

Data Security and Compliance

ABSTRACT

One of the most valuable resources of a corporation is its data. Organisations tend to prioritise the collection, distribution, and use of data as the data ecosystem grows. Clarity of how companies obtain permission, adhere to privacy policy, and handle the information they gather is crucial in maintaining accountability and confidence for consumers and stakeholders who demand privacy. Numerous businesses have discovered the value of privacy the painful way, through high-profile privacy breaches. Furthermore, privacy refers to a person's freedom to be protected from intrusive monitoring. To live in a democratic society, one must be able to peacefully reside in one's environment and openly share one's thoughts behind locked doors. Most companies assume that holding personal data protected from criminals entitles them to be fully compliant with data protection laws. This is not the truth at all. While the terms "data security" and "data privacy" are frequently used synonymously, there are many important distinctions to be made. Although data security can exist without data privacy, data privacy cannot exist without data security.

Keywords – Information Security, Risk Management, Regulatory Compliance, IDS, IPS

I. INTRODUCTION

New risks and criminal activities are taking place every day as information technology develops. The need to secure information resources from these risks and activities is one of the most urgent challenges currently facing society. However, technological, and organisational safeguards are often insufficient to preserve the information of the organisation. Since there are so many factors to consider when it comes to data management, further steps must be taken. People are just one of these considerations. Network administrators, technology analysts, staff and customers are all examples of these people who manage confidential data. They are in charge of regular operations and, as a result, the whole information infrastructure. They must behave in an ethical and moral manner, or the information infrastructure will be vulnerable to attack. The importance of legal, ethical, and professional issues in information security is explored in this article. Following that, the principles of legislation, morality, and data processing are briefly discussed. Numerous legal issues and insights from information security studies are discussed, and several articles are analysed to highlight the importance of ethics in information security. Ethical guidance processes, policymaking, and identification of important people within an organisation are also effectively tackled. However, the most important aspect of this paper is a review of the studies on legal, ethical, and professional issues in the field of information security and the processing of confidential data in the industry.

II. LEGAL, ETHICAL, AND PROFESSIONAL ISSUES IN INFORMATION SECURITY

It is possible to be held liable even though no criminal law has been broken. Liability is the legal obligation of an

organization to offer compensation or pay for injustices committed that goes beyond criminal and contract law. The truth of the matter is that if an individual, with or without the consent of the corporation, conducts an unlawful or immoral act that causes damages, the company can be held legally responsible for that behaviour. If a company refuses to take precautions identified as due care, it raises its responsibility. When a company ensures that each and every person understands what appropriate and inappropriate behaviour is, as well as the implications of unlawful or immoral acts, due care requirements are fulfilled. Due diligence allows an entity to make a legitimate attempt to safeguard others and to uphold that commitment over time. Due to the worldwide scope of the Internet, anyone who may be harmed or treated unfairly by the workforce of an organisation may be located anywhere in the world [1]. If the organisation is to be legally consistent with the use, storage, and processing of data, it must comply with a variety of information security laws [1]. Appendix A contains a list of the most relevant items of legislation in the United Kingdom.

Laws are rules that enforce or forbid specific behaviours, and they are derived from ethical principles that describe morally appropriate behaviour. The primary distinction between laws and ethics is that laws are backed by the jurisdiction of a legislative body, whereas ethics are not. Ethics, on the other hand, are focused on cultural traditions, such as the defined moral beliefs or norms of a social society. Most moral principles are common. Murder, burglary, robbery, and vandalism, for example, are acts that violate ethical and legal standards all over the world [1].

Information security experts help manage security within an enterprise by establishing and enforcing policies. These regulations that define what is and is not permissible in the work environment, function as corporate rules, along with fines, judicial practises, and penalties to ensure enforcement. Since these rules serve as regulations, they must be carefully formulated and enforced to guarantee that they are comprehensive, relevant, and equally applicable to all employees. However, there is a distinction between a policy and a law in such a way that negligence of a policy is an appropriate defence. As a consequence, in order for the policy to be binding, it must satisfy the five conditions mentioned below [1]:

- Dissemination: The company must be prepared to show that the applicable policy was made easily accessible to the individual for analysis. Hard copy and electronic delivery are both popular methods of dissemination.
- Review: The company is required to show that the content was distributed in an appropriate way, such as copies for illiterate, foreign and read-impaired personnel. Transcripts of the policy in English and other languages are popular methods of review.

- **Comprehension:** The company must be able to prove that the individual was aware of the current policy criteria and contents. Questionnaires and other tests are effective approaches of comprehension.
- **Compliance:** The company is required to prove that the individual committed to follow the policy by adopting or affirming it. Notification signs, which involve a simple activity to accept an agreement, or a signed contract simply stating the individual has read, acknowledged, and committed to abide by the policy, are two common strategies of compliance.
- **Uniform compliance:** Irrespective of individual status or assignment, the entity must be prepared to show that the policy has been applied consistently.

An entity can only prosecute personnel who breach the policy without risk of civil retaliation if all of the provisions set out above are complied with [1].

III. STRUCTURE OF THE INFORMATION SECURITY DIVISION

From CEOs to technicians, technological automation, cloud computing, and a complex threat environment are pushing organisations to reconsider the responsibilities of each individual on their security departments. With millions of remote employees around the world, the pace of innovation in data security is growing. Organizations are moving away from conventional security strategies to keep company properties secure, towards more efficient zero trust policies to protect customers, records, and financial assets where they reside. This revolution ushers in technological advancements while simultaneously raising concerns about people's jobs and obligations in this modern environment. Simultaneously, in contrast to conventional defence methods, secure development frameworks require security professionals to collaborate more closely during product development and strategic planning in order to successfully handle cyber threats. This necessitates a deeper understanding of the market environment and closer partnership collaboration [2].

