European Journal of Computer Science and Information Technology, 12 (2),93-107, 2024
Print ISSN: 2054-0957 (Print),
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Human and Technology Components in Data/Information Security

Felicia Bosede Kehinde Fasae
Management Sciences
Office and Information Management
Bamidele Olumilua University of Education, Science and Technology, Ikere-Ekiti

doi: https://doi.org/10.37745/ejcsit.2013/vol12n293107 Published May 04, 2024

Citation: Fasae FBK (2024) Human and Technology Components in Data/Information Security, *European Journal of Computer Science and Information Technology*, 12 (2),93-107

ABSTRACT: *This paper reviewed the relationship between human and technology components in data/information security, looking into how humans and technological components affect the security of data/information. The paper considered information resources, importance of data/information, data/information security, human factors in data/information security, technological components in data/information security, importance of human and technology components in data/information security, and risk assessment. The paper concluded that effective management of humans and technology is indispensable in order to ensure protection to data. It was recommended, among others, that organizations should train their workers on the importance of data/information security; ensure that workers comply with laid down regulations regarding data/information security; and Computer Science community should, as a matter of urgency, conduct researches in aspects that explore the human factors and technology in cybersecurity from a multidisciplinary perspective.*

KEYWORDS: human factor, security, data/information, technology factor, threat.

INTRODUCTION

Data and information play a crucial role in the success of organisations in today's economic world. However, due to their significance, organisations confront many security concerns that necessitate the implementation of security measures to prevent unauthorised use, loss, or leakage. Security is the systematic implementation of measures to prevent loss or unauthorised access. Duhigg (2012) and Schneier (2015) noted that data and information have become very important assets for organisations in modern society. However, their extensive use also poses considerable issues, especially in terms of data security. Musty (2023) observed that in the present day, companies are faced with the challenge of managing substantial amounts of data, which is crucial for making important decisions and carrying out daily operations. These extensive data sets, originating from various sources, require effective handling in order to derive maximum benefit from them.

Data and information are essential resources that organisations require to make informed decisions in order to achieve their organisational objectives. They are necessary for the allocation of resources, establishment of organisational objectives, assuring the achievement of goals through informed decision-making, and promoting the harmonious functioning of the entire system. The terms "data" and "information" are often used interchangeably, and this will also be the case in this study. Organisational data encompasses all information pertaining to many aspects of an organisation, such as personnel, finance, administration, management, health, and maintenance. Oseni-Ope (2004) defines data as discrete units of information that are typically organised in a certain format, such as numbers or text on physical documents. Data is crucial for any company since it enables the extraction of present and future insights. In Kaur's (2012) perspective, 'Information' encompasses all valuable forms of information, regardless of whether they originate from within or outside the organisation. This includes data resources such as production data, personnel-related records and files, market research data, and competitive intelligence obtained from various sources.

There is a requirement to effectively and efficiently handle data/information, utilising the suitable technologies to avoid loss, leaks, thefts, and attacks. Kaur (2012) emphasised that the term 'information management' is used with ambiguity in various fields such as computer science and its applications (information technology management/data management), business or management studies (technology management with a focus on the relationship between information technology and business performance and competitiveness), and librarianship and information science (emerging market for information workers (managers) who perceive information as encompassing data, organisational intelligence, competitive intelligence, external information resources, and the associated technology for handling these sources).

The significance of ensuring the security of data and information cannot be overemphasised, considering their crucial role in the success of an organisation. In his study, Lopez (2013) emphasised several factors that justify the need to protect data and systems, such as establishing confidence across different sources, developing a positive reputation, and fostering collaborative efforts within a social context. He observed that the systems must handle the data in accordance with limitations while also upholding other prerequisites for data infrastructures, as well as protecting the systems from potential external threats. The speaker asserted that there are four specific ways in which significant effort is needed to address schemas for security metadata. These include: identifying the structure, elements, attributes, and values of the metadata schema itself; expressing these schemas when security information is transmitted using various protocols; handling the multi-domain nature of these metadata; and ensuring seamless integration of security metadata with general metadata formats.

