuals ('Encryption and Cybersecurity', 2022). This feature allows consumers to develop a sense of trust in their online interactions, reducing the potential hazards connected with impersonation and phishing assaults. In the current age of cloud storage and portable devices, encryption is crucial in safeguarding data at rest. This is achieved by encrypting the information kept on servers, databases, or devices, rendering it inaccessible to unauthorized individuals in the case of physical theft or breaches in data centers.

4. Awareness and its importance

Awareness is highly critical with the dynamic change seen in the current scenario. It is said to serve as a foundational defense, often again threats. Awareness is said to encompass educating individuals, organizations, and employees regarding the various risks and vulnerabilities within the digital realm and enable them to recognize any potential threat and also understand the best practices to mitigate them (Gioulekas *et al.*, 2022; Wong *et al.*, 2022). The importance of cybersecurity awareness cannot be overstated in the context of mitigating insider threats. A considerable portion of cybersecurity incidents involve individuals within an organization, often unintentionally. By implementing an awareness program, employees can enhance their comprehension of security policies, the repercussions of negligent behaviors, and the tactics employed by malicious insiders. Consequently, the risk of security breaches instigated by insiders is diminished (Gioulekas *et al.*, 2022). Furthermore, awareness plays a pivotal role in ensuring cybersecurity regulations and standards compliance. Numerous industries and organizations are subject to specific cybersecurity requirements, and maintaining compliance is not only a legal obligation but also a crucial element in upholding trust with clients and stakeholders. A well-informed workforce is more inclined to adhere to the requisite protocols.

Studies have highlighted that developing a culture that gives cybersecurity importance. One study highlights five initiatives in Australian organizations to improve the cyber security culture. This includes identifying key critical behaviors, establishing a champion to advocate movement and change, developing a brand for the team, building a security hub, and creating security awareness activities through internal and external campaigns. The said initiatives are said to have helped the organization exceed its standard compliance requirement and create a more functional culture that values cybersecurity (Alshaikh, 2020). It is mentioned that peer behavior and employee action experience in cybersecurity also play a critical role in improving an organization's awareness and cybersecurity behavior. It is recommended that the organization develop the culture by integrating a reward system that would help create a pro-security atmosphere. Those employees who follow the regulations and rules need to be encouraged, which would allow them to get clear cues from their peers. Organizations should also promote sharing experiences regarding mitigating risks and threats, which could be achieved in training programs but would add more depth and value to the people (Li *et al.*, 2016). In a controlled study, two groups of people were with one being provided a low-information awareness campaign on passwords and computer security. In contrast, the other group was provided with high information conditions that included every aspect of the risk, threat, and challenges and how to mitigate them. The findings show that the password strength of participants in the second group with the high information condition was stronger compared to the other group. This also highlights that security could be improved if individuals are trained, and a culture is created for awareness (McCrohan, Engel and Harvey, 2010). Thus, we can say awareness has a critical role in tackling Internet Security threats.

5. Conclusion

This comprehensive study on Internet security has delved into various aspects and components that play a critical role in safeguarding the digital realm. Internet security is not a static concept but a concept that, with technology, has evolved due to the increasing threats, making it highly dynamic. The dynamic nature also means there is a need for constant upgradation or change and increased vigilance to tackle a broad range of emerging and existing threats. This study has provided insights into the importance of internet security, including the various layers of defense, such as encryption, authentication, and access control. Additionally, it has highlighted the crucial role of cybersecurity governance in safeguarding our digital infrastructure. In light of the growing integration of the Internet into various aspects of our lives, such as online communication, cloud storage, remote work, and e-commerce, the significance of implementing strong Internet security measures has become increasingly crucial. By adopting the ideas elucidated in this research, companies and people may strengthen their defensive measures and effectively traverse the digital environment, guaranteeing the sustained preservation of data integrity, confidentiality, and availability, as well as enhancing online experiences.

References

Alazab, A. *et al.* (2012) ‘Using feature selection for intrusion detection system,’ in *2012 International Symposium on Communications and Information Technologies, ISCIT 2012*. Available at: https://doi.org/10.1109/ISCIT.2012.6380910.

Alfalah, A.A. (2023) ‘The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study,’ *International Journal of Advanced and Applied Sciences*, 10(4). Available at: https://doi.org/10.21833/ijaas.2023.04.017.

Alicea, M. and Alsmadi, I. (2021) ‘Misconfiguration in firewalls and network access controls: Literature review,’ *Future Internet*. Available at: https://doi.org/10.3390/fi13110283.

