Sergei Beliaev

Personal Cyber Security

Helsinki Metropolia University of Applied Sciences

Master's Degree

Information Technology

Personal Cyber Security

2023

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Sergei Beliaev Personal Cyber Security xx pages + x appendices 04 January 2023
Degree	Master's Degree
Degree Programme	Information Technology
Specialisation option	Networking and Services
Instructor(s)	Ville Jääskeläinen, Principal Lecturel

Cybersecurity has become a critical concern for individuals and society as a whole in today's constantly changing digital environment. As cyber threats grow in complexity and frequency, users are often the weakest link in the security chain.

This thesis explores the landscape of personal cybersecurity, examining current risks, common user behaviours, and available protective technologies. Emphasis is placed on the layered security approach known as "Defense in Depth," highlighting models such as the Cybersecurity Armadillo, which frames personal security through concentric layers—from endpoint and network protection to cloud services and governmental oversight.

The study investigates the roles and responsibilities of key stakeholders, including Internet Service Providers, device manufacturers, and software developers, in creating a safer internet experience. The thesis concludes by arguing that sustainable cybersecurity requires a shift toward system-level responsibility, which reduces the burden on end users while providing them more secure tools and environments.

Keywords	Internet, IT cyber security

Contents

Abbreviations/Acronyms

2FA = Two-Factor Authentication
ABAC = Attribute-Based Access Control
AES = Advanced Encryption Standard
BYOD = Bring Your Own Device
DiD = Defense in Depth
DLP = Data Loss Prevention
DNS =
DoS = Denial of Service
DRP = Disaster Recovery Plan
EDR = Endpoint Detection and Response
EPP = Endpoint Protection Platforms
GDPR = General Data Protection Regulation
HIPAA = Health Insurance Portability and Accountability Act
IAM = Identity and Access Management
IDPS = Intrusion Detection and Prevention Systems
IDS = Intrusion detection systems
IOT = Internet of Things
IPS = intrusion prevention systems
MDT = Mobile Threat Defense
MFA = Multi-Factor Authentication
OS = Operating Systems
PoLP = Principle of Least Privilege
PSK = Pre-Shared Key
RBAC = Role-Based Access Control
RPO = Recovery Point Objectives
RTO = Recovery Time Objectives
SAE = Simultaneous Authentication of Equals
SEM = Security Event Management
SIEM = Security Information and Event Management
SIM = Security Information Management
SSDLC = Secure Software Development Life Cycle
SOC = Security Operations Center
VLAN = Virtual Local Area Networks
VPN = Virtual Private Network

1 Introduction

Cybersecurity refers to the practice of protecting computers, networks, and sensitive information from unauthorized access, theft, damage, or other malicious activity. As technology continues to evolve, so does the importance of cybersecurity as cyber threats become more sophisticated and widespread.

One of the main reasons cybersecurity is so important is because of the increase of digital information. Data is becoming one of the most valuable assets of businesses and organizations, and it is imperative to protect it from cyberattacks. Cyber threats come in many forms, including viruses, malware, phishing scams and cyber espionage.

Another reason cybersecurity is so important is that it helps preserve privacy. In today's digital age, personal information is often stored on computer systems, and cybersecurity measures help keep that information confidential and protected from hackers.

Cybersecurity involves several components, including technology, processes and people. Using up-to-date software and hardware to protect against cyber threats is critical. It is also necessary to establish cybersecurity protocols and policies to prevent cyberattacks. Finally, educating employees and individuals about cybersecurity best practices can reduce the likelihood of successful attacks.

In summary, cybersecurity is an important measure for any organization or individual using digital technologies. With the increase in digital information and cyber threats, it is imperative to protect sensitive data and maintain privacy. By implementing cybersecurity measures, organizations and individuals can reduce the risk of cyberattacks and ensure the safety of their digital assets.

The purpose of this thesis is to investigate the effective implementation of corporate cybersecurity protocols for home users, while also considering the perspective that users are at the centre of protection irrespective of corporate aspects. As more individuals work remotely and rely on digital technologies for both personal and professional tasks, there is a growing need to adapt corporate cybersecurity practices to the home environment. This research aims to explore strategies for translating and implementing corporate cybersecurity rules and policies in a manner that is accessible, practical, and tailored

to the needs of home users. By examining the challenges and opportunities associated with extending corporate cybersecurity measures to home environments, this thesis seeks to provide insights and recommendations for enhancing cybersecurity practices among individuals outside the traditional corporate network.

To address the problem of implementing corporate cybersecurity rules for home users, the following approach was taken: a comprehensive review of existing literature was conducted to understand current practices and challenges in corporate cybersecurity. Case studies of organizations that have successfully implemented cybersecurity measures for remote workers were analyzed to identify best practices and lessons learned. Surveys and interviews were conducted with cybersecurity experts, corporate IT professionals, and home users to gather insights into effective cybersecurity practices and user behaviours.

The scope of the study is focused on providing practical recommendations for home users to enhance their cybersecurity posture, drawing upon insights from corporate cybersecurity practices. While it does not cover all aspects of cybersecurity, it aims to address the specific challenges faced by individuals working from home and provide actionable guidance for mitigating risks.

This thesis has been divided into five sections. The first section introduces the problem, outlines the research objectives, and explains the significance of the study. It sets the foundation for understanding the importance of cyber safety and the need for a user-centric approach to enhancing security.

The second section focuses on cyber safety, providing an overview of the current landscape of cyber threats and the challenges individuals and organizations face in maintaining security. It explores the evolving nature of cyberattacks and the increasing complexity of defending against them.

The third section presents the User-Centric Model (as a alternative Defence in Depth model). This model highlights the crucial role of end-users within the security framework, placing them at the core and building multiple layers of defense around them to minimize vulnerabilities. The model is designed to empower users with knowledge and tools to identify and mitigate potential threats.

The fourth section introduces the concept of the Cyber Security Armadillo, which serves as a metaphor for a robust and adaptable security framework. Inspired by the natural defense mechanisms of an armadillo, this approach emphasizes flexibility, resilience, and proactive threat detection.

The fifth section summarizes the key findings of the study and reflects on the implications of adopting a user-centric and layered defense model. It highlights how the proposed framework can enhance overall cyber resilience and reduce the impact of cyber threats. A conclusion that synthesizes the main insights from the research. It underscores the importance of continuous improvement in cyber safety strategies and suggests directions for future research and development in the field of cybersecurity.

2 Cyber Safety

Cyber safety, also known as online security or internet security, refers to the practice of protecting oneself and others from potential risks and threats in the digital world. It encompasses a set of measures and precautions that individuals, organizations, and communities can take to protect their online activities, personal information, and digital devices from various forms of cyber threats, including cyberbullying, identity theft, hacking, phishing, malware, and other cybercrimes.

Cyber safety pays close attention to one's online behavior and takes steps to minimize risks and protect oneself from potential harm. This includes understanding how to use technology safely, practicing good digital hygiene (viruses), being cautious about sharing personal information online, using strong and unique passwords, keeping software and devices up-to-date with the latest security patches, being vigilant against phishing and scam attempts, and being aware of the potential consequences of online activities.

In today's digital age, Internet safety has become a critical aspect of responsible online behaviour. Given our increasing reliance on the Internet for communication, information exchange, and financial transactions, it is imperative that we proactively protect ourselves from potential risk and harm.

Cyber security layers are a way to process and handle defense strategy of our virtual environment. Multiple layers of protection implemented in a computer system or network to protect against various cyber threats such as malware, hacker attacks, data breaches, and other cyber-attacks. These layers work together to create a layered defense mechanism that helps mitigate risk and protect the confidentiality, integrity and availability of digital assets.

Cyber threats are constantly evolving, and a single security measure may not be enough to prevent all types of attacks. By implementing multiple layers of security, organizations and societies can develop a multi-layered defense strategy that increases complexity for attackers and improves the overall security posture.

In today's cybersecurity landscape, multiple layers of security are essential to provide a comprehensive protection against a wide range of threats, increase resilience, ensure secure access, protect sensitive data, and enable timely detection and response to security incidents. These layers work together to create a robust and multi-layered defense

mechanism that helps organizations and average users mitigate risk and protect their systems, networks and data from cyber threats.

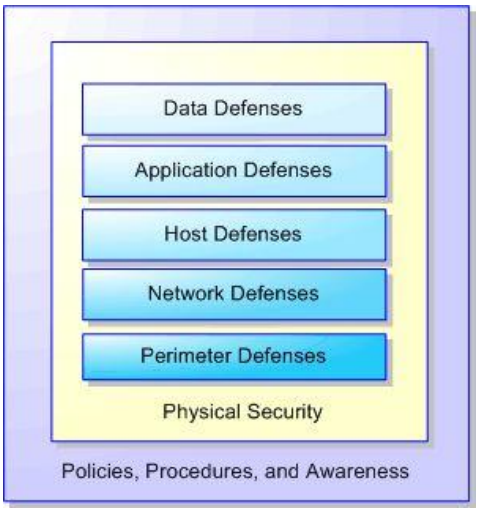
From a cybersecurity perspective, a more detailed view of the different levels of cybersecurity is presented in the following sections.

2.1 Defense in Depth

Cybersecurity layers refer to the implementation of multiple security measures in a system or network to create a strong defense against cyber threats. These layers can include defense-in-depth strategies, redundancy and resiliency measures, multi-factor authentication, encryption, security monitoring, and incident response processes.

Each layer provides additional protection and helps mitigate different types of risks such as unauthorized access, data breaches, system outages and other cyberattacks. By using multiple layers of security, organizations can create a comprehensive and robust cybersecurity structure that improves their overall security and minimizes the risk of successful cyberattacks.

There are several models of cybersecurity layers, but a commonly used framework is the Defense in Depth (DiD) model [1]. This model assumes that there should be multiple layers of security controls, each providing a different level of protection to mitigate the risk of a cyberattack. Here are the typical layers of the DiD model: Physical Security, Perimeter Security, Network Security, Host Security, Application Security, Data Security, Monitoring and Response.



Kuvio 1. Defence in Depth model. [6]

Defense in Depth (DiD) is a cybersecurity strategy that incorporates multiple layers of security controls to protect computer systems and networks from attack. The model assumes that no single security measure is perfect and therefore a combination of measures is required to provide comprehensive protection.

Each level of the Defense in Depth model should have its own set of controls that should be designed to work together. In addition, the model should be constantly reviewed and updated to adapt to changing security threats.

The first line of defense in a DiD strategy is usually perimeter defence. This includes digital measures such as firewalls and intrusion detection systems. The goal of perimeter security is to prevent unauthorized access to a network. Additionally, physical security measures are frequently incorporated into perimeter defense strategies. These measures may include secured entry points with locked doors, surveillance cameras for monitoring, and considerations for the physical location of assets or facilities.

The next level is network security, which includes measures to protect against threats that have penetrated the perimeter. This could include network segmentation to prevent lateral movement within the network and monitoring and anomaly detection tools to identify suspicious network activity.

Host security involves protecting individual devices such as computers and mobile devices, which is the next level of security. This can include antivirus software, device encryption and secure configuration. Endpoint security is particularly important given the rise of remote working, which have greatly expanded the number of potential entry points for attackers.

Application security involves securing individual software applications. This includes secure coding practices to prevent common vulnerabilities such as buffer overflows or SQL injection, and regular patches and updates to address known vulnerabilities.