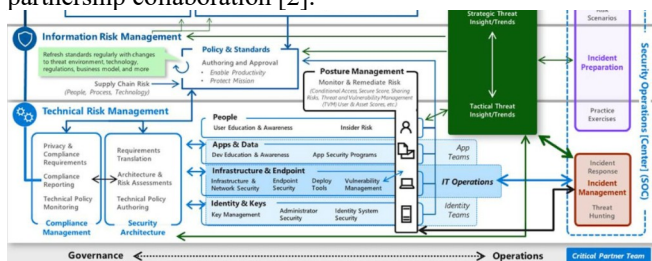


Fig. 1. Managing cyber risk. Adapted from [3].

The human aspect of a security scheme is defined by security protocols. They are the roles and responsibilities that employees of the organization conduct to assist in the security of the company. Employees may be assigned to one or more roles, based on the scale and nature of the business; in certain situations, numerous individuals may be delegated to a single role as a group as seen in Figure 1. Highly trained security teams are mindful of their respective duties, but often consider themselves as members of a broader team fighting against threats. The security measures seen in Figure 1 reflect a fully staffed corporate security department, which Byron Bros can aspire to. Based on the degree of risk, available funds, and expectations, the above company must prioritise where to spend first on a daily basis [3].

A hierarchical diagram must specifically describe the hierarchy of a company's employees usually beginning with the C-level personnel and progressing to people that answer to certain C-level positions. The aim of this document is to establish a consistent representation of an organisational hierarchy that helps workers to recognize hierarchy of the organization, inter-organizational relationships, and who they can respond to as concerns occur. Organizational diagrams can be created to illustrate an entire corporation's management approach and structure, or they can be created for specific management levels, which is most common in medium or large enterprises. An example of a cohesive team organisational diagram is one created primarily to demonstrate the layout of an Information Security division. Finally, in addition to be a trustworthy source of information, a corporate chart should be an active file, which guarantees that it will be revised as staff numbers change or positions are transferred [4].

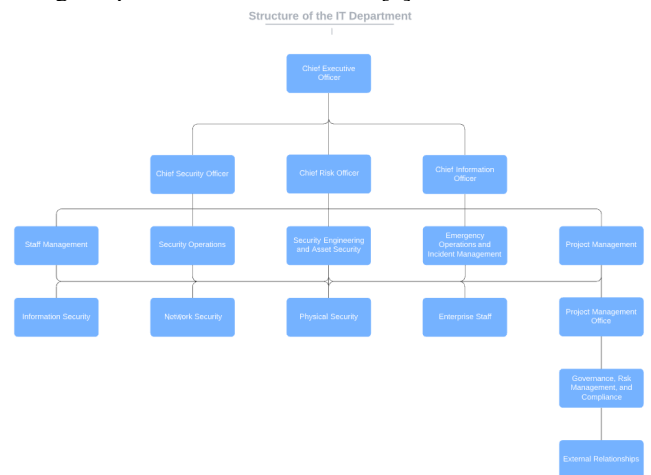


Fig. 2. Structure of the IT department.

Figure 2 demonstrates the proposed architecture for the new department, which classifies key personnel and responsibilities to ensure that adequate assurance and governance can be provided on behalf of the company with respect to the documents and information stored. Appendix B contains more detailed information on each position.

IV. REGULATORY COMPLIANCE WITH THE CURRENT REGULATIONS

The policies of a company are at the core of its activities. They specify how people can react to specific situations, guaranteeing that everyone is on the same board and implementing agreed-upon best practises. The European General Data Protection Regulation (GDPR), which regulates the handling of personal information from individuals within the EU, no longer extends to the United Kingdom following Brexit. Instead, the United Kingdom has enacted its own variant, named United Kingdom General Data Protection Regulation (UK-GDPR). Furthermore, since the Data Protection Act 2018 extends to all companies that process personal data, proactive policies are even more essential [5] [6].

People in the United Kingdom now have more transparency over their confidential records as well as confidence that their data is adequately protected across the country, due to the UK-GDPR. Private information is characterized as any information about an individual, such as a name, surname, physical address, email address, credit card

details, location information, health records, or phone number, as set out in the UK-GDPR Regulation. There is no difference between confidential information about people in their personal, social, or professional lives. Anything in a business-to-business environment is about people communicating and exchanging data with and about one another. Customers in the business-to-business industry are clearly enterprises, but the partnerships that deal with company issues are individuals. The UK-GDPR is an initiative by the United Kingdom to allow people, consumers, vendors, suppliers, and staff to have more authority over their data while at the same time providing less control to organisations that gather and share information for commercial gain [5] [7] [6]. Individuals have eight fundamental rights under UK-GDPR, as shown in the Appendix C.

This latest data privacy policy places the customer in charge, and companies and organisations are responsible for terms of this legislation. Otherwise, they are not upholding the rules. With certain variations, the UK-GDPR mainly refers to customers and providers based in the United Kingdom. If private information is exported outside the United Kingdom, people run the risk of losing security under the UK-GDPR. On this principle, the UK-GDPR prohibits exchanges of private information outside the United Kingdom, or the enforcement of the UK-GDPR, unless interests of people in relation to their sensitive records are covered in some manner, or one of a small range of exclusions occur. Both organisations and businesses who handle sensitive information may assign a data protection officer or data controller to oversee the UK-GDPR enforcement [7] [8] [6].

Privacy by design is a central feature of the UK-GDPR law. Privacy by design necessitates a thorough examination of the data of a company and how it is handled by all divisions. In order to comply with UK-GDPR, a business must take a range of measures to safeguard confidential data. If the organisation has not taken the next step in the enforcement process, now is the time to avoid tough sanctions. Fines of up to 4% of annual worldwide sales or 17.5 million Pounds, whichever is higher, can be imposed on businesses and corporations that do not comply with the UK-GDPR [9] [6]. Appendix D includes proposed policies that will allow the organisation to comply with these regulations and bring the organisation into regulatory compliance with the mentioned current regulations.