Alshaikh, M. (2020) ‘Developing cybersecurity culture to influence employee behavior: A practice perspective,’ *Computers and Security*, 98. Available at: https://doi.org/10.1016/j.cose.2020.102003.

Anwar, R.W., Abdullah, T. and Pastore, F. (2021) ‘Firewall best practices for securing smart healthcare environment: A review,’ *Applied Sciences (Switzerland)*. Available at: https://doi.org/10.3390/app11199183.

Asha, S., Shanmugapriya, D. and Padmavathi. G. (2023) ‘Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment,’ *Computers and Electrical Engineering*, 105. Available at: https://doi.org/10.1016/j.compeleceng.2022.108519.

Balarezo, J.F. *et al.* (2022) ‘A survey on DoS/DDoS attacks mathematical modeling for traditional, SDN and virtual networks,’ *Engineering Science and Technology, an International Journal*. Available at: https://doi.org/10.1016/j.jestch.2021.09.011.

Bluvector (2022) *The True Cost of Ransomware Goes Beyond the Ransom Payment*. Arlington, VA.

Bocchino, S. (2022) *UNDERSTANDING THE NIST CYBERSECURITY FRAMEWORK*, *WebIT*. Available at: https://www.webitservices.com/blog/understanding-nist-cybersecurity-framework/ (Accessed: 15 October 2023).

Cao, Y. *et al.* (2023) ‘Towards Nonintrusive and Secure Mobile Two-Factor Authentication on Wearables,’ *IEEE Transactions on Mobile Computing*, 22(5). Available at: https://doi.org/10.1109/TMC.2021.3133275.

Cao, Y., Lien, S.Y. and Liang, Y.C. (2021) ‘Deep Reinforcement Learning for Multi-User Access Control in Non-Terrestrial Networks,’ *IEEE Transactions on Communications*, 69(3). Available at: https://doi.org/10.1109/TCOMM.2020.3041347.

Carruthers, A. (2022) ‘Role-Based Access Control (RBAC),’ in *Building the Snowflake Data Cloud*. Available at: https://doi.org/10.1007/978-1-4842-8593-0_5.

Chatterjee, S., Das, A.K. and Sing, J.K. (2014) ‘A novel and efficient user access control scheme for wireless body area sensor networks,’ *Journal of King Saud University - Computer and Information Sciences*, 26(2). Available at: https://doi.org/10.1016/j.jksuci.2013.10.007.

Chaudhry, J.A., Chaudhry, S.A. and Rittenhouse, R.G. (2016) ‘Phishing attacks and defenses,’ *International Journal of Security and its Applications*, 10(1), pp. 247–256. Available at: https://doi.org/10.14257/ijsia.2016.10.1.23.

CISA (2020) ‘COVID-19 Exploited by Malicious Cyber Actors’, *National Cyber Awareness System* [Preprint], (April).

Cisco Systems (2021) ‘Cyber Security Threat Trends: Phishing, Crypto Top the List,’ *Cisco Systems Inc* [Preprint].

Clancy, M. (2021) *The True Cost of Ransomware*. Available at: https://www.backblaze.com/blog/the-true-cost-of-ransomware/ (Accessed: 17 September 2022).

Conti, M., Dragoni, N. and Lesyk, V. (2016) ‘A Survey of Man in the Middle Attacks,’ *IEEE Communications Surveys and Tutorials*. Available at: https://doi.org/10.1109/COMST.2016.2548426.

Dalal, R.S. *et al.* (2022) ‘Organizational science and cybersecurity: abundant opportunities for research at the interface,’ *Journal of Business and Psychology*, 37(1). Available at: https://doi.org/10.1007/s10869-021-09732-9.

Delbene, K., Medin, M. and Murray, R. (2019) ‘The Road to Zero Trust (Security),’ *Defense Innovation Board* [Preprint].

DİCLE, S.Z. (2022) ‘Man-In-The-Middle Attack,’ *European Journal of Science and Technology* [Preprint]. Available at: https://doi.org/10.31590/ejosat.1187984.

Dzurenda, P., Martinasek, Z. and Malina, L. (2015) ‘Network Protection Against DDoS Attacks,’ *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, 4(1). Available at: https://doi.org/10.11601/ijates.v4i1.103.

‘Encryption and Cybersecurity’ (2022) in *Blockchain for Real World Applications*. Available at: https://doi.org/10.1002/9781119903765.ch8.

Frayssinet Delgado, M. *et al.* (2021) ‘Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations’, *3C TIC: Cuadernos de desarrollo aplicados a las TIC*, 10(2). Available at: https://doi.org/10.17993/3ctic.2021.102.123-141.