Data defence as an Identity and Access Management (IAM) is also an important part of a DiD strategy. This involves ensuring that only authorized individuals have access to the network and that they can only access the resources required for their role. IAM measures can include strong authentication procedures such as two-factor

authentication, as well as regular auditing of access rights. The "Data" layer focuses specifically on safeguarding sensitive information from unauthorized access, manipulation, or disclosure. Data encryption involves converting plaintext data into ciphertext using cryptographic algorithms, rendering it unreadable to anyone without the appropriate decryption key. By encrypting data, organizations can ensure that even if unauthorized individuals gain access to the data, they cannot understand or exploit it without the decryption key.

Encrypting data adds an extra layer of security, especially when data is transmitted over networks or stored on devices susceptible to theft or unauthorized access. In addition to these layers, a good DiD strategy also includes business continuity and disaster recovery measures in the event of a successful attack. This could include regular data backups, incident response plans, and crisis communication plans.

DiD also requires regular monitoring and auditing to ensure that all layers of defense are functioning as intended and to identify potential areas for improvement. Given the rapidly evolving nature of cyber threats, a DiD strategy must be dynamic and adaptable, able to respond to new challenges as they arise.

While DiD is an effective strategy for mitigating cyber threats, it is not a panacea. No strategy can guarantee 100% security. Defense in Depth represents an approach to cybersecurity that is comprehensive, multi-faceted, and adaptable. It recognizes the complexity of the cyber threat landscape and the importance of defense on multiple fronts. By integrating a range of strategies and techniques, DiD offers a robust and resilient response to the challenges of cybersecurity.

2.2 Common Cyber Security Layers

Using the same principle as DiD, one gets a slightly different structure, if one puts the most important functions in the center of the model. This slightly different model is the Common Cybersecurity Layers model [4]. It is a set of standard security measures that are commonly used in the industry to protect against cyber threats. One of the most important parts of this model is the identification and protection of mission-critical resources.

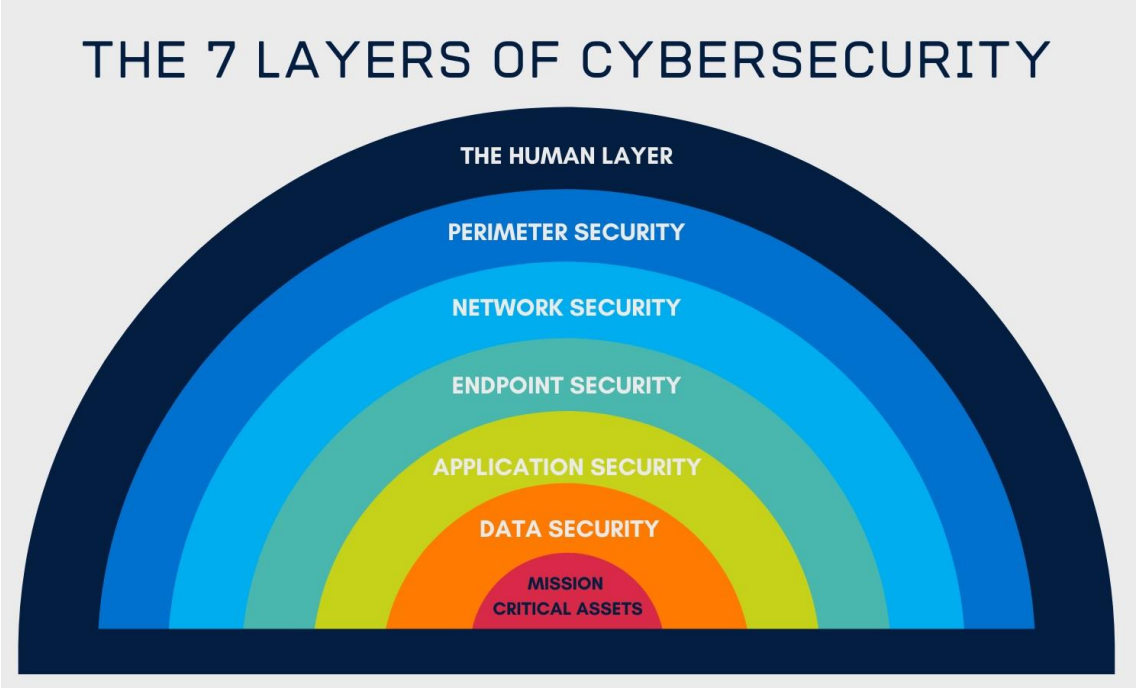
Business-critical assets are the most important components of a company's infrastructure and are essential to the effective operation of the business. These assets may

include sensitive data, intellectual property, financial information, or other information that is critical to the operation of the business.

The Common Cybersecurity 7 Layers model emphasizes the importance of identifying these assets and implementing specific security measures to protect them. For example, access controls and encryption can be used to ensure that only authorized personnel have access to these assets. Firewalls and intrusion detection systems can be used to monitor and prevent unauthorized access attempts.

Protecting mission-critical assets is important because they are often the target of cyberattacks. Cybercriminals attempt to steal, manipulate or destroy these assets to achieve their malicious goals. A successful attack on mission-critical assets can result in significant financial losses, damage to the company's reputation, and disruption of operations.

Therefore, the Common Cybersecurity Layers model recognizes the importance of identifying and protecting mission-critical assets as a critical part of any organization's cybersecurity strategy. By prioritizing the protection of these assets, organizations can reduce the risk of cyberattacks and mitigate the impact of successful attacks.



Kuvio 2. The Common Cybersecurity 7 Layers model. [4]

The Common Cybersecurity 7 Layers model refers to the categorization of security measures and protocols that operate at different levels of a network architecture to protect against cyber threats.

There are different orders, but the purpose and operation of the model remain the same. Following sections take a close look at each level.

2.2.1 Mission Critical Assets

Mission-critical cybersecurity assets are the most important and sensitive elements of an organization's digital infrastructure that are critical to its operation and success. These assets are typically identified as the most valuable, sensitive, or critical to the organization's mission, and their protection is paramount to ensuring business continuity, data integrity, and operational efficiency.

Mission-critical assets can include various components of an organization's infrastructure IT, such as servers, databases, applications, network devices, intellectual property, customer data, financial data and other sensitive information. These assets can be on-premise or in the cloud and are critical to the company's day-to-day operations, revenue generation, customer trust and competitive advantage.

Protecting mission-critical assets is an essential component of cybersecurity due to the increasing sophistication and frequency of cyber threats. Cyber attackers constantly target companies' valuable assets to gain unauthorized access, steal sensitive data, disrupt business operations, or cause financial or reputational damage. A successful attack on mission-critical assets can have serious consequences, such as financial losses, legal liabilities, brand damage, and loss of customer trust.

Organizations must implement robust cybersecurity measures to protect their mission-critical assets. This may include implementing layered defenses such as firewalls, intrusion detection and prevention systems, endpoint protection, access controls, encryption and continuous monitoring. In addition, organizations should have contingency plans and backup and recovery strategies in place to quickly detect, respond to and recover from cyberattacks targeting mission-critical assets.

“Mission Critical Assets”- layer usually have an actual physical location, such as servers, cloud services, open terminals, etc, one can call them a physical layer of data. Protecting the physical layer from a cybersecurity perspective is critical to protecting the integrity, availability, and confidentiality of a system's data and communications.

One can improve security by restricting physical access to critical infrastructure such as data centers, communications rooms, and network closets to authorized personnel only. Implement strong access control mechanisms, such as biometric authentication, smart cards, and access protocols to prevent unauthorized access.

Implement video surveillance, motion sensors, and other monitoring techniques to immediately detect and respond to physical security breaches. Monitoring physical access points, equipment rooms, and other critical areas in real time to detect and respond to unauthorized activity is also important.

2.2.2 Data Security

Data security is an important layer of cybersecurity that focuses on protecting data from unauthorized access, damage, theft, or loss. It involves implementing a combination of technical, organizational, and procedural measures to protect sensitive information, whether it is stored, transmitted, or processed. Data security is important to organizations, governments, and individuals because it helps ensure the confidentiality, integrity, and availability of data.

The classification and management of data allow organizations to implement appropriate security measures and access controls in accordance with their sensitivity and value. By implementing a well-structured framework to classify and manage sensitive data, organizations can minimize the risk of unauthorized access and data breaches by ensuring that sensitive data is appropriately protected.

In organizations, all data access is governed by access control. Access control mechanisms regulate who may access, modify, or delete data. These include user authentication, passwords, biometric authentication or multi-factor authentication and authorization, and role-based or attribute-based access control.

A password is the most common method of user authentication. Users create a unique combination of characters, numbers, and symbols that must be entered in correctly in order to gain access to a system. However, the reliance on passwords alone can pose a risk due to weak or reused passwords, phishing attacks, or brute-force attacks. To increase security, it is important to encourage users to create strong, complex passwords and to change them regularly.

The process of biometric authentication verifies a user's identity based on unique physical characteristics, such as fingerprints, facial recognition, or iris scanning. This method offers a greater level of security, as biometric data is more difficult to replicate or steal than a password. However, biometric authentication can be subject to false positives or negatives and raise privacy concerns, since biometric data can potentially be misused if not properly stored.

With multi-factor authentication (MFA), two or more different authentication methods are combined, substantially enhancing security by requiring multiple layers of verification. A user may use a password as a factor, something they possess (e.g., a mobile device or a hardware token), or something they are (e.g., biometric information).

Authorization as a role-based access control system (RBAC) assigns access rights based on roles within an organization instead of individual users. The roles are accompanied by a set of permissions which define the actions that can be taken on specific resources. By modifying roles instead of updating individual user accounts, RBAC simplifies access control management.

Authorization as an attribute-based access control policy (ABAC) defines access control policies based on the attributes associated with users, resources, and the environment. These attributes may include factors such as job titles, locations, or times of the day. As policies can be easily modified to meet changing organizational needs, ABAC provides an approach to access control that is more dynamic and granular.

Encryption of data is an important aspect of cybersecurity. It provides a solid layer of protection to safeguard sensitive information from unauthorized access and potential cyber threats. It involves converting plaintext data into a complex, unreadable format (ciphertext) using sophisticated algorithms and encryption keys. The encryption process ensures that the data remains secure, as it can only be accessed by those who have the

appropriate decryption key to convert it back to its original form. Data breaches and cyber-attacks have become increasingly common in the digital age, making data encryption a necessity for businesses, governments, and individuals. Data that is encrypted can be protected, kept private, and the organization can adhere to regulatory requirements, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [3]. There are various techniques of encryption available, such as symmetric key algorithms (e.g., Advanced Encryption Standard (AES)) and asymmetric key algorithms (e.g., RSA) [3]. Asymmetric key encryption uses a public key for encryption and a private key for decryption, while symmetric key encryption uses the same key for encryption and decryption. There are advantages and disadvantages to each method, and the choice is dictated by the organization's or individual's specific security needs and resources. As opposed to asymmetric key algorithms, symmetric key algorithms are faster and easier to implement, but they require that both parties share a secret key. While asymmetric key algorithms are slower and more complex, they do not require a shared secret key, which makes them more secure. Symmetric key algorithms are also susceptible to brute force attacks, whereas asymmetric key algorithms are more resilient to such attacks.

Additionally, end-to-end encryption has become increasingly popular in communication platforms, providing privacy by ensuring that only the sender and recipient can access the message content. The encryption of data is a crucial component of cybersecurity, as it prevents unauthorized access to sensitive information, helps maintain privacy, as well as enables compliance with regulations.

Data backup and recovery is a crucial aspect of information security and risk management to ensure the continuity of business when data is lost, a system fails, or natural disasters occur. Developing a disaster backup and recovery strategy requires two key components: regular backups of critical data and a comprehensive disaster recovery plan.