Throughout history, secretaries, office managers, and information managers have been responsible for overseeing various tasks related to information management, such as receiving, recording, processing, safeguarding, and filing. They possess expertise in office management and administration. The name secretary implies the ability to maintain confidentiality, which is a crucial professional attribute for a secretary. Advancements in

information processing and technology have improved data and information management in organisations. This highlights the importance for office professionals to enhance their skills to keep up with current advances. Prior to the present time, Wellings (2023) concluded that workers' sensitive information was traditionally stored securely in locked filing cabinets and drawers labelled as 'confidential'. However, in order to protect this information from cyberattacks, it is now imperative to implement strong and advanced data security measures for the benefit of employees and HR teams. Thus, it is incumbent upon every employee, regardless of their position within the company, to protect crucial data. This responsibility extends beyond the IT department and requires the active participation of every individual in the organisation.

Humans are the primary and indispensable asset of an organisation, particularly in the field of information management. Their temperament, attitude, willingness, perception, and behaviour play a crucial role in determining the security of data, making them the most significant threat to data security. Abebe and Lessa (2020) emphasised that human factors are a crucial concern in the security of information systems within organisations. They argued that relying solely on information systems security technologies does not always lead to enhanced security, as security is primarily influenced by human behaviour. The relationship between humans and information systems has consistently presented numerous security vulnerabilities (Alhogail et al., 2015; Naidoo, 2020).

Given the significance of data in organisations, the management and security of data have become essential. Siponen, et al (2014) stressed the importance of security and regarded employee compliance with information security policies as crucial for protecting sensitive data in organisations. In contrast, Herley (2017) demonstrated that comprehending the reasoning behind users' choices regarding security advice is vital for creating efficient security measures.In view of the importance of security to data/information, this study reviewed the relationship between human and technological factors in data/information management in order to reveal their impact on data/information security.

Information Resources

Information resources consists of a range of things such as people, technologies - --hardware and software), information bearing materials, texts – physical or electronic, equipment, data and information, among others. Fashola, et al (2020) saw information resources as a collection of valuable information generated by human activities, including related equipment, personnel and capital, required to produce information, including hardware, software, technical support, users, facilities, data systems and data. Information Resources as Strategic Tools (wiley.com, 2024), stated that information resources (IS) are not just the infrastructure, but the available data, technology, people, and processes within an organization to be used by the manager to perform business processes and tasks. IS infrastructure is an information resource, as is each of its constituent components. The relationship between a firms' IS managers and its business managers is another type of information resource. E.g. hardware, software, network, and data components are is infrastructure; information and knowledge, proprietary technology, technical skills of the IT staff, end users of the IS, r/ship between it and business managers, business processes, etc.

Kaur (2012) sees information resources in organizations as constituting: d*ata (*data on organizations' state of markets, economic circumstances of the country or of its exports markets, which enable the firm to identify potentially profitable products, markets and export areas, and may have potential for competitive advantage and must be maintained securely and effectively if the organization is to benefit from having them available); r*ecords (*a personnel record identifies an individual's data such as age, training level, sex, marital status, courses attended, year of entry to the organization, and many more, which may be textual in character and will consist of files of reports, test results, correspondence with suppliers, etc.); t*ext (dealing* with the acquisition, organization, storage and dissemination of printed materials, most often from outside the organization of which the library or information Centre formed a part, but also often including the maintenance of stores of internal reports, particularly in research-intensive organizations, with the development of office automation systems and the creation of many more electronic documents in organizations, there is increasing awareness of the need for effective information retrieval systems to underlie the database of electronic documents); m*ultimedia (a*ll the above, together with sound recordings, graphics, pictures and video, may now exist together in a single 'document', published as CD-ROM packages); and, i*nformation technology which are* computers, telecommunications and software systems that aid the organization, transmission, storage and utilization of what might better be called the 'knowledge resources' mentioned earlier. He added that information resources may include expert systems and other manifestations of developments in artificial intelligence, such as the 'learning' systems created through neural net technology.