V. FRAMEWORK FOR THE RISK MANAGEMENT

In an enterprise setting, an information security framework is a compilation of recorded mechanisms for establishing guidelines and rules for enforcing and retaining management, operational, and physical security controls. These concepts should be used to create an information management policy that handles risk and eliminates vulnerabilities. These structures may be utilised by information management experts to identify and prioritise the activities needed to incorporate security into an enterprise. Frameworks are often designed to address complex issues related to data security. Certain frameworks have been established for particular markets and regulatory compliance objectives. They also come with all types of scales and levels of sophistication. As these systems grow, there is a significant amount of convergence in terms of basic security principles [10].

ISO is an independent, non-governmental international organisation founded in 1946 by a group of trained professionals from a number of fields. This organisation has helped a vast group of companies across the globe. Its goal was to create a common standard that could be used to improve and standardise organisational capacities, with an emphasis on a fair commitment to implementing the standard protocols for adopting, sustaining, and developing those organisations. The ISO 27000 standard was developed in 2009 to clarify the meanings of description, language, and terminology in the Information Security Management System (ISMS). It offers a highly reliable information management architecture that can be used by both big and small businesses. Despite the fact that the ISO/IEC 27000 group encompasses a wide range of standards, ISO 27000 is well established. It helps every company to maintain the protection of data such as user records, intellectual property, financial documents, and secure communication by third parties [11].

A broad database of information security principles and practises has been collected by the National Institute of Standards and Technology (NIST) in the United States. Since its inception in 1990, the NIST Special Publication 800 range has been expanded to offer guidance on nearly every field of information technology. Other models have originated from the NIST SP 800-53 framework; however, they are not purely data security models. NIST SP 800-53 is used by state and federal agencies to meet the Federal Information Processing Standards (FIPS) 200 specifications. Despite the fact that it is tailored to government departments, the NIST model may be used in any sector and therefore should not be ignored by businesses seeking to develop an information management policy [12].

The CIS Controls are diametrically opposed to the NIST security model. This system is a comprehensive compilation of technological controls and the most feasible and most efficient settings that can be used in any situation. It is primarily based on strengthening technical systems to minimise vulnerability and improve robustness, unlike the NIST security model, which addresses risk identification and risk mitigation. Since they offer specific administrative recommendations, the CIS Controls are a great extension to the wide selection of security mechanisms. To better mitigate potential threats, the CIS Controls work effectively with other external risk management systems. They are also an outstanding platform for IT divisions with little to no specialised computer security knowledge [13].

A constructive understanding of risk is required in every corporation's search for financial security and high reliability. The implementation of a risk management system that integrates best practises into the operational risk of a business is the foundation of its economic future. The objective of a successful risk management approach is to conserve the wealth and profits of the company while allowing it to flourish. In addition, clients choose to invest in companies that implement successful risk management policies. This usually leads to lower funding rates, quicker access to money, and improved long-term market outcomes [14]. The appropriate framework for the Byron Bros company is included in the Appendix E.

VI. SOFTWARE MEASURES IN THE INFORMATION SECURITY FRAMEWORK

Security controls are mechanisms used by enterprises to secure different types of information and systems. Any

precaution or preventive measure used to deter, identify, mitigate, or eliminate security threats to physical objects, data, computer networks, or other assets is referred to as a security control. Given the rising incidence of cybercrime, data security safeguards are more relevant than ever. Simultaneously, data privacy laws are becoming more stringent, making it necessary for companies to improve their data security practises or face penalties [15]. This paper is intended to support Byron Bros company in establishing a robust collection of security measures that will aid in the implementation of a threat-based, cost-effective information security policy. Security measures include administrative, organisational, and technical activities aimed at preventing, delaying, identifying, and minimising cyberattacks and other risks to information technology [16].

Data security includes a robust collection of security measures that address electronic security (i.e., network infrastructure), physical security, and personnel security. It frequently entails safeguarding infrastructure services (such as electricity supply, communications, and environmental regulations) that are used by information management networks. The implementation of security controls is essential to an Information Security Management System.

The collection and development of adaptable security measures is driven by an organizational security programs and strategies [16]. Since not all organizations can afford to buy, implement, manage, and operate costly security controls and associated systems, security management implementation choices must address potential threats as well as financial considerations. When budgets are restricted, security controls expenditures must be geared toward enforcing a series of measures that minimise overall risk the most, provided the available funds. This paper proposes security controls for the following data protection strategy topic areas [15]:

- Access Controls.
- Firewalls.
- VPNs.
- Cryptography.
- Physical Security.
- Other Security Tools.

Upon identifying the potential security management options, an organization should choose and enforce an acceptable range of security controls focused on risk factors and funding issues. The correct implementation and upkeep of these protection procedures, as well as the corresponding commitments, tasks, milestones, and timelines, should all be controlled [17].

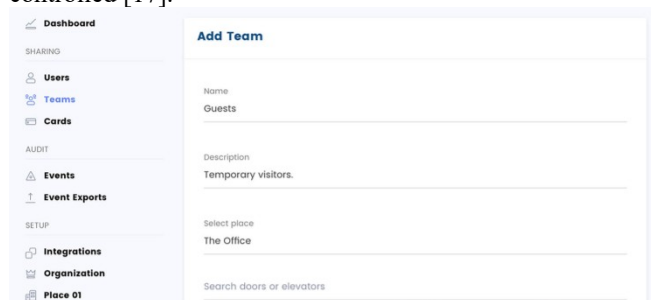


Fig. 3. Kisi access control software.