By regularly backing up critical data, an up-to-date copy of essential information is readily available in case of data loss, corruption, or system failures. A variety of backup techniques can be performed, depending on the organization's needs and resources, including full backups, incremental backups, and differential backups. In order to protect backup data from potential onsite disasters, it is necessary to store it offsite or in a secure cloud environment.

A disaster recovery plan (DRP) outlines the necessary steps and procedures to follow in the event of a data loss, system failure, or other disruption. Prioritizing critical systems and processes during recovery and defining recovery personnel's roles and responsibilities. To minimize downtime and data loss, one needs to define recovery time objectives (RTOs) and recovery point objectives (RPOs). One should also implement alternative communication channels, temporary work locations, or remote work capabilities to maintain business operations during recovery. Making sure the plan remains effective and adapts to changing business needs must be followed.

2.2.3 Application

The application layer is critical to the overall security of an organization because it serves as the primary interface between users and their digital assets. This layer includes web applications, mobile applications, and desktop applications that users use to interact with underlying systems, networks, and databases. Consequently, the application layer becomes a prime target for cybercriminals who exploit vulnerabilities in applications to gain unauthorized access to sensitive data, disrupt operations, or compromise systems.

The particular challenges faced by the application layer can be attributed to its high level of visibility and accessibility. Cyber attackers often exploit software vulnerabilities, unsafe coding practices, and poor access control measures to gain unauthorized access to applications. In addition, the application layer is also vulnerable to social engineering attacks such as phishing and spear phishing campaigns that exploit human error and psychological manipulation to trick users into divulging sensitive information or installing malware.

To mitigate these risks and to ensure robust application-level security, organizations must take many steps and investments. One of many is secure software development practices, such as the Secure Software Development Life Cycle (SSDLC) [7], which focuses on integrating security measures throughout the software development process. This approach emphasizes regular security testing, code reviews and vulnerability assessments to identify and address potential security vulnerabilities in applications before they can be exploited.

Organizations need to continuously monitor their application environments to identify and respond to potential security incidents in a timely manner. This can be achieved by using security information and event management (SIEM) tools and establishing a dedicated security operations center (SOC) that continuously analyzes application logs and network traffic for potential threats [8].

By adopting secure software development practices, implementing strong access control measures, promoting security awareness among employees, and continuously monitoring application environments, organizations can effectively protect their digital assets and reduce the likelihood of successful cyberattacks.

Identify and document security requirements may include legal and regulatory requirements, data privacy considerations, and specific security features such as encryption or two-factor authentication.

Determining the security architecture is necessary. Threat modelling is often performed to identify potential security risks so that mitigations can be incorporated into the design. Developers write the software, adhering to secure coding guidelines to avoid common vulnerabilities such as buffer overflows or injection attacks. Static code analysis tools are often used to automatically detect potential security problems [9]. Software is tested for functionality and security. This often includes both dynamic analysis (such as penetration testing or fuzz testing) and code reviews. Software is deployed in a secure environment with appropriate access controls, monitoring and logging capabilities.

Regular updates and patches are applied to the software to address new threats. Incidents are responded to and lessons learned are incorporated into future development.
The SSDLC aims to identify and mitigate security issues early, as they are usually cheaper and easier to fix. It also aims to develop software that is secure by design, rather than relying on additional security measures or patches. The SSDLC is therefore a key component of a proactive, preventive approach to software security.

Security Information and Event Management (SIEM) is a type of software solution that provides a holistic view of an organization's information security. SIEM systems collect, analyze and present information from various sources in IT infrastructure.

SIEM solutions combine two product categories: SIM and SEM. Security Information Management (SIM) are designed for long-term storage, analysis and reporting of log data and Security Event Management (SEM) focus on real-time monitoring, event correlation and incident response.

SIEM software collects data from multiple sources in a IT environment, including network devices, servers, domain controllers and more. This can include logs, events and other data. As data comes in different formats, the SIEM solution normalizes this data to make it easier to analyze. The SIEM software analyzes the data for abnormal activities that could indicate a security threat. It uses predefined correlation rules, as well as machine learning and statistical analysis, to identify patterns of activity that could indicate an attack, security breach, or unauthorized access. When the SIEM system identifies a potential security issue, it sends an alert with detailed information about the activity to security analysts in an organization. SIEM solutions provide dashboards for security teams to monitor events and alerts in real time. They also have capabilities for generating detailed reports on security-related incidents and events. When a security incident occurs, historical data stored by the SIEM can be used to investigate how the breach occurred, what the attacker did, and how to prevent similar attacks in the future.

SIEM systems are thus important tools in the arsenal of security teams, helping them to detect, prevent and respond more effectively to security incidents. They also help with compliance reporting and incident investigation, making them invaluable in the modern cybersecurity landscape.

2.2.4 Endpoint Security

Endpoint security, also known as endpoint protection, is a critical aspect of enterprise cybersecurity strategies. It refers to the approach to protecting an enterprise network accessed through remote devices such as desktops, laptops, servers and mobile devices. Any device that connects to the network is a potential entry point for security threats. Therefore, endpoint security is designed to protect these access points from risky activities or malicious attacks.

Endpoint security has evolved significantly over the years. The focus is no longer on protecting individual devices, but on a holistic approach that emphasizes network-wide security [10]. This shift has been driven primarily by changing ways of working, including

increased remote working, the use of personal devices for work purposes (also known as Bring Your Own Device, or BYOD), and the growing popularity of cloud services.

At its core, endpoint security aims to protect any endpoint that connects to a network from potential threats. These endpoints include laptops, desktops, cell phones, tablets, servers and even Internet of Things (IoT) devices. Each of these devices represents a potential entry point that can be exploited by malicious actors to gain access to the network. Endpoint security solutions include several key components in order to prevent such an event from occurring.

Endpoint Protection Platforms (EPP) are comprehensive security solutions that include a variety of protection features such as antivirus, anti-malware, data encryption, personal firewalls, intrusion detection and more [11]. While traditional EPP solutions were focused on on-premises network security, the rapid adoption of cloud computing has led to the development of cloud-based EPP solutions. These offer a number of advantages, such as scalability, easier management, and real-time updates.

Endpoint Detection and Response (EDR) solutions continuously monitor endpoints for signs of cyber threats [11]. EDR is a newer component of EPPs, providing increased visibility into endpoint data and potential security threats. EDR capabilities enable the monitoring and recording of endpoint and network events, and storing the information in a centralized database where further analysis, detection, investigation, reporting, and alerting take place.

Mobile Threat Defense (MTD) is a security solution designed to protect enterprise networks and data from a variety of threats, vulnerabilities, and risky behaviors that can occur on employees' mobile devices. [12]

Data loss prevention (DLP) solutions are designed to prevent unauthorized users to send sensitive data outside the network [13]. These solutions work by identifying, monitoring, and protecting data in use, in transit, and when it is stored on desktops, laptops, phones, and tablets. Organizations can effectively control and monitor the flow of data, ensuring that it remains secure and is only accessed by authorized individuals.

Patch management: this includes managing updates or patches to software applications. Regular updates and patches of software are important to protect against vulnerabilities that could be exploited by hackers.

Device Control: This protects the system by restricting access to external devices, such as USB drives, that could potentially contain malicious software.

Application control/whitelisting: this involves restricting the applications that can run on a system by allowing only approved or whitelisted applications. This can prevent malware and other unauthorized software executed.

Endpoint protection therefore plays an important role in the overall cyber defense strategy by providing security at the device level, reducing the risk of threats entering the network through vulnerable devices.

2.2.5 Network Security

Network security refers to the practices and policies designed to protect the integrity, confidentiality, and accessibility of computer networks and data [14]. Given the increasing scale and sophistication of cyber threats, a robust network security system has become essential for any organization, regardless of size or industry.

Network security operates on multiple levels, using a combination of hardware and software solutions to protect the network and its traffic. It involves a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data, using both hardware and software technologies.

By implementing a range of strategies and techniques during the design phase, cyber-secure design aims to limit the potential damage and lateral movement within a network in the event of a security breach.

The segmentation of a network is one of the key strategies, as it involves splitting the network into smaller, isolated segments [15]. Each segment is secure with its own set of controls and operates independently. As a result, an attacker who gains access to one segment is restricted to that area and cannot easily move to other parts of the network.

Segmentation can be achieved through various means, including Virtual Local Area Networks (VLANs), subnetting, or firewalling [16].

Another important strategy is the principle of least privilege (PoLP), which ensures that users, systems and applications have only the minimum access rights required to perform their functions [17]. By limiting access rights, the potential damage of a security breach can be significantly reduced. For example, if a user's account is compromised, the attacker can only access the data and systems that the user is authorized to access.

Adding access controls to a secure network design is also important. They manage the access rights of individuals and what they can do once inside the network. Authentication of users includes verifying their identities and authorizing them to access specific resources in accordance with their responsibilities and roles.

Regular audits and penetration testing are critical to maintain the security of the network. These practices help to identify potential vulnerabilities and evaluate the effectiveness of existing security measures. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are used to monitor network traffic and identify suspicious activity [18]. These systems can detect potential security threats and take action to prevent them from spreading through the network.

Network security design involves a holistic approach that aims not only to prevent breaches, but also to limit the potential damage if a breach does occur. It is about creating a network that is not only secure, but also resilient and adaptable to the ever-evolving cyber threats.

2.2.6 Perimeter Security

The first line of defense in a layered cybersecurity approach is perimeter security. As a barrier, it protects internal networks and sensitive data from external threats and acts as a barrier to external threats. Its goal is to prevent unauthorized access to the network, detect intrusion attempts, and provide a response mechanism when a threat is detected. A perimeter must be defined before it can be secured. An important aspect of defining a network perimeter is to identify all points of entry. There are several types of connections one can use to connect to the network, including internet connections, remote access points, wireless access points, and physical connections, such as USB ports.

Additionally, this applies to any device that is permitted to connect to the network, including employee laptops, smartphones, and third-party devices.

In order to monitor and control these entry points, security measures can be implemented to the defined entry points. Firewalls, intrusion detection and prevention systems, secure gateways, and network access control systems may be used to do so. By controlling access and monitoring for malicious activity, each of these components contributes to secure the perimeter.

However, today, the process of defining a network perimeter has become increasingly difficult. Taking into account cloud computing, mobile computing, and the Internet of Things (IoT), the traditional concept of a well-defined, rigid perimeter around a network has become less common. Due to this change, the cybersecurity industry is moving toward models such as Zero Trust, which assume that no device or user is implicitly trusted, inside or outside the perimeter [19]. In these modern approaches, the focus is more on securing individual resources rather than a defined perimeter. This involves stronger identity verification, granular access controls, and continuous monitoring and assessment of network activity.

Perimeter security has evolved into perimeterless security. As a result of a perimeterless security model, the primary focus has shifted away from defending a single perimeter and has moved toward protecting data spread throughout the network, devices, and cloud. By assuming breaches can and will occur, this model emphasizes limiting the damage they can cause and detecting breaches as quickly as possible rather than focusing solely on preventing them.

2.2.7 The Human Layer

People are often referred to as the weakest link in security, as reiterated in cybersecurity circles. Although firewalls, encryption systems, and intrusion detection systems are often highly sophisticated, human behavior often decides between a secure operation and a major data breach. Understanding and addressing the human component of cybersecurity is not only advisable, but it is essential to create a cybersecurity framework that is effective.

A human layer in cybersecurity refers to the individuals who interact with systems and networks under protection. As the first line of defense against potential threats, this layer also represents the greatest vulnerability in any cybersecurity strategy because it is simultaneously the most significant.

Threats to the human layer are frequently categorized into two main categories: insider threats and social engineering [21]. An insider threat is a threat that occurs when an individual within the organization acts negligently or maliciously. In contrast, social engineering attacks, such as phishing, baiting, and pretexting, utilize human psychology to manipulate individuals into divulging confidential information, thus breaching security protocols.