Gibert, D., Mateu, C. and Planes, J. (2020) ‘The rise of machine learning for detection and classification of malware: Research developments, trends, and challenges,’ *Journal of Network and Computer Applications*. Available at: https://doi.org/10.1016/j.jnca.2019.102526.

Gioulekas, F. *et al.* (2022) ‘A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures,’ *Healthcare (Switzerland)*, 10(2). Available at: https://doi.org/10.3390/healthcare10020327.

Hsu, F.H. *et al.* (2012) ‘Antivirus software shield against antivirus terminators,’ *IEEE Transactions on Information Forensics and Security*, 7(5). Available at: https://doi.org/10.1109/TIFS.2012.2206028.

Humayun, M. *et al.* (2021) ‘Internet of things and ransomware: Evolution, mitigation, and prevention,’ *Egyptian Informatics Journal*. Available at: https://doi.org/10.1016/j.eij.2020.05.003.

Junaid, T.-S. (2023) ‘ISO 27001: Information Security Management Systems Management Systems’, *ResearchGate* [Preprint].

Khilar, P.M., Chaudhari, V. and Swain, R.R. (2019) ‘Trust-Based Access Control in Cloud Computing Using Machine Learning,’ in. Available at: https://doi.org/10.1007/978-3-030-03359-0_3.

Kim, G., Lee, S. and Kim, S. (2014) ‘A novel hybrid intrusion detection method integrating anomaly detection with misuse detection,’ *Expert Systems with Applications* [Preprint]. Available at: https://doi.org/10.1016/j.eswa.2013.08.066.

Kim, S. *et al.* (2020) ‘Secure Collecting, Optimizing, and Deploying of Firewall Rules in Software-Defined Networks,’ *IEEE Access*, 8. Available at: https://doi.org/10.1109/aCCESS.2020.2967503.

Kolesnikov, N. (2023) *50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who & What is Targeted*, *Techopedia*. Available at: https://www.techopedia.com/cybersecurity-statistics (Accessed: 11 October 2023).

Kuwatly, I. *et al.* (2004) ‘A dynamic honeypot design for intrusion detection,’ in *Proceedings - The IEEE/ACS International Conference on Pervasive Services, ICPS2004*. Available at: https://doi.org/10.1109/perser.2004.3.

Lehto, M. (2022) ‘APT Cyber-attack Modelling: Building a General Model,’ *International Conference on Cyber Warfare and Security*, 17(1). Available at: https://doi.org/10.34190/iccws.17.1.36.

Lella, I. *et al.* (2021) ‘ENISA threat landscape for supply chain attacks.’, *ENISA Publication* [Preprint].

Li, L. *et al.* (2016) ‘Cyber security awareness and its impact on employee’s behavior,’ in *Lecture Notes in Business Information Processing*. Available at: https://doi.org/10.1007/978-3-319-49944-4_8.

Liao, H.J. *et al.* (2013) ‘Intrusion detection system: A comprehensive review,’ *Journal of Network and Computer Applications* [Preprint]. Available at: https://doi.org/10.1016/j.jnca.2012.09.004.

Machado de Sousa, E., and Shahzad, A. (2022) ‘Data Loss Prevention from a Malicious Insider,’ *Journal of Computer Information Systems*, 62(6). Available at: https://doi.org/10.1080/08874417.2021.1980748.

Mallik, A. *et al.* (2019) ‘Man-in-the-middle-attack: Understanding in simple words’, *International Journal of Data and Network Science*, 3(2). Available at: https://doi.org/10.5267/j.ijdns.2019.1.001.

Martínez, J. and Durán, J.M. (2021) ‘Software supply chain attacks, a threat to global cybersecurity: SolarWinds’ case study,’ *International Journal of Safety and Security Engineering*, 11(5). Available at: https://doi.org/10.18280/IJSSE.110505.

McCrohan, K.F., Engel, K. and Harvey, J.W. (2010) 'Influence of awareness and training on cyber security,' *Journal of Internet Commerce*, 9(1). Available at: https://doi.org/10.1080/15332861.2010.487415.

Melaku, H.M. (2023) 'A Dynamic and Adaptive Cybersecurity Governance Framework,' *Journal of Cybersecurity and Privacy*, 3(3). Available at: https://doi.org/10.3390/jcp3030017.

Microsoft (2022) *Zero Trust defined*, *Microsoft*. Available at: https://www.microsoft.com/en-in/security/business/zero-trust#:~:text=Zero%20Trust%20is%20a%20high,if%20they%20were%20authenticated%20earlier. (Accessed: 15 October 2023).