Wondering how data/information could be secured, Lopez (2013) asserted that security must become pervasive and be dynamically associated with data themselves and their metadata so the entities in the different ecosystems can apply the policies they consider relevant. These security metadata should contain access requirements for datasets, accounting records to evaluate their provenance and integrity, and reputation records that will allow the entities to decide on the trust and usability of each dataset. Derived datasets built for whatever purpose (interdisciplinary access, privacy preservation, correlation, etc.) will generate their security metadata from the origin dataset(s) so as to provide a coherent availability of security information across different ecosystems and access patterns. Security metadata accuracy requires well-established services for identifying not only entities but also datasets themselves, and therefore a system guaranteeing global, well-structured, verifiable permanent identifiers should be in place. Entities should be able to prove their identities by different mechanisms at identity providers (IdPs), according to security and usability criteria. Identity attribute values will be established by means of attribute authorities (AAs), under control of different organisations and communities. The identity will be transferred to applications by means of identity relying parties (IRPs) that will accept data of recognized IdPs and AAs. This requires an established trust framework between the interacting parties. Whereas this can be considered the current status of identity federations, we envisage evolution along these main lines: the dynamic establishment of federation associations, the aggregation (and possibly translation) of identity data from different sources, and the possibility of expressing the levels of assurance for identification mechanisms and attributes.

Importance of Data/Information

The significance of data/information management to an organisation cannot be underestimated. Efficient data management is crucial for making informed decisions about the organization's operations, personnel, and both current and future aspects of the organisation. According to Stedman and Vaughan (2023), data is now being seen as a valuable resource for businesses. It can be utilised to make more informed decisions, enhance marketing strategies, streamline processes, and minimise expenses, all with the aim of boosting revenue and profits. The Council on Quality and Leadership (CQL) (2024) stated data as useful information collected to support organizational decision-making and strategy and highlighted the following as reasons why data/information are important to organizations:

i. Effective data system can enable organizations to improve the quality of people's lives by allowing you to measure and take action.
ii. By utilizing data for quality monitoring, organizations are able to respond to challenges before they become full-blown, therefore, monitoring the health of important systems which will help organizations to be proactive rather than reactive and able to maintain best practices over time.
iii. When strategies are put into place to overcome a challenge, collecting data will allow organizations to determine how well their solution is performing, and whether or not the approach needs to be changed over the long-term.
iv. Data allows organizations to visualize relationships between what is happening in different locations, departments, and systems and helps to develop more accurate theories, and put into place more effective solutions.
v. Utilizing data will help organizations present a strong argument for systems change whether advocating for increased funding from public or private sources, or making the case for changes in regulation.
vi. Whether or not your strategies and decisions have the outcome you anticipated, you can be confident that you developed your approach based not upon guesses, but good solid data.
vii. Effective data collection and analysis will allow you to direct scarce resources where they are most needed, thereby increasing efficiency.
viii. Data allows you to replicate areas of strength across your organization by identifying high-performing programs, service areas, and people in order to develop strategies to assist in each regard.
ix. Good data allows organizations to establish baselines, benchmarks, and goals to keep moving forward.

Kaur (2012) maintained that records management gave birth to the idea of an information life cycle which is central to the overall process of information management. The life cycle of records (sometimes referred to as 'document control') includes: design and creation of records; identification; authorization; verification, validation, auditing; circulation, access, loan, use; back-up procedures and disaster recovery; plans; and retention schedules and

destruction and it varies from organization to organization depending on the nature of the information, the means used to organize it, the extent of use and the controls put upon use.
On increasing importance for organizations to implement evidence-based practices and develop systems to collect and analyze data, CQL (2024) emphasized that funding is increasingly outcome and data-driven, considering the shift from funding that is based on services provided to funding that is based on outcomes achieved.

Data/Information Security

Data/information security is necessary due to potential threats to its safety. A threat refers to a deliberate action aimed at compromising or pilfering data, or causing disruption to an organization's operations. This might arise from data leakage or inadequate network control, potentially exposing data to hackers, insiders, internal disasters, or human mistake. Any action that has the potential to compromise the secrecy, accuracy, or accessibility of data originating from etc.