Insider threats are a significant cybersecurity concern since they involve individuals within an organization who have legitimate access to data and systems. Employees, contractors, or partners with access rights to the organization's network, applications, and databases can pose threats, either maliciously or unintentionally, which result from activities that violate an organization's cybersecurity policies.

Individuals with an intent to harm the organization are responsible for malicious insider threats. In addition to stealing sensitive data for personal gain, malicious insiders may perform sabotage to disrupt operations, or damage the organization's reputation by committing sabotage. In addition to exfiltrating trade secrets, deliberately introducing malware into the system, or deleting critical data, motivations may range from financial gain to disgruntlement or revenge. An 'Unintentional Insider Threat' occurs when an individual unknowingly compromises security through their actions. It may include falling victim to phishing attacks, misconfiguring security settings, using weak passwords, or unintentionally sharing sensitive information. Although there is no malicious intent, the damage caused by such actions can be just as significant.

In contrast to other forms of cyberattacks, social engineering attacks directly target the human layer of cybersecurity and exploit human psychology to gain access to sensitive information or systems. Social engineering attacks are based on tricking individuals into breaking normal security protocols rather than exploiting software or hardware vulnerabilities. Some types of social engineering attacks include Phishing, Pretexting, Baiting, Quid Pro Quo Attacks and Piggybacking [22]. All those deceptive tactics used by cybercriminals to exploit individuals and gain unauthorized access to sensitive information or

systems. When cybercriminals obtain information or gain unauthorized access, they may use that information for various purposes, including identity theft, financial fraud, unauthorized transactions, espionage, data breaches, malware dissemination, or even the sale of the information on the dark web, perpetuating their malicious activities and causing harm to individuals, businesses, and organizations.

The first and most important aspect of addressing these challenges is the creation of a robust cybersecurity culture through employee awareness programs and training. Addressing these challenges necessitates a multifaceted approach that goes beyond traditional technical solutions. The training programs should not only provide a general understanding of potential threats and how to mitigate them, but they should also motivate each individual to take an active role in maintaining security as well.

In addition, organizations should create comprehensive security policies that outline how sensitive information should be handled and outline the procedures to follow in case of a security incident, defining acceptable and unacceptable behavior. All staff members should be informed of these policies on a regular basis.

To effectively manage the human layer, it is also necessary to focus on insider threats. This can be addressed through the implementation of strict access controls, which ensure that individuals have access to only the data required to perform their duties. Furthermore, robust user activity monitoring can assist in identifying and mitigating potential threats as a result of identifying abnormal or suspicious behavior.

Humans are not only responsible for identifying threats and vulnerabilities, but they are also the most powerful resource for enhancing cybersecurity. They are responsible for establishing, implementing, and managing security technologies. It is their skills, knowledge, and creativity which are driving the ever-evolving field of cybersecurity.

A key component of empowering the human layer is investing in continuous education and skill development. The promotion of cybersecurity certifications and the provision of opportunities for employees to learn about the latest trends and threats can help an organization enhance its cybersecurity posture.

An effective cybersecurity strategy relies heavily on the human layer. An effective human layer strategy includes the establishment of a culture of security, the implementation of

clear security policies, the proactive management of insider threats, and the empowering of individuals through continuous education. Organizations can strengthen their cyber-security frameworks by focusing on the human layer, which enables them to adapt to the constantly changing threat landscape in a way that is resilient.

2.3 Defence in Depth Summary

To conclude, cyber security on the business side may be summed up as the result of many factors, no single security measure is able to limit or, more importantly, make safety available critical information whenever it is needed. Several tactics, techniques, and strategies are required to achieve complete cybersecurity in business. It is important to understand that no one measure can provide a comprehensive level of protection.
The following are some basic principles that should be reviewed.

Risk Management - The cornerstone of a comprehensive cybersecurity strategy is risk management. It involves identifying potential threats to your organization and assessing their impact on your business. Upon identification of these threats, you develop strategies for managing them, which may involve transferring the risk to another party, avoiding the risk, reducing its negative effect or probability, or even accepting some or all of the risks' actual or potential consequences.

Security Architecture and Design - Designing secure network infrastructure and systems involves incorporating features such as firewall configuration, secure server design, secure coding practices, and implementing secure communication protocols into network infrastructure and systems.

Security Awareness Training - The weakest link in security is usually a person, rather than a piece of software or hardware. Phishing attacks, in which the attacker tricks the user into disclosing sensitive information, can be particularly damaging. Employees can be taught to recognize and avoid these attacks through regular training.

Data Protection - There are many aspects of data protection that must be considered, including techniques such as encryption, which encrypts data into a format that cannot be decrypted without a decryption key. Access controls are also crucial, where certain information is only accessible to authorized users.

Patch Management - Managing patches is an important aspect of software security. Updates, or patches, are issued regularly by software developers to correct security vulnerabilities. It is imperative to apply patches as soon as possible to prevent attackers from exploiting these flaws.

Regular Audits and Assessments - It is important to conduct regular audits and assessments of your system to identify any weaknesses or areas that need to be improved. This may also include penetration testing, where, to identify any security vulnerabilities, cybersecurity professionals attempt to breach your system.

Vendor Management - You should ensure vendors follow good security practices as well. A breach in one of your vendors' systems may result in a breach in your own.

Intrusion Detection and Prevention Systems (IDPS) - A system for detection and prevention of intrusions (IDPS) monitors network traffic and can detect potential attacks. When an attack is detected, the system can take measures to prevent or mitigate the attack.

Security Policies - A security policy is a set of rules and procedures that everyone in a company should follow to ensure that their data is safe. These rules may include password complexity requirements, procedures for handling sensitive information, and policies for the use of company-owned devices.

Following table explains different techniques involved in layers in terms of Cyber Security data protection.

Implementing multiple layers of cybersecurity measures can provide a defense-in-depth strategy that makes it more difficult for cybercriminals to penetrate a system or network and reduce the risk of a successful cyberattack. It is important to regularly update and monitor these layers to keep up with evolving cyber threats and ensure the continued security of your digital assets.

3 User Centric Model

Cyber threats are prevalent and evolving in a digitally connected world, making individuals' involvement in cybersecurity increasingly crucial. Users are the first line of defense against cyber-attacks. By understanding the importance of cybersecurity and implementing best practices, individuals can significantly contribute to protecting their personal information, privacy, and overall digital well-being by implementing best practices.

Effective cybersecurity relies on user awareness. By providing information about common cyber threats, including phishing, malware, social engineering, and identity theft, individuals are able to identify potential risks and take preventative measures to minimize them. Disseminating information about emerging threats and best practices can be facilitated by awareness campaigns, workshops, and online resources.

Users must understand the importance of strong and unique passwords, regularly updating software and applications, enabling two-factor authentication, and exercising caution when sharing personal information online. They should also learn to identify suspicious emails, websites, and messages so that they may avoid becoming victims of scams or malicious activities. Individuals should take responsibility for their own security by adopting safe digital practices. Regularly backing up data, employing robust security software, and keeping systems up to date are vital steps in protecting against malware and data loss. Users should exercise caution while downloading files, clicking on links, or accessing unknown websites.

It's crucial to uphold responsible online behaviors. Users must exercise caution when sharing personal information on social media platforms, refraining from oversharing details that could be exploited by cybercriminals. Practicing good digital hygiene further enhances protection. This includes logging out of accounts after each use, steering clear of public Wi-Fi networks for sensitive transactions, and leveraging encrypted communication channels. Additionally, users should hone critical thinking skills to assess the reliability of online information. By exercising skepticism and verifying the authenticity of sources, individuals can steer clear of falling prey to misinformation or online scams.

The user-centric approach emphasizes the importance of collaboration and knowledge sharing within communities. The user can exchange information, share experiences, and learn from experts by participating in online forums, cybersecurity communities, and

social media groups. Users can benefit from engaging in discussions regarding emerging threats, software vulnerabilities, and best practices.

Additionally, users should notify appropriate authorities or organizations as soon as possible about suspicious activities, phishing attempts, and security breaches. Users who report such incidents to appropriate authorities or organizations contribute to the collective effort of identifying and mitigating cyber threats, ultimately resulting in a safer digital ecosystem.

In order to remain vigilant and adaptive to cyber threats, users should prioritize constant learning and staying up to date on the latest cybersecurity trends, attack vectors, and protective measures. You can get valuable insights and updates by subscribing to cybersecurity newsletters, following reputable blogs, and attending webinars or conferences.

By fostering user awareness, promoting education, and encouraging proactive engagement, individuals can significantly contribute to the collective defense against cyber threats. Empowered users who adopt responsible digital practices, collaborate with others, and continuously learn and adapt can create a more secure digital environment. The user-centric model recognizes that cybersecurity is a shared responsibility, where every individual has the power to make a positive impact and safeguard their own digital well-being and that of the broader community.

User as a critical asset: one of the key reasons for the importance of users is their ability to act as the first line of defense against cyber threats. Even though organizations and service providers employ various security measures, users are often the ones who detect the initial signs of a breach. It is important for users to be cautious when receiving unexpected requests for personal information, and to examine suspicious emails, check for anomalies in website addresses, and to be alert to suspicious website addresses. As long as users remain vigilant and informed, they can prevent the success of phishing attacks, protecting their own data and alerting others to emerging threats. In many cases, users are the weakest link in cybersecurity, so as an alternative perspective, they should be considered as a critical asset, and the rest of the cybersecurity layers should be designed to protect them. Under this perspective, cyber security is viewed as a more human-centered issue rather than just a matter of technology. Given the complexities of human behavior, it's imperative to devise a solution framework that seamlessly

integrates both human nature and technical safeguards.. A guideline surrounded by armor of technical solutions. Cybersecurity becomes more human-centered, highlighting the need to integrate human nature and technical protections to create a robust defense system against cyber threats. Human nature is complex, and it plays a crucial role in the field of cybersecurity. Understanding the psychology, motivations, tendencies, and vulnerabilities of individuals is a key aspect of developing effective cybersecurity strategies.

4 Cyber Security Armadillo

Similar to the Defense-in-Depth (DiD) model, this thesis operates on the principle of protecting a core by employing layers of defense. In this context, the "core" pertains to the user. Within the realm of cybersecurity, the concept of "Armadillo Belts" draws parallels to the layers or protective shells found in armadillos. It symbolizes the array of defense mechanisms and security measures individuals should adopt to fortify their cybersecurity. These belts of security help fortify the core.

Each "Armadillo Belt" symbolizes a distinct layer of defense, with its unique set of security protocols and strategies. Here are layers to consider:

- Endpoint Security: Devices and there's OS and applications
- Network Security: user friendly network and safety parameters.
- Cloud Security and Digital Footprints: Investigating Digital Identity and Footprints.
- Operator and Government: Accountability for User Security

4.1 Cyber Security Armadillo: Endpoint Security

In the term "Endpoint security," although we find the word "end", but for users, their journey into the digital realm often starts at this endpoint, what is a computer or another digital device. That digital device must be the first line of defense, ensuring safety while remaining user-friendly. It should be fortified against attacks, yet provide seamless access to all its features.

A wide array of endpoint devices can be categorized into three main groups: user's computers, user's mobile devices, and user's IoT devices. User's computers typically include desktops, laptops, and workstations, serving as primary tools for various tasks such as work, entertainment, and communication. User's mobile devices encompass smartphones and tablets, offering mobility and flexibility for accessing information, applications, and services on the go. User's IoT devices represent a diverse range of interconnected gadgets and sensors, including smart home appliances, wearable devices, and industrial sensors, facilitating automation, monitoring, and control in various environments. Each group presents unique security challenges and considerations, emphasizing the importance of robust endpoint security measures to safeguard against evolving cyber threats and vulnerabilities.