Preparation, monitoring, arranging, and organising information security is what access control management is all about. It is a field that is still evolving as new challenges, norms, and technology emerge. Significant advances in technologies and platforms, such as cloud computing, Bring-Your-Own-Device (BYOD), and the Internet of Things (IoT), have made access security procedures, deployment, network traffic monitoring, password management, and administration more difficult for companies. To address these implementation and maintenance issues, businesses have incorporated common access management procedures, strategies, templates, and innovations, as well as best practises. ISO/IEC27002:2013, an information security management system, outlines the procedures and practises needed to successfully enforce and maintain access control steps. The systems that govern how individuals obtain data resources are known as access control models [15]. The three categories of access control models are mandatory access control, discretionary access control, and role-based access control. Despite the increasing adoption of discretionary and role-based access control models, most organisations grant privileges to users for a special and immediate purpose, and the privileges granted to individuals are often improperly recorded [18]. As a result, authentication flaws such as under-privileges, least privilege violation, and expensive access control protection administration may occur. Furthermore, access control mechanisms such as Kisi, must be correctly enforced and controlled as seen in Figure 3; otherwise, they can have a substantial organisational impact on both human performance and the ability of the organization to achieve its goals [17].

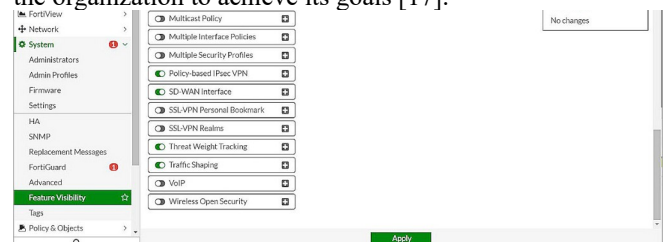


Fig. 4. FortiGate firewall settings.

The area of computer and network security develops solutions that deter unauthorised users from causing serious damage. The expression "damage" is used widely to relate to anything from unauthorised data access to unapproved computer network access, as well as direct physical damage to the network infrastructure. Firewalls have always been a popular method of safeguarding systems and applications. A firewall is any machine that restricts network access. It is a set of elements that reside between two or more networks and monitor network traffic in compliance with a particular security policy. Firewall could be a software installed on a device or a server. It could also be a specialised hardware unit connected to a network. Firewalls are highly powerful authentication measures and should be used in every security framework [19]. A firewall, such as FortiGate can be used in a variety of scenarios as seen in Figure 4, varying from a straightforward packet filtering to a mixture of numerous firewalls. The selection of firewalls is rather appealing. They are available in a variety of sizes, shapes, and capabilities, all of which are tailored to meet the needs of the client. Changes to the firewall policies need not be feared. It is a normal and essential part of expanding an organization, and it can represent changes in the security landscape or rising customer expectations. However, without a well-defined

implementation strategy, even a relatively trivial firewall policy change may have catastrophic consequences for an organization's network. Changing the configuration of a firewall presents a business implementation and maintenance challenge. The higher the possibility of significant damage, the more important it is to test a setup before moving to the next phase. It is best not to change firewall rules on the development unit that protects the network. Testing adjustments in a virtual machine that mimics organisational structures and serves as a testing platform is an excellent approach. These machines should be entirely disconnected from the operating equipment, or they should be equipped with an unavailable network interface. Furthermore, the existence of a firewall on the local computer or network could have an effect on outgoing connections, which should be addressed before beginning the deployment process [20].

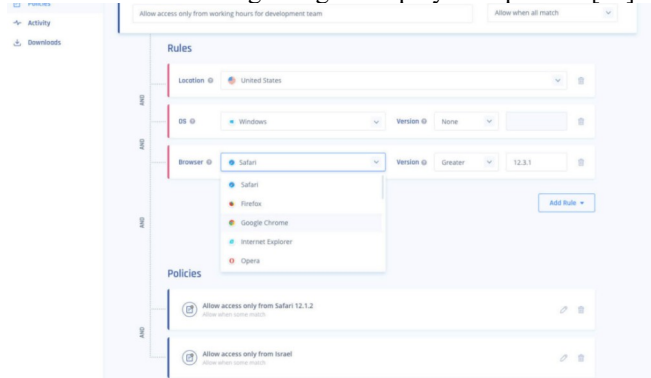


Fig. 5. Perimeter 81 settings.

Virtual Private Network (VPN) is a network architecture that is used to preserve secrecy in a distributed public network. In networking and communications firms, it has proved to be a cost-effective and dependable solution. VPNs are the most advantageous aspect of any IT sector, as they save a large amount of money on connectivity by using the public Internet and provide a highly secure communication platform between the company headquarters and distant areas and clients. The tunnelling protocol is used to enhance the features of a VPN. It also creates a safe form of transport for network services that are not explicitly supported by the traditional network infrastructure. Perimeter 81 enterprise VPN as seen in Figure 5, enables a software or hardware device to safely transmit and capture data through many networks as if it is exclusively linked to the private network, while simultaneously using the public network's compatibility, accessibility, and control measures. There are an endless number of ways to develop a technology, and no innovation is without shortcomings. One of the key reasons for VPN withdrawals is the lack of a widely recognised VPN standard that might be established in the future. Individuals can be prevented from using VPN if it is incompatible with a wide variety of devices, such as a VPN-enabled router that the enterprise can use. As a consequence, not everyone will be able to make use of it. The primary benefit of VPN, on the other hand, is cost savings since the internet is a comparatively inexpensive medium; however, VPN implementation is based on the reliability of the internet, which cannot be controlled [21].