Data security refers to the utilisation of technologies to ensure the protection and preservation of data. The authors Ugochukwu-Ibe, et. al, published a paper in 2014. According to Wikipedia (2012), data security refers to the employment of techniques to safeguard data against harmful forces and unauthorised actions by users without permission. Abebe and Lessa (2020) asserted that in order to enhance the security of information assets, it is necessary to have a comprehensive grasp of the human element. The authors observed that the framework developed by Alhogail et al. (2015) offers a thorough understanding of the human factors that impact individuals' behaviour towards information security within organisations. According to Pollock (2017), academics have long recognised that human mistake is the primary cause of information systems security breaches, and this continues to be the main issue today. Quantifying the impacts of information systems security incidents is frequently challenging due to the tendency of studies to either exaggerate or underestimate the associated expenses. Human mistake is consistently a primary factor contributing to failure in numerous organisations and professions, often disregarded or underestimated as an unavoidable occurrence. Furthermore, other factors contribute to an information systems security breach resulting from human error, including insufficient awareness, monotony, inadequate training, and a lack of risk perception. However, human error can occur unintentionally due to either the improper implementation of a plan (slips/lapses) or the accurate but insufficient execution of a plan (mistakes). Regardless of intentionality, errors have the potential to result in vulnerabilities and security breaches, as mentioned in (Pollock, 2017). Therefore, humans continue to be the most vulnerable aspect in the process of interacting with the computers they use and in maintaining the security of information systems.

Lopez (2013) defines "data security" as including several aspects of data infrastructures, including technical and organisational elements such as procedures, rules, and physical access. Implementing data security is crucial for all components of a data infrastructure, since any weak point could possibly compromise the entire secure system. According to the ISO/IEC 27031 standard from 2011, the author categorised security concerns into three main groups: Business continuity, Incident handling, and AAA (Authentication, Authorization, and

Accounting). Authentication enables users, whether they are human or other agents, to verify their identity by providing traits that are associated with them and are pertinent to a certain purpose. Authorization grants a user the permission to carry out a specific action on a specific resource at a specific time, based on the user's identification attributes and the relevant regulations set for accessing the resource. Accounting gathers information on both approved and denied access requests to resources, documenting the credentials provided by the requester, the sought resource, and the result of the request. The data can be further analysed for many purposes, but its most significant application in terms of security is its capacity to track activities and identify breaches, attack patterns, and compromised entities. Based on the definitions provided, it is evident that in a complex and collaborative setting that spans multiple administrative domains and national boundaries, authentication should be conducted as close to the users as feasible. On the other hand, authorization should be determined as close to the resources as possible. Additionally, accounting must be carried out in a coordinated manner in order to derive any meaningful information from the records.

Furthermore, despite the use of security measures, Acquisti & Grossklags, 2005; Ponemon Institute, 2020) have noted that the complex nature of data security is highlighted by the importance placed on privacy and the economic consequences of data breaches. Given the significance of data, legislative frameworks like the EU General Data Protection Regulation (GDPR) create criteria and recommendations for ensuring data security and adhering to regulations (EU GDPR, 2016). Lopez (citing Kizza, 2019) highlighted the importance of technological components, particularly encryption techniques, in protecting data from unauthorised access. Frameworks provided by organisations such as the National Institute of Standards and Technology (NIST) play a significant role in enhancing cybersecurity (NIST, 2017).

In addition, CQL (2004) has created the PORTAL Data System to assist organisations in documenting, monitoring, analysing, and recording personal outcomes and support services for individuals receiving assistance. This system includes the widely recognised Personal Outcome Measures and Basic Assurances, which are used to assess and evaluate various aspects of quality of life such as health, safety, social roles, rights, relationships, community integration, employment, and more. In addition, Oseni-Ope (2024) emphasised strategies for mitigating the difficulties related to data/information management, including: establishing a suitable work environment for completing tasks; identifying the necessary tools/office equipment such as computer systems and accessories, filing systems, and other essential tools; Archiving involves guaranteeing the thorough documentation of your work. Efficiently storing data to ensure its accessibility and usability when required; and distributing data to the Central Hub, among other tasks.

Human Factors in Data/Information Security

People determine the success or otherwise of organizations and are often linked to causing threats to information/data safety. The importance of humans in data/information security cannot be overemphasized. Every human being is unique and this uniqueness tends to affect everything that has to do with human. Same with data/information security. The reasons, as identified by Rahman and Kanthamanon (2021) is not unconnected with neglect by Computer

Science (CS) researchers who have investigated only the technical aspects of cybersecurity through, focusing on the encryption and network security mechanisms and neglected the human aspect, which is also very important. Their review considered the top conferences on network and computer security for the past six years and results showed that both expert and non-expert users pose different threats and challenges to any cybersecurity system in general, and, in particular, it was expected that mistakes made by the experts will have more severe and long-lasting consequences on the security aspect, since they are closely involved with the building, working, and maintenance of such systems.