Upon closer examination of the user's computer group, it becomes evident that the demarcation between desktop and laptop computers has diminished significantly in contemporary contexts. Moreover, considering the portability aspect of laptops, it can be revied as a mobile device.

Mobile devices include a diverse range of portable electronic gadgets designed to facilitate communication, productivity, entertainment, and various other functions while on the move. Here are some common types of mobile devices: Smartphones, Tablets, Laptops, Smartphones, Wearable Devices and Gaming Device.

Many of them are handheld devices that combine the functionality of a mobile phone with advanced computing capabilities. They typically feature touchscreen interfaces, internet connectivity, cameras, and support for a wide range of applications (apps) for tasks such as email, web browsing, social media, and multimedia consumption.

The fundamental principle of an endpoint device is its composition, which typically includes hardware components, an operating system, and specific applications tailored to fulfill certain functions or requirements.

While hardware itself is not directly involved in cybersecurity, it's the various communication ports and techniques like WiFi and Bluetooth that introduce vulnerabilities.

Ensuring the safety of your endpoint device is crucial, requiring various proactive measures. This thesis aims to recognize the user as a critical asset and explores methods to enhance endpoint security even without direct user involvement. One key aspect is to regularly maintain endpoint updates, a fundamental step in mitigating vulnerabilities and strengthening overall security posture.

Consistently updating your endpoint is among the most effective measures one can take. This extends to one's security software. By ensuring one has the latest OS and software version, one equips her or his device with optimal protection. Endpoint device is not only a computer, there is an OS update in every smart device such as phones, tablets, smart-TV and many IOT-devices.

Software's and Aps updates are as much important, cause often come with enhanced security features and bug fixes. These updates are designed to address not only known

vulnerabilities but also emerging threats. They can include improvements in firewall settings, intrusion detection, and malware scanning, among other security enhancements.

Beyond security benefits, updates can also lead to improved device performance. Updates may optimize resource usage, enhance compatibility with other software and devices, and provide new features that can boost productivity and overall user experience. Running outdated software and operating systems can lead to compatibility issues with newer applications and services. Staying up to date ensures that one's endpoint devices remain compatible with the latest software and online services, reducing disruptions and potential security risks.

Automatic updates ensure that security patches are applied as soon as they are released. Users don't need to manually search for updates and install them, which can be a cumbersome and error-prone process. Often the update process is pending cause the user won't apply the update, for example in a smart phone, or as a "Restart pending" notifications are typically issued by operating systems or software after installing updates that require a system or device restart to take effect fully. Those small actions can be forgotten by users for weeks or more and can be a cause a security break.

It is imperative for software and OS developers to continually improve the update mechanisms, ensuring that updates are seamlessly applied. Users should be encouraged and guided, if necessary, to adhere to update provisions, prioritizing their device's security and performance.

There's a distinct difference between updating apps and operating systems (OS) on one's phone. While apps typically require updating to access their latest features and security enhancements, OS updates often involve more significant changes and may require user approval.

Keeping your mobile apps up to date is essential for enjoying their full functionality and security benefits. Mobile app updates typically include bug fixes, performance improvements, and exciting new features that enhance your overall user experience.

When it comes to your phone's operating system (OS) updates, the process may involve user approval. These OS updates often bring fundamental changes to the core software that powers your device, including system-level improvements, security patches, and

new functionalities. Given the significance of OS updates, users are usually given the option to review and approve them.

The process of asking for user approval before installing an operating system (OS) update is designed to respect the user's autonomy and ensure they have control over their device. Security updates are often handled differently to prioritize device security.

The results of a small-scale survey conducted at work and among friends were surprising: In 100% of mobile devices was selected automatic updates, but only 75% of them was up to date. Same state in apps, several of them still in use with older version.
The primary reason for the lack of updates in mobile devices often stems from technical issues, such as insufficient storage space or incompatibility with certain applications due to the current operating system version. The reasons remain much the same as they were 20 years ago, there's ample opportunity for manufacturers to pioneer better solutions to enhance device and app compatibility.

In laptop and desktop computers, despite the announcement, many updates remain in the queue on the computer. Regardless of automatic updates, many updates were not implemented, cause finishing of updates needed to restart the endpoint device. The update will initiate once you restart your computer, but before, all important security patches, performance improvements, and bug fixes to ensure your system remains secure and efficient, will be unavailable.

Another important cornerstone in the defense against cyber threats, evolving to address a wide spectrum of malicious software (malware) including viruses, worms, trojans, ransomware, and spyware, is antivirus software.

As cyberattacks become more sophisticated and frequent, there is a compelling argument for operating systems (OSs) developers to integrate antivirus software directly into their products. In this way, users will be able to enhance their security posture, simplify their protection mechanisms, and be able to combat a wider variety of cyber threats with a more cohesive defense.

One of the primary reasons OS developers should include antivirus software is to enhance user security. Users often lack the expertise to choose and configure the right antivirus solutions. By integrating antivirus software into the OS, developers ensure that

every device has a baseline level of protection from the moment it is turned on. This built-in security can help detect and neutralize threats such as malware, ransomware, and phishing attacks before they cause significant damage. In addition, integrated antivirus solutions can be optimized so that they work seamlessly with the operating system, thus ensuring better performance and fewer conflicts when compared with third-party solutions.

To enhance cybersecurity for users, it is logical and necessary to integrate antivirus software into operating systems. Providing a baseline level of protection, simplifying user experience, and enabling an integrated and effective security strategy are all advantages of the system. In light of the continuing evolution of cyber threats, OS developers should embed robust antivirus solutions into their products in order to ensure user security. This proactive measure can significantly reduce the risk of cyberattacks, safeguarding both individual users and the broader digital ecosystem.

In conclusion, endpoint security, ensuring that user devices are automatically updated and equipped with essential software and applications is paramount. Automatic updates play a crucial role in maintaining device integrity and security, addressing vulnerabilities as soon as they are discovered. This proactive approach minimizes the risk of exploitation by cyber threats, ensuring that security patches and updates are promptly applied without requiring user intervention.

Incorporating critical security software, such as antivirus programs and firewalls, directly into the operating system further enhances protection. By embedding these tools, OS developers can provide a seamless and robust defence mechanism that works out-of-the-box, eliminating the need for users to manually select, install, and configure their security solutions. This not only simplifies the user experience but also ensures that all devices maintain a consistent level of protection against malware, phishing, and other cyber threats.

The combination of automatic updates and integrated security applications ensures that devices remain protected with the latest defences. This reduces the likelihood of successful cyberattacks and enhancing overall cybersecurity resilience. This strategy is essential for safeguarding individual users and the broader digital ecosystem in an increasingly interconnected world.

4.2 Cyber Security Armadillo: Network Security

As users increasingly rely on home networks and public Wi-Fi for daily activities, including online banking and remote work, understanding and implementing robust network security measures has never been more critical.

Network security is important for several reasons. First and foremost, it protects sensitive information from intercepting or accessing by unauthorized parties. This includes personal data, financial details, and private communications. Additionally, a secure network prevents unauthorized users from exploiting network resources or launching attacks from within the network. This includes malware distribution or denial-of-service attacks (DoS).

Users' networks can be divided into two categories: their own network (at home) and all other networks they use on a daily basis. The main component of a home network is the router or modem. Home router security often goes overlooked despite being a critical component of protecting personal networks from cyber threats. Since routers serve as the link between a home's internal network and the external internet, they are prime targets for cybercriminals. Ensuring robust security measures are in place for home routers is essential for safeguarding sensitive information and maintaining overall network integrity.

One of the most crucial steps in securing a home router is changing the default login credentials. Manufacturers often ship routers with generic usernames and passwords, which are widely known and can be easily exploited by attackers. Users should create strong, unique passwords that combine letters, numbers, and special characters. This simple action can significantly reduce the risk of unauthorized access.

Maintaining router security requires regular firmware updates. Manufacturers release updates to patch vulnerabilities, fix bugs, and enhance functionality. Users should regularly check for and apply firmware updates to ensure their routers are protected against the latest threats. Modern routers offer automatic update features, which simplify this process and ensure timely protection.

A remote management feature allows users to access their routers from an external network. However, this feature can be exploited by attackers if it is not properly protected.

In general, remote management should be disabled unless absolutely necessary and protected by strong authentication methods.

The majority of routers are equipped with wireless network capability. There is no doubt that wireless networks are among the least secure networks at home. One of the most effective ways to enhance Wi-Fi security is by enabling Wi-Fi Protected Access 3 (WPA3). The latest and most advanced security protocol for wireless networks, providing several significant benefits over its predecessors, WPA2 and WPA. It implements stronger encryption algorithms that make it harder for hackers to decrypt data transmitted over the network. In WPA3-Enterprise mode, 192-bit encryption is employed to ensure the security of data transmitted over the network.

WPA3 includes a feature called Simultaneous Authentication of Equals (SAE), which replaces the Pre-Shared Key (PSK) method used in WPA2. SAE provides more robust protection against brute-force attacks by requiring a new key exchange each time a device joins the network, making it harder for attackers to guess the password.

By enabling forward secrecy, WPA3 ensures that if an attacker is able to capture and decrypt current session data, previous sessions remain secure. This feature is especially useful when protecting long-term privacy.

The introduction of Wi-Fi Easy Connect in WPA3, simplifies the process of connecting Internet of Things (IoT) devices to a network. At the same time, it enhances the security of smart home devices, which often lack adequate security measures.

Protecting your home's Wi-Fi network is essential to ensure one’s personal data remains secure and private. While WPA3 provides enhanced security features, even without it, one can significantly improve your network’s security by implementing these best practices. By changing default settings, enabling strong WPA2 encryption, using robust passwords, keeping firmware up-to-date, and segmenting one’s network, one can take effective steps to protect your network.

The other issue is open public networks. The convenience of open networks—public Wi-Fi available in cafes, airports, hotels, and other public spaces—cannot be overstated. These networks offer easy access to the internet on the go, enabling us to stay connected virtually anywhere. However, the convenience of open networks comes with

significant security risks. As a private individual, it is crucial to understand these risks and adopt strategies to use open networks safely.

The nature of open networks makes them incapable of providing robust security controls. As opposed to private networks, which typically require passwords and use encryption to protect data, open networks are often unprotected. Cybercriminals exploit vulnerabilities and intercept data by taking advantage of this lack of security.

One of the primary risks associated with open networks is the potential for data interception. Without encryption, any data transmitted over an open network—such as login credentials, financial information, and personal messages—can be easily intercepted by malicious actors. This can lead to identity theft, financial loss, and unauthorized access to personal accounts.

Another risk is the possibility of connecting to rogue hotspots. Cybercriminals can set up fake Wi-Fi networks with names similar to legitimate ones, tricking users into connecting. Once connected, these rogue hotspots can capture all data transmitted by the user, further compromising their security. And many others such as malware distribution, session hijacking, phishing attacks and Man-in-the-Middle attacks, when cybercriminals can insert themselves between the user and the Wi-Fi connection, intercepting and potentially altering communications and data transfers.

In order to avoid all of this risks, there are a number of security strategies that can be implemented.

Use a Virtual Private Network (VPN), A VPN encrypts your internet connection, making it difficult for cybercriminals to intercept your data. By routing your traffic through a secure server, a VPN provides a layer of privacy and security, even on unsecured networks. Always use a reputable VPN service, and ensure it is activated whenever you connect to an open network.