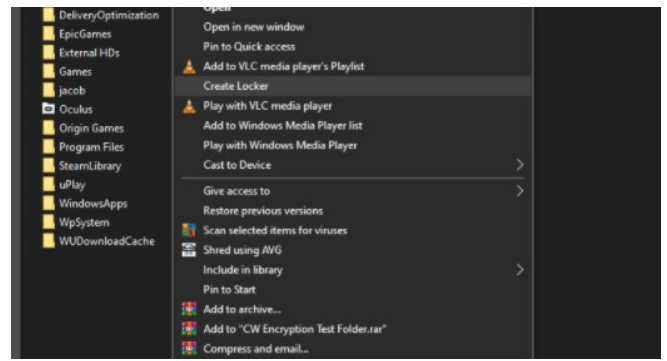


Fig. 6. NordLocker encryption software.

Cryptography is a data transformation method that can be used to incorporate a range of security features such as anonymity, maintainability, verification, and authorization. It is constructed around two fundamental components: an algorithm (a method of encrypting data) and a key. The key is a part of data transformation, and the algorithm is a method of computation. Since exploits can be found over time, or improvements in computing processing power can indicate that even a trial-and-error method are no longer a time-consuming operation, selecting the correct algorithm is crucial. As a result, companies should decide whether their encryption system is still sufficient on a continuous basis. A data protection officer should use a reliable and tested algorithm, such as NordLocker encryption software seen in Figure 6, instead of developing a personalized algorithm. Moreover, certified solutions will guarantee appropriateness while still encouraging data protection officers to show compliance with applicable legal requirements. Although the implementation and realistic use of cryptography technology is becoming extremely accessible, there is a scarcity of expertise and eagerness in this area, limiting its size and propagation. Companies must implement an approach that incorporates the best capabilities, policy, and a robust business model, all of which must be supported by certified technical solutions, in order to address these implementation and maintenance issues [22].

Physical security is extremely important, although some businesses do not provide it. It is needed if corporations do not want their details to be stolen or damaged in the event of a natural disaster. The perpetrator could attempt to steal data for a number of reasons, including personal benefit, monetary reward, vengeance, or that company was the most insecure victim accessible. If this protection is not adequately preserved, every one of the safety mechanisms will be made worthless once the intruder has physical entry. Physical security is becoming to be much more difficult than in earlier centuries, as more smart gadgets are available, making data theft simple and painless. That being said, there are a number of physical security services available, each with its own set of benefits. The first layer of security is boundary protection, which includes mantraps, walls, guard towers, electric fences, and turnstiles. Among other things, secure locks with keys that are difficult to replicate and surveillance in areas where it will not be exposed or where the perpetrator will not be able to interfere with it. Furthermore, each individual employee identification must be checked, thus badges are required [23].

In order to operate a profitable enterprise, companies must have administrative, technical, and physical controls in

their overall information security framework. Other protection tools, such as those seen in Appendix F, can also be included.

VII. RECOMMENDED INTRUSION DETECTION AND PREVENTION SYSTEM

Theoretically, security mechanisms are aimed to determine, recognise, and react to security threats on a computing device, database, or software system in general. These threat actors seek to compromise the security of such systems, to extract passwords and, in certain instances, to harm infrastructures, leaving them inaccessible. Intrusion Detection System (IDS) is a software or hardware that streamlines network security, controls internet traffic for malicious behaviour, and alerts the user. The Intrusion Prevention System (IPS) is a programme or device that prohibits hackers from implementing changes to a system, and even from targeting a network. Security researchers are now recommending technology solutions that incorporate intrusion detection and prevention features, allowing them to recognise, report potential breaches, deter attacks, and communicate decisions to the network administrator. Intrusion Detection and Prevention System (IDPS) guarantees the security accessibility, reliability, and transparency of information systems. IDPS has become crucial when it comes to bringing regulatory compliance into perspective, storing information, securing data against unapproved access or misuse, and maintaining the consistent availability of resources offered by information systems [24].

The significance of security of information has never been greater. Modern networks are starting to gather traction. They transcend even more physical borders to expand hybrid and cloud environments. In addition, most of them are affected by the integration of various cloud services and physical networks. An intrusion detection and prevention system (IDPS) capable of processing and inspecting incredibly high volumes of data streaming through the network is required to protect and control rapidly increasing, complex and crucial networks. At the same time, network protection strategy must be adaptable and expandable in order to meet future specifications. A well-configured and appropriately positioned IDPS helps build a robust multi-layered security framework in hybrid environments [25].

McAfee Network Security Platform is recommended IDPS that can identify infrastructure threats that exploit unpatched security flaws, and it can also eliminate potentially unwanted data packets. All of this aims to prevent different cyber threats, deter a stealth attack that spreads laterally across the system to maximize an attacker's impact, and counteract specialized external attacks such as Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS), thus closing all system vulnerabilities and delivering extensive security measures without sacrificing stability or usability. The McAfee IDPS structure integrates Network Security Manager, a centralised control platform for controlling, customising, and managing IDPS deployments in all environments, which helps to create a robust, multi-layered security framework to support current standards [25].

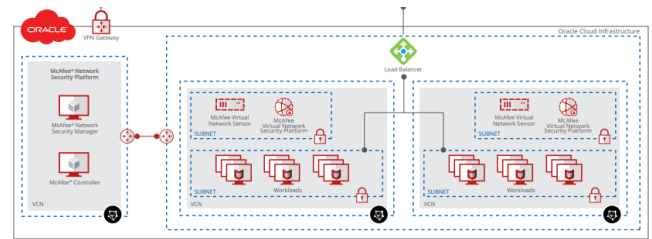


Fig. 7. McAfee Network Security Platform. Adapted from [26].