Abebe and Lesser (2020) noted that human factors represent essential issue in information systems security in organizations, since they determine the behavior of employees toward information systems security; the only application of information systems security technologies could not always result in the improved information systems security as security is largely associated with people. Kaur (2012) however noted that functional divisions of an organization often have more expertise in the matters underlying software packages than the computer managers (office manager). Ludwig et al. (2014) also noted that human cognition and decision-making related to information systems is majorly reflected in a comparatively sparse set of disconnected publications, sometimes using inconsistent theory, methodology, and terminology.

Ugochukwu-Ibe, and Onyemachi (2014) identified three reasons why human factors are responsible for impacting the usage of data/information to be cognitive biases, perception and behaviour of humans.

(a) Cognitive Biases: These are inherent in human decision-making processes and usually affect data/information usage and security outcomes. Biases such as confirmation bias, where individuals seek information that confirms their preconceptions, and availability heuristics, where people base decisions on readily available information, can lead users to underestimate or overlook potential security risks (Yerby, Senft & Besmer, 2021). Being a side effect of the application of heuristics, cognitive biases are defined as systematic errors in human decision-making, the results of which are objectively non-rational decisions that often lead to suboptimal outcomes for the decision-maker or other individuals who are affected by the particular decision (Wilkinson and Klaes, 2012).

Unavailability of standardized security-specific scales that can measure the cybersecurity perception of the users was also identified by Suryotrisongko and Musashi (2019) in Rahman and Kanthamanon (2021) observing that the Computer Science (CS) community failed to work on the concept and range of cybersecurity, including an overlap of data, systems (technology), and most importantly the human beings. Concluded that the highly subjective and complex human psychology that cannot be avoided in any cybersecurity scenario, and often considered to be the weakest link in the cybersecurity chain needs to be explored from multiple angles involving the CS community, the Information Science (IS) community, the social science community and from a psychological viewpoint.

b. Behavioural Aspects Affecting Data Security: Behavioural aspects, encompassing user habits and routines, are pivotal in determining the efficacy of data security measures. Gupta, et al. (2020) revealed a prevalent tendency among users to prioritize convenience over security considerations, resulting in risky behaviours such as password sharing and neglecting software updates. Capone (2018) opined that people should be the last thing in charge of cybersecurity, people should be removed while transparency and automation be added for true protection. He highlighted four reasons why people should not be in charge of cybersecurity to be: the world is just too dangerous; manual methods can't keep up; too much sharing is hard to manage; and some data breaches are intentional and concluded that while people are certainly an important aspect of data security and serve as critical administrators, they cannot serve as the be-all-end-all because human behavior has proven that we choose to take the easy road, cut corners and make mistakes. He agreed that humans are prone to mistakes but when it comes to critical data, maintaining intellectual property, staying in compliance, sensitive information and brand reputation are just too important that we cannot afford to make mistakes.

(c) User Perceptions and Attitudes Towards Security Measures: Every individual is a peculiar person, hence, human perceptions and attitude tend to differ, depending on the person and the organization and these factors significantly influence adherence to security protocols. Jiang *et al.*, (2019) observes that perceptions of personal risk, trust in technology, and usability concerns shape users' willingness to adopt security measures, therefore, tailoring security measures towards user perceptions and attitude can enhance their effectiveness in mitigating security risks. Oates (2018) reiterated that human perception aspect has often been neglected or given less priority by CS scholars, even though most of the large-scale security incidents have often been traced back to human errors, like mistake or forgetfulness.

Technological Components in Data/Information Security

Technological components play a critical role in safeguarding data and information from various threats. Whitten & Tygar (1999) explained that the following security technologies are indispensable for protecting data from unauthorized access, manipulation, and theft.

a. Encryption methods: With the proliferation of cloud computing and remote data storage solutions, Acar *et al.*, 2016) saw encryption as a way of protecting sensitive information from unauthorized access and interception. Advanced encryption algorithms, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), ensure confidentiality by converting plaintext data into ciphertext, which can only be deciphered with the corresponding decryption key (Jagannath & Jacob, 2020).

b. Access controls and authentication mechanisms: Access control mechanisms, such as role-based access control (RBAC) and attribute-based access control (ABAC), enable organizations to enforce granular access permissions tailored to users' roles and responsibilities (Alotaibi, Ho, Zhu & Alqahtani, 2019). Additionally, multi-factor authentication (MFA) methods, including biometric authentication and token-based authentication, add an extra layer of security by requiring users to provide multiple forms of verification before accessing protected resources (Liang, Li, Zhang & Shen, 2019).