Ensure that websites you visit use HTTPS, which encrypts data between your browser and the website. Many browsers now flag HTTP sites as insecure, helping users to avoid them. Use browser extensions that force HTTPS connections whenever possible, adding an extra layer of security.

Avoid conducting sensitive transactions, such as online banking or shopping, when connected to an open network. If one must perform these tasks, use a VPN or wait until one is on a secured, private network. Be cautious about entering personal information, such as passwords and credit card details, while connected to public Wi-Fi.

As a conclusion, it is important to remember that any public network poses a potential security risk, even if it is password-protected or requires authentication. Password protection and authentication can offer a false sense of security, as these measures may not be sufficient to deter sophisticated attackers. Therefore, it is imperative to exercise caution and employ additional security practices, such as using a Virtual Private Network (VPN) and avoiding the transmission of sensitive information while connected to public networks.

4.3 Cyber Security Armadillo: Cloud Security and Digital Footprints

Digital footprints are the trails one leaves behind when one uses the Internet. It consists of a wide range of information that can be traced back to the user, both actively and passively collected, reflecting one’s online activities, preferences, and behaviours. Understanding and managing one’s digital footprint is essential for maintaining privacy and security in the digital age.

Digital footprints can be categorized into two types: active and passive. Active Digital Footprints are the data traces that individuals intentionally leave behind. This includes social media posts, online reviews, emails, and any other information willingly shared on the internet. For instance, when one updates his status on Facebook, tweet, or write a blog post, one is actively contributing to his digital footprint. Passive Digital Footprints, on the other hand, are the data collected without the user's explicit consent. This includes browsing history, cookies, and location data. Websites and apps often track user activities to understand behaviour patterns, which can be used for targeted advertising or improving user experience.

One of the most immediate and critical implications of digital footprints is the threat to privacy. The extensive data collected through online interactions can reveal intimate details about an individual's habits, preferences, and daily activities. This data, often aggregated and analyzed by various entities, can lead to a comprehensive profile that exposes sensitive aspects of one’s life. Obtaining unauthorized access to this data by

cybercriminals, corporations, or even government agencies can pose significant risks to the privacy of all individuals. Individuals' personal information may be sold to third parties without their consent, resulting in unwanted solicitations and a general erosion of their privacy. Cybercriminals can exploit detailed digital footprints to orchestrate sophisticated attacks, such as identity theft, phishing scams, and social engineering attacks. By piecing together information from various online sources, attackers can create convincing and personalized schemes to deceive individuals and gain access to sensitive information. Additionally, data such as passwords, financial details, and social security numbers, if intercepted or improperly secured, can lead to significant financial and personal harm.

Digital footprints also have a profound impact on an individual's personal and professional reputation. Information shared online can be permanent and far-reaching. Employers, educational institutions, and other organizations often conduct online searches to learn more about individuals. Inappropriate or controversial content from the past can resurface, affecting job prospects, academic opportunities, and personal relationships. Even seemingly harmless posts can be misconstrued or taken out of context, leading to unintended consequences. Managing one's digital footprint is thus essential to maintaining a positive reputation and avoiding potential fallout from past online activities.

Digital footprints are a goldmine for advertisers and corporations. Companies use the data collected from online activities to build detailed consumer profiles, allowing for highly targeted advertising. While this can enhance the user experience by delivering relevant ads and personalized content, it also raises significant ethical and privacy concerns. The extent of surveillance and data collection practices by corporations can feel intrusive and may lead to a sense of constant monitoring. Moreover, consumer profiling can perpetuate biases and inequalities, as algorithms may reinforce existing prejudices based on the data they analyze.

The most straightforward method of protecting oneself and managing one’s digital footprint is to regularly search one’s name on search engines to see what information is publicly accessible. This can help one to identify and address any unwanted information. Check the privacy settings on social media accounts and limit the amount of personal information visible to the public. Remove any old or unnecessary posts, photos, and comments. Make a list of all online accounts one has created over the years, including old email addresses, social media profiles, and subscriptions. For accounts one no longer uses, go through the process of deactivating or deleting them. This reduces the

number of platforms where one's personal data is stored and minimizes potential vulnerabilities.

In additional to that periodically change passwords and avoid reusing the same password across multiple sites. Ensure that all accounts have strong, unique passwords to reduce the risk of password-related breaches. Add an extra layer of security by enabling 2FA on all accounts, requiring a second form of verification beyond just a password. Prefer authenticator apps over SMS-based 2FA for better security, as SMS can be intercepted.

4.4 Cyber Security Armadillo: Operators and Governments

Individuals must take precautions to protect themselves online, but the responsibility of maintaining a secure digital environment extends far beyond their control. Governments and Internet Service Providers (ISPs) both play an important role in safeguarding the internet by enforcing regulations and implementing protective measures. Governments establish cybersecurity laws, national defence strategies, and public awareness campaigns, while ISPs provide secure network infrastructure, threat detection systems, and user protection services. Together, these entities form the backbone of a safer digital space, ensuring that internet users can navigate the online world with greater confidence and security.

4.4.1 Government's Role in Cybersecurity

Governments worldwide have recognized cybersecurity as a national security concern and have implemented various measures to protect internet users. These efforts encompass regulatory frameworks, awareness campaigns, national cybersecurity strategies, and public-private collaborations. Governments establish cybersecurity laws and regulatory frameworks to ensure a standardized level of security across industries.

The General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, is one of the most comprehensive data protection laws in the world. It was introduced by the European Union (EU) to strengthen individuals' rights regarding their personal data while imposing strict obligations on businesses that handle such information. While the regulation primarily aims to enhance privacy, it has also significantly transformed the way businesses approach cybersecurity. GDPR has forced organizations to

adopt stricter security measures, implement new policies, and change their approach to data processing, ultimately making the digital landscape safer for users.

One of the most profound impacts of GDPR on businesses is the requirement to enhance data security. Organizations are now mandated to implement strong technical and organizational measures to protect personal data from unauthorized access, loss, or breach. This has led to increased investment in cybersecurity infrastructure, including encryption, anonymization, and secure storage solutions. Companies that previously neglected data protection have had to upgrade their systems, hire cybersecurity experts, and adopt best practices to comply with GDPR.

Furthermore, businesses must conduct regular risk assessments to identify vulnerabilities in their data processing activities. This proactive approach ensures that companies remain aware of potential security threats and take preventive measures to mitigate them. As a result, GDPR has not only improved security for personal data but also raised overall cybersecurity standards in businesses across different industries.

Before GDPR, many businesses were not legally required to disclose data breaches, leading to situations where users remained unaware that their personal data had been compromised. GDPR introduced a strict 72-hour data breach notification requirement, compelling organizations to report significant breaches to the relevant Data Protection Authority (DPA) and, in some cases, to affected individuals.

This obligation has encouraged businesses to develop clear incident response plans to handle data breaches swiftly and efficiently. Many companies have invested in real-time threat detection and monitoring systems to identify breaches as soon as they occur, minimizing potential damage. The transparency enforced by GDPR has also improved consumer trust, as individuals are now promptly informed about any security risks related to their data.

GDPR emphasizes the principle of Privacy by Design and Default, meaning that organizations must incorporate privacy considerations into their systems and services from the outset rather than as an afterthought. Businesses must ensure that only necessary data is collected, that it is processed securely, and that default settings prioritize user privacy.

This shift has had a significant impact on how companies develop software, design websites, and handle customer information. Organizations must now conduct Data Protection Impact Assessments (DPIAs) for high-risk data processing activities, ensuring that potential risks to users' privacy are identified and mitigated before new technologies or services are deployed. This approach has made privacy and security an integral part of business operations, rather than optional add-ons.

GDPR has placed a strong emphasis on accountability, requiring organizations to document their data processing activities, demonstrate compliance, and be prepared to justify their decisions regarding data security. Businesses must now keep detailed records of how they collect, store, and process personal data. They must also be transparent about their data practices, providing users with clear information on their rights and how their information is being used.

This focus on accountability has significantly improved consumer trust. Users are now more aware of their data rights and can exercise greater control over their personal information, such as requesting data deletion under the "Right to be Forgotten". Companies that prioritize data protection benefit from enhanced brand reputation and customer loyalty, as consumers are more likely to engage with businesses that respect their privacy.

One of the most impactful aspects of GDPR is its strict enforcement and heavy penalties for non-compliance. Organizations that fail to meet GDPR requirements can face fines of up to €20 million or 4% of their global annual revenue, whichever is higher. Several high-profile companies, including Google and British Airways, have been fined millions of euros for failing to comply with GDPR regulations.

These financial consequences have acted as a strong deterrent, compelling businesses to take cybersecurity and data protection seriously. Companies are now investing in compliance programs, training employees on data security best practices, and continuously improving their security measures to avoid regulatory scrutiny and potential fines.

Although GDPR is an EU regulation, its impact extends far beyond Europe. Any company that handles the personal data of EU citizens, regardless of where it is based, must comply with GDPR. This has led many multinational corporations to adopt GDPR-level

security practices worldwide, rather than implementing different standards for different regions.

Additionally, GDPR has inspired similar privacy regulations in other countries, such as the California Consumer Privacy Act (CCPA) in the United States and Brazil's General Data Protection Law (LGPD). The global adoption of GDPR-like principles has helped create a more consistent approach to data protection, making the internet a safer place for users worldwide.

To combat criminal activities and cyber threats, governments have established specialized law enforcement units and response teams dedicated to investigating cybercrimes, dismantling cybercriminal organizations, and mitigating the impact of cyberattacks. Agencies such as the FBI's Cyber Crime Division, Europol's European Cybercrime Centre (EC3), and Interpol's Cybercrime Unit play a crucial role in international cybercrime enforcement. Additionally, Computer Emergency Response Teams (CERTs) operate at national and regional levels, providing rapid responses to cyber incidents. This essay explores the importance of cybercrime law enforcement, the role of response teams, and the challenges they face in ensuring cybersecurity.

Law enforcement agencies worldwide have established specialized units to tackle the increasing threat of cybercrime. These agencies focus on investigating cyber threats, arresting cybercriminals, preventing cyberattacks, and promoting international cooperation to combat digital crime on a global scale.

Within the European Union (EU), Europol's European Cybercrime Centre (EC3) plays a key role in combating transnational cybercrime. EC3 was established in 2013 to support EU member states in addressing cyber threats, particularly in the areas of online fraud, child exploitation, and critical infrastructure attacks.

EC3 works closely with law enforcement agencies across Europe, providing operational support, intelligence analysis, and cybersecurity training. The center has led high-profile cybercrime operations, such as takedowns of dark web marketplaces where illegal activities like drug trafficking, weapons sales, and financial fraud occur. One such example is the dismantling of AlphaBay and Hansa Market, two of the largest dark web platforms for illicit transactions.

While law enforcement agencies focus on investigating and prosecuting cybercriminals, Computer Emergency Response Teams (CERTs) specialize in incident response and cyber risk mitigation. CERTs operate at national, regional, and organizational levels, helping governments, businesses, and individuals respond to cyber threats effectively. CERTs continuously analyse cyber threats, tracking new attack techniques and vulnerabilities. In the event of a cyberattack, CERTs provide immediate assistance to contain the damage, recover affected systems, and prevent further breaches. As part of their security assessments, CERTs identify vulnerabilities in critical systems and patch them before cybercriminals could exploit them. Individuals and organizations are educated on best practices for cybersecurity through the CERT program, reducing the likelihood of security breaches as a result of human error.