Mijwil, M.M. *et al.* (2023) 'The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment,' *Mesopotamian Journal of Cyber Security* [Preprint]. Available at: https://doi.org/10.58496/mjcs/2023/001.

Mir, A.W. and Ram Kumar, K.R. (2021) 'Zero Trust User Access and Identity Security in Smart Grid Based SCADA Systems,' in *Advances in Intelligent Systems and Computing*. Available at: https://doi.org/10.1007/978-3-030-73689-7_68.

Mishra, A. *et al.* (2022) 'Cybersecurity Enterprises Policies: A Comparative Study,' *Sensors*, 22(2). Available at: https://doi.org/10.3390/s22020538.

NIST (2021) *Defending Against Software Supply Chain Attacks*.

Pérez-sánchez, A. and Palacios, R. (2022) 'Evaluation of Local Security Event Management System vs. Standard Antivirus Software,' *Applied Sciences (Switzerland)*, 12(3). Available at: https://doi.org/10.3390/app12031076.

Planas, E. *et al.* (2022) 'Towards Access Control Models for Conversational User Interfaces,' in *Lecture Notes in Business Information Processing*. Available at: https://doi.org/10.1007/978-3-031-07475-2_21.

Podrecca, M. *et al.* (2022) 'Information security and value creation: The performance implications of ISO/IEC 27001', *Computers in Industry*, 142. Available at: https://doi.org/10.1016/j.compind.2022.103744.

Pomputius, A.F. (2018) 'A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory,' *Medical Reference Services Quarterly*, 37(4). Available at: https://doi.org/10.1080/02763869.2018.1514912.

Rainey, C. (2017) *Starbucks Tells Hacked Customers to Create Better Passwords*, *Grub Street*. Available at: https://www.grubstreet.com/2017/05/starbucks-mobile-app-hacks-weak-passwords.html (Accessed: 19 October 2020).

Reznik, L. (2021) 'Firewall Design and Implementation,' in *Intelligent Security Systems*. Available at: https://doi.org/10.1002/9781119771579.ch2.

Rose, S. *et al.* (2019) 'Zero Trust Architecture', *Nist* [Preprint]. Available at: https://doi.org/https://doi.org/10.6028/NIST.SP.800-207-draft.

Scarfone, K. and Mell, P. (2007) ‘Guide to Intrusion Detection and Prevention Systems (IDPS),’ *National Institute of Standards and Technology* [Preprint].

Statista (2023) *Number of internet and social media users worldwide as of July 2023*, *Statista*. Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%202023&text=As%20of%20July %202023%2C%20there,population%2C%20were%20social%20media%20users. (Accessed: 10 October 2023).

Stobert, E. and Biddle, R. (2014) ‘The password life cycle: user behavior in managing passwords’, in *Proceeding SOUPS*.

Sudhakar and Kumar, S. (2020) ‘An emerging threat Fileless malware: a survey and research challenges,’ *Cybersecurity*, 3(1). Available at: https://doi.org/10.1186/s42400-019-0043-x.

Tassiulas, L. (2021) ‘Enabling Intelligent Services at the Network Edge,’ *ACM SIGMETRICS Performance Evaluation Review*, 49(1). Available at: https://doi.org/10.1145/3543516.3453912.

Thomas, K. *et al.* (2017) ‘Data Breaches, Phishing, or Malware?’, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: ACM, pp. 1421–1434. Available at: https://doi.org/10.1145/3133956.3134067.

Thornton-Trump, I. (2019) ‘The politics of cyber,’ *EDPACS*, 59(3). Available at: https://doi.org/10.1080/07366981.2019.1564193.

Wong, L.W. *et al.* (2022) ‘The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities,’ *International Journal of Information Management*, 66. Available at: https://doi.org/10.1016/j.ijinfomgt.2022.102520.

Xu, S., Qian, Y. and Hu, R.Q. (2022) *Cybersecurity in Intelligent Networking Systems*, *Cybersecurity in Intelligent Networking Systems*. Available at: https://doi.org/10.1002/9781119784135.

Zhang, J. *et al.* (2018) ‘T2FA: Transparent Two-Factor Authentication’, *IEEE Access*, 6. Available at: https://doi.org/10.1109/ACCESS.2018.2844548.

Zukis, B. (2022) ‘Digital and Cybersecurity Governance Around the World,’ *Annals of Corporate Governance*, 7(1). Available at: https://doi.org/10.1561/109.00000032.