c. Emerging technologies for enhancing data security: Swan (2015) believed that blockchain technology, known for its decentralized and immutable nature, holds promise for ensuring the integrity and authenticity of data through cryptographic hashing and distributed consensus mechanisms. Similarly, Lauter, Naehrig and Vaikuntanathan (2016) agreed that homomorphic encryption, a cutting-edge cryptographic technique, allows for computations to be performed on encrypted data without decrypting it, enabling secure data processing in untrusted environments. Also, artificial intelligence (AI) and machine learning (ML) algorithms are increasingly being leveraged for anomaly detection, threat intelligence, and behaviour-based authentication, augmenting traditional security measures with proactive threat mitigation capabilities (Zheng *et al.*, 2021).

Importance of Human and Technology Components in Data/Information Security

Considering the usefulness of data in organizations, there is the need to identify, assess and implement strategies for controls in order to prevent applications defects and vulnerabilities. Ability to assess the threats facing data/information systems networks and data and assessing the potential consequences that they face should these adverse events occur.

The relationship between human behaviour and technology in the context of data/information security is a complex and dynamic one that significantly influences security outcomes. Human behaviour shapes technology usage patterns, while technology, in turn, influences human decision-making processes and behaviours. Stanton, et al (2005) observed that data/information security is not solely reliant on technological measures but is also deeply influenced by human factors such as cognitive biases, perceptions, behaviours, and knowledge, which significantly impact data-handling practices and security outcomes. For instance, users' lack of awareness about security best practices and susceptibility to social engineering tactics can undermine even the most robust technological defences.

Although technological components play a critical role in safeguarding data and information from various threats, Whitten and Tygar (1999) noted that the effectiveness of these technological measures can be compromised if human factors are not adequately considered and that complex authentication procedures may lead to user frustration and circumvention of security protocols. The synergy between human behaviour and technology is evident in security incidents, with many breaches stemming from human errors like inadvertent data disclosures and falling prey to phishing (Dhamija, et al, 2006).

Risk Assessment

The significance of integrating human elements (human-centered risk assessment) into risk assessment frameworks for a thorough evaluation of security threats cannot be overstated, given the intricate nature of the link between humans and technology. Organisations must develop tailored security awareness initiatives to prevent unauthorised access to data/information. These are methods for guaranteeing the security of data/information in the context of human and technology interaction, a procedure employed to identify probable risks and choose appropriate actions in the event of an incident. There are numerous hazards to consider, and each hazard could have many possible scenarios happening within or because

of it (https://www.ready.gov>planning (2024). Gertenbach (2023) has the following tips to offer on best practices for data security, among others.

1. **Establish access controls:** Decide who can access sensitive , that is, who truly needs to access this data – and who doesn't and implement permissions for employee data protection. Store the data in such a way that only certain allowed users—determined by a special login or other identification method—can access the files.
2. **Encrypt all company data:** Encryption is a form of cryptography, and works a bit like sending secret messages. When you encrypt a file, its contents are scrambled and can only be unscrambled or decoded by a person or program that holds the encryption key. If anyone else intercepts the file and tries to open it, they won't be able to read the contents.
3. **Use antivirus and anti-malware software:** Computer viruses, malware, and other malicious files can hide in innocent-looking downloads, links, and programs. Once these files enter your workplace computer system, your entire company can be at risk. Antivirus and anti-malware software programs like Avast or Avira are one line of defense against these issues.
4. **Implement security policies:** For your security measures to work, it's advisable to develop clear policies *and* train your team on how to follow them. Policies such as when and how to request systems access permissions, how frequently, and in what way, team members need to create new passwords, which tools and programs are allowed for use in the work environment, among others.
5. **Appoint a data security officer:** If your company must adhere to data privacy laws—like the European Union's General Data Protection Regulation (GDPR) or California's Consumer Privacy Act (CCPA)—you *could* be required to appoint a designated data security officer.
6. **Back up all data by implementing regular backups:** Typically, a backup creates a complete copy of your computer, server, or mobile device—though you can also set up backups to only copy select files and programs. You may store these backups locally—such as on another computer or server—or in the cloud. It's typically a good idea to do both. This way, if anything happens to your physical backup, you can pull from the cloud and vice versa. Others are secure mobile devices, outsource work securely, conduct security audits, prepare for security incidents, among others.