Incoming SSL traffic decryption that derives outside of the local network and is directed to the protected web service, is of special concern. This method could be used to hide malicious activities on public or intranet websites that could result in data loss, security breaches or infringement. A robust Secure Socket Layer (SSL) decryption and analytics functionality is required to overcome such system vulnerabilities. With its industry-leading incoming SSL scanning solutions, McAfee Network Security Platform offers true north-south and east-west traffic monitoring and security as seen in Figure 7. The McAfee IDPS can assist both the standard man-in-the-middle inspection and the shared key approaches for DHCE analysis. It is also equipped with a 100% decoding provision for outgoing connections while retaining maximum detection capability [25].

Modern risks necessitate sophisticated identification methods. McAfee Network Security Platform includes a signature archive of patented signatures created and managed by McAfee Labs, as well as personalised signatures. It can detect and defend against visible and invisible attacks, malware, Denial-of-Service attacks, zero-day attacks (threats which use avoidance methods), ransomware, as well as other cyberthreats. To prevent sophisticated coordinated attacks, this IDPS includes outbound and inbound SSL analysis, Gateway Antimalware (GAM) software and zero-day support, hybrid approach and behavioural evaluation, and dynamic analysis. McAfee Network Security Platform is indeed a unique automated threat identification and prevention software that supports latest detection techniques, fast bandwidth, low latency, and administration from a unified interface. It is also a comprehensive system that synchronises vulnerability intelligence from the machine to the cloud [25].

The very presence of false positives leads every security expert to become concerned. False positives, on the other hand, can differ from person-to-person. It is critical to analyse the precise definitions of various types of warnings in order to apply acceptable responses by using IDS and IPS technology to help handle security threats. There are three categories of warnings in Network Security Platform that are often misinterpreted as "false positives":

- Events that were improperly defined.
- Properly defined events that are subject to interpretation by usage policy.
- Accurately identified events that were meaningless to the individual.

By using initial policy specification and policy tuning, false positives can be avoided. The main objective of initial policy and policy tuning is to remove false positives and distortion, as well as to prevent an avalanche of genuine yet expected warnings [27].

There are few other, but substantial, limitations to this system, such as:

- Access rules should only be used for fragmented traffic with a TCP flow violation set to out-of-order permit.
- Syn-cookie cannot be used while the access rules for fragmented traffic are enforced.
- Firewall logging is not supported for fragmented traffic access rules.
- Since the interconnect ports of a sensor failover pair cannot be used for controlling traffic, they cannot be granted a QoS policy or a Rate Limiting profile.

It is important to understand that the problems listed above are present in many other Intrusion Detection and Prevention Systems and should not be used as a key guideline when selecting this software because the potential benefits of using this technology are much greater than the limited number of disadvantages indicated [28].

CONCLUSION

In today's modern world, where virtually any operation can be made and accomplished digitally, enhanced security is crucial in countering multiple cybersecurity threats. Cyberattacks, data fraud, and other types of information security threats have plagued enterprises in various economies. It is no wonder that businesses who prioritise data security invest not just in the right equipment, but also in the most knowledgeable security experts who stay current on industry trends and meet global expectations. Unfortunately, it is often human error that gives criminals access to secured networks and confidential details. While hackers may use "gifts" such as zero-day vulnerabilities to gain access to a device, their effectiveness is mostly dependent on manipulating or capitalising on user mistakes. Furthermore, the CIA triad, or confidentiality, integrity, and availability principles, is a paradigm intended to act as a reference to information management strategies used in an enterprise or organisation. Information security governance and risk management are inextricably linked since they both deal with corporate data assets as well as the identification, creation, and enforcement of policies, protocols, and guidelines. Data integrity, confidentiality, and availability are the objectives of information security governance and risk management. Control mechanisms such as risk evaluation and data analysis are used by businesses to classify resources, evaluate their limitations, and mitigate risks in order to efficiently enforce security measures. Security governance relates to management's direct impact on the risk management framework of the enterprise. It ensures that risk management in the company, especially among senior leadership, is not overwhelming to the point of exceeding the latter's risk profile.

APPENDIX A

Below is a list of the most relevant items of legislation in the United Kingdom:

- Data Protection Act 1998: Governs how businesses use sensitive information. The term "personal data" refers to knowledge about a living, recognisable person [29].

- Freedom of Information Act 2000: People have the right to access to records maintained by the organisation under this Act, limited to a few exceptions [30].

- Privacy and Electronic Communications Regulations 2003: Restrict the use of digital data as a means of advertisement and provide people with the ability to opt out of future interaction. People can also manage the digital advertising material they collect from organisations under Section 11 of the Data Protection Act [31].

- Regulation of Investigatory Powers Act (RIPA) 2000: Governs the rights of government authorities to conduct monitoring and investigations, as well as communications interception [32].

- Copyright, Designs and Patents Act 1988: Identifies and governs copyright law in the United Kingdom. CDPA classifies the various categories of projects covered by copyright [33].

- Computer Misuse Act 1990: It was enacted partly in response to a particular court case (R v Gold and Schifreen) and was designed to prohibit offenders from using a device to aid in the conduct of a criminal offence or from disrupting or impeding data that is stored on a device [34].

- Human Rights Act 1998: Incorporates the rights outlined in the European Convention on Human Rights from 1953 into United Kingdom law. Article 8, which deals with privacy, is particularly relevant to information security because it guarantees that the "private and family life, his home, and his correspondence" of a person are respected, a privilege that is also protected by the Data Protection Act [35].

- Equality Act 2010: It was enacted in October 2010 to replace a variety of several other pieces of equity law, including the Equal Pay Act, the Disability Discrimination Act, and the Race Relations Act. The Equality Act puts the four main EU Equal Treatment Directives into effect [36].

- Terrorism Act 2006: Establishes a variety of terrorism-related crimes. Organizations are required to report information to intelligence services under Section 19 of the Act if there is a presumption or knowledge of a terrorist crime being committed. Failure to reveal relevant details is a crime in itself [37].