Despite the efforts of law enforcement agencies and CERTs, combating cybercrime presents several challenges. Cybercriminals often operate across international borders, making it difficult for law enforcement agencies to track and prosecute them. Differences in legal frameworks and law enforcement capabilities create obstacles in pursuing cybercriminals worldwide. Cybercriminals continuously develop new attack methods, making it challenging for law enforcement and CERTs to stay ahead. Advanced tactics like ransomware-as-a-service (RaaS), deepfake technology, and artificial intelligence (AI)-driven cyberattacks require constant adaptation. Cybercriminals leverage tools such as VPNs, the dark web, and cryptocurrency to conceal their identities, making it difficult for law enforcement to trace and apprehend them. Many governments, especially in developing countries, lack the resources and expertise needed to effectively combat cyber threats. Cybersecurity funding and training for law enforcement agencies remain a significant challenge. Striking a balance between law enforcement surveillance and individual privacy rights is a major challenge. Overly invasive cybersecurity measures could violate privacy laws, leading to legal and ethical debates.

To strengthen global efforts against cybercrime, law enforcement agencies and CERTs must adapt to new technologies and enhance international cooperation. Future developments in cybercrime enforcement may include Artificial Intelligence and Machine Learning. AI-driven cybersecurity solutions can help detect cyber threats in real time, automate security responses, and identify malicious activities more efficiently. Greater collaboration between governments, private companies, and cybersecurity firms can improve intelligence-sharing and threat mitigation strategies. Governments should invest in training

cybersecurity professionals to strengthen national defences and equip law enforcement agencies with skilled personnel.

4.4.2 Role of Internet Operators in Cybersecurity

Telecommunications companies and internet operators—including Internet Service Providers (ISPs), backbone providers, and network infrastructure companies—hold a particularly critical position, as the primary gateways to the internet. Their role in cybersecurity is preventing, detecting, and mitigating cyber threats that could harm end-users. Internet operators are responsible for maintaining and protecting network infrastructure, which includes routers, switches, data centers, and cables that carry data across the globe. Operators secure network infrastructure by deploying advanced technologies. Firewalls and IDS to monitor and block malicious traffic. DDoS Mitigation Services to prevent large-scale cyberattacks from disrupting services. End-to-End Encryption to safeguard data integrity and confidentiality. Leading ISPs implement Domain Name System (DNS) filtering, which blocks access to known malicious websites, protecting users from phishing scams and malware infections. As the service that translates domain names into IP addresses, DNS is frequently targeted by attackers. ISPs can protect against threats such as DNS hijacking, cache poisoning, or domain-based malware by implementing DNSSEC (Domain Name System Security Extensions) and maintaining secure, redundant DNS servers.

Moreover, operators can offer DNS filtering services to block access to harmful websites. These filters can be updated regularly based on intelligence from cybersecurity organizations, preventing users from visiting phishing sites or downloading malicious software.

ISPs can detect suspicious or malicious traffic passing through their networks. By using technologies such as Deep Packet Inspection (DPI), anomaly detection systems, and firewall rules, they can block harmful data packets, as a Known phishing sites, Malware distribution channels, Botnet command-and-control communications, Spam and scam-related domains.

For example, some ISPs proactively blacklist IP addresses and domains associated with cyberattacks and update these lists continuously using real-time threat intelligence feeds from cybersecurity partners.

Many ISPs have started offering value-added security services to home users, businesses, and organizations, such as Anti-virus and anti-malware suites bundled with internet packages, Parental control tools to protect children online, Secure DNS services that prevent access to harmful websites, Firewall and router configuration support for home networks, IoT device monitoring tools to detect compromised smart devices.
These services help reduce cyber risks for customers who may lack the technical knowledge to secure their own systems.

ISPs often identify infected or compromised user devices through traffic patterns—such as unusual connections to known botnet servers or rapid spam activity from a home connection. When detected, ISPs notify the customer that their device is likely infected, provide tools or guidance to clean the device, throttle or temporarily suspend infected traffic to prevent wider harm. This role in incident response helps limit the spread of cyberattacks and educates users at the same time.

ISPs also play a role in enabling modern secure internet protocols, such as IPv6, which has stronger security features compared to IPv4. HTTPS (SSL/TLS) encryption support and enforcement, DNS over HTTPS (DoH) and DNS over TLS (DoT) for encrypted DNS queries.By adopting and promoting these protocols, ISPs help build a safer internet architecture. To enhance user security, operators provide: Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) mechanisms. Secure Wi-Fi Protocols to prevent unauthorized access to networks. Spam and Phishing Protection through advanced email filtering techniques.

Major ISPs, such as Elisa or AT&T, integrate these security measures into their services to ensure that users have a safer online experience. From a service architecture perspective, ISPs integrate Security as a Service (SECaaS) offerings into consumer and enterprise packages, providing cloud-based antivirus, endpoint detection and response (EDR), and web filtering tools. These services are centrally managed and maintained, reducing the operational security burden on users while increasing overall network hygiene.

Additionally, ISPs maintain close collaboration with national cybersecurity centers, Computer Emergency Response Teams (CERTs), and global threat intelligence networks to dynamically update their security policies and blocklists. This ensures rapid response to emerging threats, such as zero-day vulnerabilities or large-scale phishing campaigns.

By embedding security into the infrastructure, ISPs act as critical control points in the internet supply chain. Their integrated approach not only protects subscribers but also contributes to the systemic resilience of the internet. In doing so, providers like Elisa and AT&T are not merely conduits of connectivity, but active participants in the global cybersecurity ecosystem.

One of the most impactful forms of collaboration is between ISPs and cloud service providers like Google and Microsoft. These tech giants operate some of the most advanced threat intelligence platforms in the world, leveraging machine learning and AI to monitor trillions of signals daily across their ecosystems. Through partnerships, ISPs gain access to curated threat intelligence feeds, indicators of compromise (IOCs), and automated response mechanisms that help identify and neutralize threats before they can propagate through ISP networks.

For instance, collaborations with Microsoft's Defender Threat Intelligence platform allow ISPs to integrate real-time information on phishing domains, malware signatures, and attack infrastructure directly into their DNS and routing layers. Similarly, Google's Safe Browsing API and Chronicle Security Platform provide ISPs with automated threat detection and anomaly reporting mechanisms that can be embedded into customer-facing services such as secure DNS resolvers or edge firewalls.

Beyond large cloud providers, ISPs also partner with dedicated cybersecurity firms—such as Palo Alto Networks, Fortinet, Check Point, and CrowdStrike—to implement scalable security solutions at both the infrastructure and user levels. These partnerships enable ISPs to offer Security-as-a-Service (SECaaS) products to consumers and enterprises, including firewalls, endpoint protection, DDoS mitigation, and behavioral analytics tools. The integration of third-party solutions also enhances ISPs' ability to deploy Zero Trust Network Access (ZTNA) models and Software-Defined Perimeters (SDP), which are essential in today's hybrid and remote-first environments.

ISPs working with global cybersecurity companies can more efficiently isolate compromised nodes, reroute traffic, or issue global blocklists in the event of a cyberattack. These collaborations often extend to cybersecurity R&D, where ISPs contribute anonymized network data to help refine threat detection algorithms, while benefiting from early access to new technologies and threat indicators. In some cases, joint task forces and public-

private partnerships are formed to address large-scale threats, such as ransomware campaigns or state-sponsored cyber operations, enhancing not only the security of ISP networks but the broader internet infrastructure.

Many ISPs provide cybersecurity solutions directly to their customers, with one of the most critical offerings being automated security updates, which are used to patch vulnerabilities in network devices efficiently and proactively. Traditionally, patch management for network infrastructure has been manual, time-consuming, and often inconsistent—particularly in large or distributed environments. Devices in remote locations, user homes, or unmanaged segments of the network may remain unpatched for months or even years, posing significant security risks. Automated update systems address this issue by enabling centralized, policy-driven, and timely deployment of firmware and software updates across the network.

Automated security updates are particularly vital for ISPs and enterprise network operators, who manage thousands or millions of devices. Leveraging technologies such as TR-069 (CWMP) or Zero-Touch Provisioning (ZTP), ISPs can remotely push security patches to customer devices like modems and gateways without requiring user intervention. This not only improves security but also enhances customer experience by reducing downtime and support costs. This service ensure that non-technical users benefit from enhanced cybersecurity without requiring extensive expertise.

Future efforts of ISP should focus on three particularly promising avenues for future advancement include enhancing AI-driven cybersecurity solutions for real-time threat detection, expanding global cybersecurity partnerships to address transnational cybercrime, and improving digital literacy programs to ensure that every internet user is equipped with foundational security knowledge.

Artificial Intelligence (AI) is rapidly becoming a cornerstone of modern cybersecurity systems. With the ability to analyse massive volumes of data at machine speed, AI enables the detection of sophisticated and previously unknown threats in real time. Techniques such as anomaly detection, behavioural analysis, and deep learning allow AI to identify patterns that deviate from normal activity, flagging potential threats with high precision. Improving these solutions requires continued research into explainable AI (XAI), adversarial robustness, and automated response systems. Real-time detection is only effective when it is paired with immediate and intelligent mitigation mechanisms. Security

Information and Event Management (SIEM) platforms and Extended Detection and Response (XDR) tools are evolving to incorporate AI modules that not only detect anomalies but also recommend or implement remediation steps autonomously. Integration of AI with zero-trust architectures and threat intelligence feeds can create a more dynamic and context-aware security posture, enabling proactive defence strategies that evolve alongside attacker tactics.

The future of cybersecurity depends on a holistic and forward-thinking approach. Enhancing AI-driven security solutions will allow us to detect and respond to threats in real time, reducing the window of opportunity for attackers. Expanding global partnerships is crucial for tracking and dismantling transnational cybercrime networks, while improving digital literacy ensures that every internet user becomes a part of the security ecosystem. By investing in these three pillars—technology, collaboration, and education—we can build a safer, more resilient digital world.

As cyber threats become increasingly complex and persistent, it is evident that greater responsibility for cybersecurity must shift from the average user to the infrastructure providers. While end-user education and awareness remain important, expecting all individuals to continuously manage updates, detect threats, and follow best practices is neither realistic nor sustainable in the long term. Instead, ISPs are in a stronger position to provide security at scale, embedding protections directly into the network layer and delivering automated, seamless defence mechanisms to their customers.

Automated solutions can significantly reduce user exposure to risk without requiring manual intervention. By designing cybersecurity systems that operate “behind the scenes,” ISPs can ensure a higher baseline of protection for all users, including those who lack technical knowledge or resources.

Shifting more cybersecurity responsibility to ISPs is both a practical and strategic move. It enables the centralization of threat intelligence, faster patch deployment, and more consistent application of security policies. In doing so, ISPs become not just connectivity providers, but essential defenders in the digital ecosystem. This model promotes a more resilient internet, where users are protected by design, rather than by constant vigilance. The role of operators and governments in cybersecurity is indispensable. Governments provide the legal framework, public awareness, and enforcement mechanisms necessary to establish a secure digital environment. Meanwhile, internet operators implement

technological safeguards, threat intelligence, and consumer protection measures to reduce cyber risks. Strengthening collaboration between these entities and promoting proactive cybersecurity strategies will be essential in ensuring a safer internet for all users.

4.5 Cyber Security Armadillo Model Summary

The Cybersecurity Armadillo Model introduces a multi-layered defense architecture that places the user at the core of a structured and resilient protection system. Inspired by the natural defense mechanism of an armadillo—whose segmented armor provides overlapping protection—this model visualizes cybersecurity as a series of concentric, interdependent layers. Each ring represents a distinct aspect of digital defense, designed to shield the user from an evolving landscape of cyber threats. Rather than relying on a single security point, the model emphasizes defense in depth, where multiple barriers work in harmony to reduce vulnerabilities and enhance overall resilience.