Kumaraguru, et al (2007) argued that organisations can pinpoint areas for enhancement and optimise their security awareness initiatives by assessing metrics such as user compliance rates, incident response times, and security incident patterns. The three identified areas are: the establishment of regulatory frameworks to protect data and privacy, which involves creating laws and regulations to safeguard individuals' privacy rights and ensure responsible data handling; the consideration of ethical implications related to human and technological interventions, specifically the use of surveillance technologies to monitor online activities of employees or individuals; and the adherence to data protection laws and regulations, which involves complying with relevant regulatory requirements, implementing suitable security measures, and ensuring transparency and accountability in data processing practices.

According to Wellings (2023), being vigilant is crucial for employees to ensure data security and prevent breaches. Adopting a watchful and doubtful attitude is the initial barrier against phishing assaults. Employees have a crucial role in protecting sensitive data, and their responsibility is extremely important. It is crucial to scrutinise the authenticity of each email and online engagement. If something appears suspicious, pause briefly to confirm its genuineness. Additionally, it is imperative to promptly notify your organization's IT or security staff of any dubious activities or emails. Timely notification can preempt potential data breaches and enable security teams to promptly take appropriate measures to counteract cyber threats.

In addition, HR Future (2024) outlined six effective strategies for safeguarding employee data and privacy. These include adhering to various rules and regulations imposed by local, state, federal, and industry-specific authorities to ensure legal compliance, combating prevalent unethical practices, and identifying past instances of such practices to better equip oneself in combating them. Supervise the activities of your team that are pertinent to their safety in order to assist you; Provide training and education to individuals in order to prevent cyber assaults and ensure the safety of their data and privacy. Keep and manage records; Secure your data using encryption and ensure that your workers are well-prepared to effectively counter potential threats.

CONCLUSION

The need for data security in organizations cannot be over emphasized due to its importance. The review of literature revealed that humans and technology components in data/information security are intertwined. The need arises for effective management of humans and technology to ensure data/information protection.

Recommendations

1. It is imperative for organisations to provide training to their employees regarding the significance of data/information security.
2. Organisations must guarantee that employees adhere to established regulations on data/information security.
3. Organisations should implement measures to scrutinise the data and information that enters their websites and browsers.
4. Organisations should implement security awareness initiatives to equip personnel with the knowledge and skills to identify and address security issues in a competent manner.
5. Terminate an employee's network access promptly upon their departure from the organisation.
6. Individuals responsible for data/information should endeavour to safeguard their files by employing robust passwords that are not easily accessible.
7. Information managers must have a constant awareness of data/information security to avoid becoming targets of hackers.
8. Information managers must ensure that they consistently log out at the end of each page session.

9. Given the lack of adequate research in data/information security, it is imperative for the Computer Science community to promptly undertake research in the area that examines the human components in cybersecurity from a multidisciplinary standpoint...

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26-33.

Acar, A., Aksu, H., & Dagdelen, O. (2016). A Survey on Cryptographic Software Libraries. ACM Computing Surveys, 49(3), 1–36.

Alotaibi, M., Ho, A. T. S., Zhu, L., & Alqahtani, F. S. (2019). Enhancing Security in Cloud Computing by Integrating RBAC with ABAC Model. *Journal of Cloud Computing*, 8(1), 1–15.

Corydon, B., Ganesan, V., & Lundqvist, M. (2016). Transforming government through digitization

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06), 581–590.

Duhigg, C. (2012). The Power of Habit: Why We Do What We Do in Life and Business. Random House.

Emily Gertenbach, E. (2023). Protecting Employee Data: 12 Best Practices for Data Security. https://www.upwork.com/resources/employee-data-protection

EU General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

Gupta, M., Brooks, R., Vos, J. de, & Dewhurst, D. (2020). Understanding User Perceptions and Behaviours Towards Software Updates. In Proceedings of the 12th International Conference on Human Factors in Information Security (pp. 1–11).

Herley, C. (2017). So long, and no thanks for the externalities: The rational rejection of security advice by users. In Proceedings of the 2009 Workshop on New Security Paradigms Workshop (pp. 133-144). ACM.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27031 (2011) Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity.