- Limitation Act 1980: Prescriptive period that establishes clear time limits for pursuing legal action for violations of the law [38].

- Official Secrets Act 1989: Section 8 of the Act considers it illegal for a government agency to keep information longer than it is needed for official purposes and it requires them to better protect classified information from unintended exposure [39].

- Malicious Communications Act 1988: Sending or delivering letters or other documents for the intent of causing stress or distress is prohibited under the Malicious Communications Act. This includes electronic correspondence such as emails and tweets sent via social networking networks [40].

- Digital Economy Act 2010: In the United Kingdom, the Digital Economy Act governs the use of electronic content. It addresses concerns such as copyright laws and the responsibility of Internet Service Providers (ISPs) to combat online copyright violations [41].

- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011: In 2011, the Privacy and Electronic Communications Regulations were amended to require websites to warn users of their cookie use and to obtain permission before adding more privacy-invading cookies [42].

- Police and Justice Act 2006: Section 39 and Schedule 11 of the Police and Justice Act update the Protection of Children Act 1978 to authorise officers to remove inappropriate images of children kept by them after a lawful arrest [43].

- Counterterrorism and Security Act 2015: Makes it illegal to visit websites or other content that supports terrorism or violent extremism, or that aims to radicalise people to these causes [44].

APPENDIX B

C-level executives are critical to the success of any company since they provide strategic vision and ensure that the business operates properly. C-level individuals earn significantly more than other workers due to varying workloads and the fact that they will be required to make decisions that will affect the entire company. Executives in the C-suite are in charge of their company's specific division. They have a lot of clout and organisational obligations within the company, such as:

- Decision making.
- Delegation of responsibilities.
- Gathering information from employees for strategic planning.
- Hiring and firing staff members, even those in management.

The Project Management Office is responsible for all tasks related to the creation and implementation of an information security strategy and the programme that is built on it. This division's list of operations contains the following:

- Create, enforce, and manage a policy, strategy, and procedures for information security.
- Define duties and obligations for information management.
- Provide sufficiently qualified and competent professionals to execute the information security policy and strategy.
- Identify, organise, and retain the job items needed to put the information security policy and strategy into action.

The Governance, Risk Management, and Compliance department is responsible for all operations necessary to guarantee proper supervision, risk protection, and compliance with legal, administrative, regulatory, and other data security requirements. This department is in charge of the following operations:

- Establish, execute, and incorporate data security procedures for an information security policy and strategy.
- Create an information security risk assessment strategy, system, and applications.

- Regulate and supervise the information security policies and strategy.
- Conduct audits to ensure that safeguards are sufficient to satisfy security standards.

The External Relationships team is in charge of staying in touch with both internal and external partners involved in the information security programme. External and internal organisational relationship management entails the following activities:

- Managing third-party and external partners' partnerships
- Managing the development process of employees and their success in compliance with security policy and standards.

The Security Operations team is in charge of the enterprise's overall security; certain tasks can be performed by IT personnel with regular monitoring and reporting to the Security Operations team. The following are examples of standard activities:

- Handling bugs, malware, and malicious software.
- Taking care of security incidents.
- Gathering information sources.
- Analysing and mitigating risks to the information security of the company.

The Emergency Operations and Incident Management department collaborates closely with the Security Operations team. When an emergency is announced, this division's main duty is to mobilise resources, trigger contingency measures and coordinate incident management and emergency operations. During regular operations, this group collaborates with representatives of the Security Operations department to carry out the following tasks:

- Preparing ahead of time for incident prevention and response.
- Creating a corporate continuity strategy.
- Preparing for an IT emergency response operation.
- Putting all response plans into assessments, simulations, and drills.

The four divisions shown in Figure 2 are part of the Security Engineering and Asset Security team responsible for the following tasks:

- Building and managing a security model for the business.
- Managing device and programme settings.
- Ensuring that new inventions and technology are approved and accredited before they are implemented.
- Managing programme and system updates.
- Managing network, infrastructure, application, and device settings.
- Create, enforce, test, and manage access measures (e.g., VPNs, Firewalls) to secure network and Internet perimeters in compliance with security specifications.

Staff management department allows employees to reach their full capacity in their employment. Effective personnel management makes it easy for workers at all levels to relate their activities to the organization's strategic priorities. Some of their main responsibilities are mentioned below:

- Selecting and recruiting new workers, as well as ensuring that they are properly educated.
- Providing regular reviews to keep everyone on the same page.
- Holding regular performance evaluations.
- Maintaining high standards of productivity and morale, as well as taking measures to boost retention.

APPENDIX C

Eight fundamental rights of data subjects under UK-GDPR:

- The right to be informed: This applies to all information collection by businesses, and people must be notified data collection process. People must agree to the processing of their data, which must be voluntarily provided instead of inferred.
- The right to access: People have the right to seek access to the confidential information and to inquire about how the business handles it once it has been collected. If required, the organisation must have a complete backup of the classified information in a digital form.
- The right to have inaccurate personal data rectified: People have the freedom to amend incorrect personal details, whether they are out of date, missing or incorrect.
- The right to be forgotten: People have the right to have their data erased if they are no longer clients or if they revoke their permission for a business to access their private information.
- The right to restrict processing: People have the choice to opt out of the processing of their private data. Their information can be kept, but it cannot be utilized.
- The right to data portability: Consumers have the freedom to migrate their confidential details from one service vendor to another. It must also be performed in a language that is widely utilised and understandable by the computer.
- The right to object: This necessitates the ability of people to opt out of having their personal details used for targeted marketing purposes. This law has no exceptions, and all activity must come to a halt as soon as the query is sent. Furthermore, people must be told of their right to privacy at the outset of each information exchange.
- The right to be notified: In the event of a violation of data that exploits the sensitive information of an individual, the client has the right to be notified within 72 hours of the very first notification of the infringement.