At the heart of the model lies the user and the layer closest to them is Endpoint Security. This ring is responsible for directly protecting the devices individuals interact with—laptops, smartphones, tablets, and IoT devices. Core components of endpoint protection include anti-virus and anti-malware software, local firewalls, multi-factor authentication (MFA), automatic software updates, and disk encryption. These tools aim to prevent unauthorized access, detect malicious software, and secure sensitive information stored on the device.

Given that endpoints are often the first targets of cyberattacks—through phishing emails, compromised downloads, or drive-by malware—it is essential that this layer is robust and user-friendly. Automated update systems and pre-configured security defaults can significantly improve protection without requiring constant user intervention. In many ways, endpoint security forms the personal shield of the digital user.

Surrounding the endpoint layer is Network Security, which focuses on safeguarding data as it moves across local and wide-area networks. This includes both home and corporate networks, where cyber threats can infiltrate through unsecured connections or vulnerable devices. Key technologies in this layer include secure Wi-Fi configurations, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), DNS filtering, and encrypted communication protocols such as HTTPS and TLS.

ISPs also play a pivotal role in network security, offering features like malware blocking, traffic analysis, and mitigation of Distributed Denial of Service (DDoS) attacks. By actively monitoring network traffic for anomalies and enforcing security policies at the infrastructure level, this layer helps intercept malicious activity before it can reach the user's endpoint. This proactive defence greatly reduces the overall attack surface.

The third ring, Cloud Security, addresses the increasing reliance on cloud-based services for storage, computing, communication, and collaboration. As users entrust more of their personal and professional data to platforms like Google Drive, Microsoft 365, and various SaaS applications, it becomes essential to ensure that this data is adequately protected—even when it's no longer stored locally.

Cloud security measures include strong access controls, identity and access management (IAM), data encryption at rest and in transit, secure APIs, and constant monitoring for unauthorized access or misuse. Cloud providers must adhere to rigorous security standards such as ISO/IEC 27001 or SOC 2, and users should be encouraged to enable features like MFA for cloud accounts. While the cloud offers scalability and convenience, it also requires a shared responsibility model—where providers secure the infrastructure, and users secure their access to it.

The outermost layer consists of Operators and Government Entities, who establish the overarching infrastructure and policies required for a secure digital ecosystem. This includes Internet Service Providers (ISPs), telecommunications companies, regulatory agencies, and cybersecurity task forces. Their responsibilities span from implementing automatic firmware updates on routers and public infrastructure, to monitoring large-scale threats, coordinating responses to cyber incidents, and enforcing legal frameworks for data protection and cybercrime.

National Computer Emergency Response Teams (CERTs), government cybersecurity centers, and international organizations (such as ENISA or NATO CCDCOE) play a crucial role in coordinating cross-border efforts, issuing threat advisories, and responding to major attacks. Their presence reinforces the model’s principle of collective defense, where large institutions bear a significant portion of the security burden—reducing the need for individual users to be constantly vigilant.

The Armadillo Model champions a shared responsibility framework, where each ring supports the next, and no single layer is expected to stand alone. It recognizes that users cannot and should not be the sole defenders of their digital lives. Instead, a resilient cybersecurity model must include intelligent automation, institutional support, and layered safeguards that operate seamlessly and transparently.

By placing the user at the center but surrounding them with increasingly robust and scalable protections, the Cybersecurity Armadillo Model offers a vision of a safer digital environment—one in which people can interact with technology confidently and securely, without being overwhelmed by its complexity.

5 Conclusions / Summary

Even the most advanced cybersecurity systems can be compromised by human behavior. Users are not perfect—many struggles with weak passwords, ignore software updates, or fall victim to social engineering tactics. These are not necessarily signs of negligence, but rather reflections of the complexity and demands of modern digital life. Despite growing awareness and the availability of security tools, expecting every individual to consistently follow best practices is unrealistic.

This reality underscores the need for a cybersecurity system that does not rely solely on perfect user behavior. Instead, we must design smarter, more automated protections that work in the background—allowing users to remain safe without needing to be constantly alert or technically skilled. While user education and awareness remain important, the ultimate goal should be to build systems that reduce the burden on the individual and provide strong, seamless security by default. Creating an internet where users can engage without constant worry is key to a safer and more inclusive digital future. To achieve this vision, major players such as ISPs, device manufacturers, and OS- developers must take greater responsibility in building a secure digital environment by design.

ISPs are in a unique position to provide security at scale. As the gateway between users and the broader internet, they have the power to implement protective measures that reduce the risk of threats before they ever reach a user's device. This includes features such as automatic firmware updates on routers, DNS-based filtering to block malicious websites, DDoS protection, and intrusion detection systems. By embedding these services directly into the network infrastructure, ISPs can deliver "invisible" security—protection that does not require user action or understanding. Additionally, ISPs can contribute to cybersecurity by participating in threat intelligence sharing and collaborating with national security organizations. They can also support users through clear communication, customer education, and easy-to-use security tools. Ultimately, shifting more cybersecurity responsibilities to ISPs reduces the pressure on individuals, making the online experience safer for all.

Device manufacturers also play a critical role in building a safer internet. Many cyberattacks exploit vulnerabilities in hardware or default configurations that leave devices exposed. To minimize these risks, manufacturers must prioritize security from the earliest stages of product development. This includes secure boot mechanisms, strong

encryption of user data, secure element chips, and hardware-level protection against tampering and exploitation. Companies should ship devices with secure default settings, enable automatic updates by default, and minimize unnecessary permissions or pre-installed software that could be exploited. Transparency around security practices and providing long-term support for updates are essential, especially in the case of Internet of Things (IoT) devices, which often remain in use for many years. When devices are built with security in mind, users can benefit from robust protection without needing deep technical knowledge.

Operating system developers—such as Microsoft, Apple, and Google—have already made major strides in improving cybersecurity over the last decade. Modern OS platforms now include built-in firewalls, sandboxing of apps, biometric authentication, and regular security patching. As cyber threats evolve, OS developers must continue advancing toward systems that anticipate risk and reduce human error. Key improvements include smarter security defaults, machine learning-based threat detection, and tighter integration between hardware and software security layers. For example, features like Windows Defender, Apple's Gatekeeper and Lockdown Mode, and Google Play Protect provide real-time protection and automated threat response. In addition, OS developers should continue to prioritize user privacy and security in the design of their permission systems and app store policies, ensuring that only trusted software can access sensitive data or critical system functions. By creating intuitive, well-guarded digital environments, OS developers help protect users who may not even be aware of the risks they face—further supporting the goal of a worry-free internet experience.

Through stronger ISP-level protections, safer devices, and smarter operating systems, we can move toward a digital future that is not only more secure, but also more inclusive—where everyone, regardless of age, ability, or technical skill, can benefit from the internet without fear. This future is both possible and necessary, and it begins with a commitment to security by design at every level of the digital ecosystem.

Another critical consideration in the cybersecurity domain is the delicate balance between protecting security and preserving user privacy. Governments and organizations often deploy surveillance tools and data monitoring systems to identify and prevent cyber threats. While these measures can be effective in early detection and response, they also raise ethical and legal concerns regarding individual privacy and data protection. The debate intensifies in contexts such as national security, law enforcement, and

pandemic-related contact tracing, where the trade-offs between privacy and public safety are contentious. Building trust with users requires transparency, clear regulations, and the implementation of privacy-preserving technologies such as differential privacy, zero-knowledge proofs, and end-to-end encryption.

Creating an internet where users can engage without constant worry is not only a technical challenge, but a societal one. It requires a shift in perspective—from blaming users for security lapses to building systems that protect users by default. While cybersecurity awareness and digital literacy remain important, the ultimate responsibility must lie with the institutions that control the infrastructure, hardware, and platforms we rely on daily.

References

1 Coole M, Woodward A, Lane A. Defence in depth, protection in depth and security in depth: a comparative analysis towards a common usage language. In: Proceedings of the 11th Australian Information Warfare and Security Conference; 2012 Nov 30; Perth, Australia. Perth: Edith Cowan University; 2012.

2 CISA. Recommended Practice: Defense in Depth [Internet]. Cybersecurity and Infra-structure Security Agency; 2016. Available from: https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

3 Scheibner J, Raisaro JL, Troncoso-Pastoriza JR, Ienca M, Fellay J, Vayena E, Hubaux JP. Revolutionizing medical data sharing using advanced privacy enhancing technologies: Technical, legal and ethical synthesis. arXiv preprint arXiv:2010.14445. 2020 Oct 27. Available from: https://arxiv.org/abs/2010.14445

4 Climer S, Khan M. What Are The 7 Layers Of Security? A Cybersecurity Report [Internet]. Chicago (IL): Mindsight; 2020 Jul 14. Available from: https://gomindsight.com/insights/blog/how-to-prevent-a-data-breach/

5 Garbis J, Chapman JW. Zero Trust Security: An Enterprise Guide [Internet]. Berkeley (CA): Apress; 2021. Available from: https://doi.org/10.1007/978-1-4842-6702-8

6 Unknown author. Defense in Depth Layer 7: Data Security [Internet]. Topics on Information Security; 2013 Jan 26. Available from: https://infosectopicsbyjen.blogspot.com/2013/02/

7 Tal L. Secure Software Development Lifecycle (SSDLC) [Internet]. Snyk. Available from: https://snyk.io/articles/secure-sdlc

8 Microsoft. What Is SIEM? [Internet]. Microsoft Security. Available from: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

9 Jit.io. Top 10 Code Security Tools [Internet]. Jit.io. Available from: https://www.jit.io/resources/appsec-tools/top-10-code-security-tools

10 SentinelOne. What is Network Endpoint Security? Benefits & Challenges [Internet]. SentinelOne; 2024 Oct 10. Available from: https://www.sentinelone.com/cybersecurity-101/endpoint-security/network-endpoint-security

11 CrowdStrike. What is an Endpoint Protection Platform (EPP)? [Internet]. CrowdStrike. Available from: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-protection-platform-epp

12 CrowdStrike. What is Mobile Threat Defense (MTD)? [Internet]. CrowdStrike. Available from: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/mobile-threat-defense-mtd/

13 CrowdStrike. What Is Data Loss Prevention (DLP)? [Internet]. CrowdStrike. Available from: https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-loss-prevention-dlp/

14 Trout Software. Network security [Internet]. Trout. Available from: https://www.trout.software/resources/glossary/network-security

15 Cisco. What is network segmentation? [Internet]. Cisco. Available from: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

16 Fortinet. What is network segmentation? [Internet]. Fortinet. Available from: https://www.fortinet.com/resources/cyberglossary/network-segmentation

17 CrowdStrike. Principle of least privilege (PoLP): what it is & why it matters [Internet]. Austin (TX): CrowdStrike. Available from: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/principle-of-least-privilege-polp/

18 BitLyft Cybersecurity. IDS vs IPS vs SIEM: What you should know [Internet]. BitLyft Cybersecurity. Available from: https://www.bitlyft.com/resources/ids-vs-ips-vs-siem

19 Oracle. What is Zero Trust Security? [Internet]. Oracle. Available from: https://www.oracle.com/security/what-is-zero-trust

20 Cisco. What is social engineering in cyber security? [Internet]. Cisco Systems, Inc. Available from: https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

21 Fidelis Security. Decoding reasons for data loss: social engineering and insider threats [Internet]. Fidelis Security. Available from: https://fidelissecurity.com/threatgeek/data-protection/leading-reason-for-data-loss-social-engineering-insider-threats/

22 SentinelOne. 15 Types of Social Engineering Attacks [Internet]. SentinelOne. Available from: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/types-of-social-engineering-attacks