Information Resources as Strategic Tools (wiley.com, 2024), https://catalogimages. wiley.com/images/ db/pdf/0471346446.ch2.pdf

Fagbola, O. O.; Smart, A. E. & Oluwaseun, B. O. (2020). Application of cloud computing technologies in academic library management: The National Open University of Nigeria library in perspective. Handbook of Research on Digital Devices for Inclusivity and Engagement in Libraries. 25 - 35, DOI: 10.4018/978-1-5225-9034-7.ch007

info@hrfuture.net: 6 Best Ways To Protect Your Employee Data And Privacy https://www.hrfuture.net/talent-management/technology/6-best-ways-to-protect-your-employee-data-and-privacy/

Jagannath, S. K., & Jacob, S. K. (2020). A Comparative Study of Encryption Algorithms for Cloud Data Security. International Journal of Advanced Research in Computer Science, 11(1), 35–40.

Jiang, L., Rajivan, P., Chiasson, S., & van Oorschot, P. C. (2019). An Exploration of Users' Security Perceptions and Attitudes Towards Online Social Networks. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19) (pp. 1–15).

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. Econometrica, 47(2), 263–291.

Kaur, B. (2012). Information Management. *Council for Innovative Research International Journal of Computers & Technology*. 3(3), 424 – 427. Nov-Dec. www.cirworld.com

Kizza, J. M. (2019). Guide to Computer Network Security. Springer.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Teaching Johnny Not to Fall for Phish. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), 617–627.

Lauter, K., Naehrig, M., & Vaikuntanathan, V. (2016). Can Homomorphic Encryption Be Practical? Proceedings of the 3rd ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography (pp. 113–114).

Liang, X., Li, X., Zhang, X., & Shen, X. (2019). A Survey on Multi-Factor Authentication Systems. *Future Generation Computer Systems*, 92, 874–889.

Musty, B. (2023). Analyzing the Changing Role of Professional Secretary in Dealing with The Impact of Digital Technology: A Case Study on Professional Secretaries in Indonesia. *International Journal of Business, Economics and Social Development*. 4(1), 12-19. www.https://journal.rescollacomm.com/index.php/ijbesd/index e-ISSN 2722-1156 p-ISSN 27722-1164

National Institute of Standards and Technology (NIST). (2017). Framework for Improving Critical Infrastructure Cybersecurity. U.S. Department of Commerce.

Oates, M. (2018). Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. Proceedings on Privacy Enhancing Technologies. 5–32.

Rahman, T; Rohan, R.; Pal, D. & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. In The 12th International Conference on Advances in Information Technology (IAIT2021), June 29–July 01, 2021, Bangkok, Thailand. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3468784.3468789

Șerban, R. A. (2017). The impact of big data, sustainability, and digitalization on company performance. *Studies in Business and Economics*, 12(3), 181-189

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224.

Suryotrisongko, H. and Musashi, Y. 2019. Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective. 2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA) (2019), 162 – 167.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

Tayo Oseni-Ope (2024). Importance of data management. https://eprints.covenant university.edu.ng/10284/3/Importance%20Of%20Data%20Management.pdf

The Council on Quality and Leadership (CQL) (2024) www.c-q-l.org

Ugochukwu-Ibe, Ijeoma Marya and Onyemachi, Chibueze Princeb (2014). Data Security: Threats, Challenges and Protection . *Journal of Universal Development Initiative (JUDI).* 1(1), 92 – 99. December. ISSN (print): 2141-6974

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium (pp. 169–184).

Wikipedia. (2012, February). *Data_Security*. Retrieved August 18, 2014, from Wikipedia the free Encyclopedia: http://en.wikipedia.org/wiki/Data_security

Wilkinson, N. and Klaes, M. (2012). An Introduction to Behavioral Economics. 2nd Edition. Palgrave, Macmillan, New York, USA.

Yerby, J., Senft, S., & Besmer, A. (2021). Misinformation: A Cognitive Bias Framework for Information Security Decision-Making. Journal of Cybersecurity, 7(1), tyaa023.

Zhang, T., Lu, J., Xiong, Y., Wu, Q., & Dou, W. (2019). Privacy-Preserving Edge Computing for Internet of Things: From Requirement to Algorithm Design. IEEE Network, 33(6), 16–21.