The foundation of UK-GDPR is established by the data subject rights, which each organisation must enforce in the light of individual customers, staff, and other vendors [6].

APPENDIX D

Most businesses ignore data encryption policies. That must improve now that the UK-GDPR is in place, and one of the central aspects is that companies must safeguard data with effective technological and operational measures. Encryption, according to current guidance, is crucial [6]. Although encryption will not preclude unauthorised individuals from accessing or using an organization's data, it will prevent them from using it. It operates by obfuscating details and swapping markers with something else, making it only available or recognisable to those who have been given access. Organizations can opt to pseudonymize data instead of or in addition to encryption [45].

If a company does not want its employees to spend the whole day on non-work-related portals, it should impose an acceptable use policy. This act specifies some explicitly prohibited behaviours, as well as time limits for how much time employees can spend on non-work-related tasks. When establishing the acceptable use policy, precautions should be taken. It is crucial to note that keeping staff safe from malware and viruses is just as vital as keeping them from skiving. Employees should be aware of when their employer watches them in order to ensure that the legislation is enforced in compliance with the acceptable use policy. Organisations should never use extensive or automatic surveillance techniques, such as spyware, or any system that shows no evidence of the surveillance [46].

Password policies must specify how a password should be created (e.g., a mix of letters, numbers, and special characters) and force employees to use new passwords for each account. They should also put in place services that require employees to update their passwords every six months.

A strategy that hardens networks and identifies spam and malware must be implemented in every company. Phishing remains one of the most serious email-based risks, and technologies can only protect employees to a small degree. Spam messages are also persuasive enough to get through spam detection, which means the only thing standing between an enterprise and a security breach is the determination of its staff members to identify the danger. Employees should be required to attend routine personnel training classes to keep up to date on the possibility of email-based theft, according to email policy [47].

Companies should implement data processing policies that monitor the movement of data through their network and evaluate when data is stored, how it is used, and who collects it. This has been even more relevant since the UK-GDPR came into force, as it requires companies to respond with any of their data and provide the right answers to those who make data topic access requests [6].

APPENDIX E

ISO 9001 is a worldwide quality management system standard. To be accredited to the ISO 9001 norm, an organisation must adhere to the specifications outlined in the ISO 9001. Companies use this framework to show a commitment to deliver goods and services that reliably satisfy consumer and regulatory standards, as well as to demonstrate performance progress. ISO 9001 establishes a framework for the basic requirements of a quality control

scheme while being diverse enough to accommodate a wide range of companies. It is critical that people recognize how the norm applies to their current business. Individuals with this adaptability will be able to meet the requirements in a manner that is suitable for the market. Ensuring that upper management recognizes what ISO 9001 does for the enterprise and why it is being applied is vital to everything functioning properly. It is much more challenging to make improvements in the company if someone is not fully committed. Attempting to incorporate a risk control framework based on the ISO 9001 standard is a significant improvement for every organisation, and people must learn how to achieve it effectively. There are numerous options, which can be advantageous or harmful depending on how the organisation does it. The best choice, though, is to decide whether the corporation can afford to hire an experienced management systems consultant, such as QMS, to manage the whole development process. This would ensure that the ISO standard's standards are followed to the letter, applied in depth, and correctly managed. Although the expense will discourage certain enterprises from taking this route, it will ensure a quicker and error-free implementation. It could also indicate that specific ISO certification is obtained easily and effectively [48] [49].

ISO 9001 aims to provide an accessible and integrated Quality Management System for all facets of the organisation in order to improve and oversee all operations. It is not about putting in place a complex and time-consuming set of guidelines to comply with the ISO 9001 standard. The goal is to have a robust management framework that is customised to the needs of the organisation. If it has the knowledgeable employees and every person knows what they are doing, it guarantees a system that strengthens all aspects of the business. Enforcing a consistent and stable ISO 9001 standard will enable the organisation to focus on the most critical aspects of the industry while improving performance. Management practises introduced in the company will lay a solid basis for improved efficiency and benefit. Customer loyalty and satisfaction will improve as a result. Some of the most significant advantages of ISO 9001 standard include [49]:

- It is appropriate for both small and big businesses.
- A more robust internal management system.
- Enhancement of production, growth, and benefit.

- Strengthened customer loyalty and satisfaction.
- Consistent findings that are assessed and tracked.
- Internationally recognised norm.
- Numerous different ISO specifications that are compatible.
- UKAS certification.

APPENDIX F

Computer viruses are destructive programmes that have the peculiar potential to duplicate themselves in the operating system and switch easily from one device to another, causing data, records, and applications to malfunction. Antivirus software, on the other hand, is designed primarily to address the risks faced by malware. They secure critical infrastructure from malicious malware by heavily relying on safeguards built in their libraries. The antivirus software examines the system for known threats by searching for unique patterns in bytes. To remain relevant, antivirus creators must update their databases when new malware variants appear. Virus creators and antivirus providers have been engaged in a never-ending battle of evading identification by inventing new virus signatures. Computer viruses have become more advanced, using specialised code subterfuge methods to avoid identification by antivirus software. Software viruses that are polymorphic or metamorphic are generally the most difficult to identify. This is why each organisation must introduce a particular antivirus programme that will fulfil all specifications [50].

The Cloud Access Security Broker (CASB) lies between the cloud software and its customers, transmitting sensitive data until it is delivered to the cloud infrastructure and swapping it with a meaningless token or encryption attribute that has no significance for the cloud. A CASB connects cloud services to the outside environment by using a mix of proxies and API connections to software to arbitrate communications. With the implementation of the CASB structure, encryption becomes straightforward and automated, allowing consumers to maintain the most comprehensive search features. In addition, CASB serves as a centralised hub for tracking and handling cloud service access [51].