جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Prioritizing Personal Data Protection in Insurance Organizations: A Review

Cosmas Knowen*, Lamek Ronoh, Anne Mugalavai
Department of Information science and informatics, Rongo University, Kenya.

CrossMark

Received 31 Mar. 2023; Accepted 14 Jun. 2023; Available Online 22 Jun. 2023

Abstract

This literature review focuses on the importance of prioritizing personal data security in insurance organizations in the context of Web 2.0 and the fourth industrial revolution. With the increasing use of digital transactions and data sharing, there is a need for improved data security postures to mitigate vulnerability issues. Personal data is a valuable asset that is targeted by malicious individuals, which highlights the importance of establishing proactive and trustworthy security frameworks. The study evaluates the security threats associated with the collection, processing, storage, and retention of personal data in insurance organizations, and examines the legal and technical provisions for its protection. Through an analytical review methodology, this paper highlights the urgent need to establish robust data security measures to ensure that personal data is secure when held in the custody of insurance organizations and personal management information systems.

I. Introduction

This paper makes a significant contribution to insurance organizations specifically by highlighting the importance of establishing proactive and trustworthy security frameworks for the protection of personal data. The motivation behind this research stems from the need to address security gaps in data processing organizations. Therefore, addressing the problems has significant implications for streamlining frameworks for personal data security. The current focus on personal data security as a valuable asset in the Darkweb raises an urgent need for prioritizing the security posture. The paper is organized as follow; introduction, literature review whereby the paper highlights the security threats associated with personal data, and legal and technical mechanisms for the protection of personal data. The paper also discusses through cyber vigilance and presents conclusions.

Technological advancements and innovations have led to paradigm shift toward cyber related risks. The revolution on cyber security place organizations at the run to seek for betterand cost-effective cyber solutions for the internet and data infrastructures. The web and the internet that seemed to be the hope to many for digital revolution has turned into a horror to people's data where hackers are now targeting the internet in order to

Keywords: Information Security, Personal Data, Digital Twin, Personally Identifiable Information, Personal Management Information Systems, Data Anomalies.

Production and hosting by NAUSS

* Corresponding Author: Cosmas Knowen
Email: cosmasknowen@gmail.com

doi: 10.26735/ENPO6596

mine personal data from people's online accounts [1]. It's on record the 2017-2019 cyber epidemic, (WannaCry Ransomware attack), that cost large organizations and government agencies huge budgets to mitigate the risks [2], [3]. The value of personal data has reached an extent where some electronic gadget (Oppo, Xiaomi, Huawei phones) manufacturers have installed backdoor programs that continuously spy on and mine data and activities carried out on the gadgets meaning that data is not even safe in PMIS [4]. The significant shift towards and dependency on technology has resulted to increase in cybercrimes where hackers now even target government information systems. The government of Costa Rica was a victim where hackers launched Conti Ransomware and compromised government databases, resulting in a data risks worth $125 million, and no data recovery was possible [5], [6].

II. Literature Review

In the cybersecurity projection calendar, it is recorded that cybercrimes have significantly escalated. This is evident from the 2022 statistics where Heimdal processed, addressed, and resolved over 25 million cybersecurity events. The cyber landscape is worsening each moment, which calls for proactive and resilient security frameworks and infrastructures to reduce the incidence of cyberattacks. It is evident that hackers make billions of dollars daily by trading personal data in black markets with cybercriminals. Similarly, states gather intelligence reports from other states in cyberwar, as exemplified by the Russian state-sponsored cyber-attack against the USA. The Russian government sponsored hackers who successfully launched an APT attack from September 2020 to December 2020 that targeted state, local, tribal, and territorial (SLTT) governments, as well as prominent individuals' online accounts, resulting in a lot of data being exfiltrated and government networks being compromised. [8].

Data processing organizations need to be vigilant and incorporate resilient ways of promoting cyber security [9]. According to Andrew Morrison, the US principle strategic cyber security advisor, he concluded, on his cyber security projection landscape 2022, that "the evolution of cyber risk is generally cumulative. That is, the drivers and opportunities in one era do not replace those of the preceding era. Rather, they expand the horizon"[7], [9]. Comprehensive cyber security mitigation measures must take into consideration the three key objectives (market drivers, key decision makers, and key new opportunities) in three phases [9] as indicated in Table 1.

Cyber space is taking a new course. Cybercrime is taking a new dimension due to the value of critical data and its landscape has become too sophisticated to be predicted[10]. According to The North Atlantic Treaty Organization (NATO) reports, State sponsored attacks are rapidly increasing due to access to intelligence reports and information of other countries [11].

. Selling of personal data in the dark market attracts millions of bitcoins to hackers. Critical confidential information of millions of citizens had spread on the internet and confined their privacy [12]. Cybercrime has now taken geopolitical path like the recent case between Russia and Ukraine whereby Ukraine government paid hackers a huge ransom to perform a counter attack against Russia. Pro-Ukrainian hacktivists performed an attack on the Belarusian railway line in an effort to keep Russian forces out of Ukraine [13].

Kenya is a no exception in the sophistication of the cybercrime landscape, according to the available data and statistics in the Communication Authority of Kenya's intelligence unit, there has been significant increase in cyber-attacks with growing number malware attacks, web application attacks, system misconfiguration and online abuse in government agencies and data processing organization in Kenya. According to the Kenya National Computer Incidence Response Team/ Control Center (KNCIRT/CC), high numbers of attacks were recorded in one quarter (37.1 million cyber threats in the last three months of 2019) which represents an increase of 47.3% from 25.2 million attacks in the previous quarter (July, August and September of 2019) [14]. Developing nations and agencies that

TABLE I
CYBER SECURITY REVOLUTION

Period	Market drivers	Key decision makers	Key opportunities
2005- 2012 (The era of compliance)	In the wake of the internet revolution, organizations focus on new standards for information security. The financial crisis also brought intensified focus on regulatory compliance in the areas of information and technology risk.	• Chief Information Security Officers (CISOs) • IT Risk Officers (ITROs)	• IT risk assessment and strategy • Identification of large scale risks and security program development • Access management • System implementation • ERP security
2013- 2021 (The era of risk)	High-profile cyber-attack across multiple industries stimulated the attention of the media, public, board and executive's management, inspiring many organizations to move beyond compliance to examine the fundamental business cyber risks.	• CISOs and ITROs • Chief Risk Officers (CROs) • Chief information officer (CIOs) • Executives (CEOs, CFOs, CLOs) • Line of business leaders • Board of directors	• Cyber security • Cyber vigilance • Cyber resilience
2022 and beyond (The era of maturity and ubiquity)	Growing maturity across the capabilities and solutions of the past 15 years will drive many organizations to seek better cost efficiency. At the same time, the increasingly ubiquitous connectivity of products and infrastructure will intensify focus on managing risk in the internet of things.	• CISOs, CCIOs, ITROs, CROs, CEOs, CFOs, CLO, LOB leaders, boards • Product management and engineers	• Cyber managed services • Cloud based security solutions • Connected service security

haven't adopted mature intelligent cyber security mechanisms are at a great risk that may originate from cyber-attacks on their critical infrastructures (insurance organizations, government intelligent data, economic organizations, healthcare and education institutions) [15]. This is evident from the previous Ransomware cyber-attack in the Kenya's big supermarket (Naivas systems), whereby critical data was stolen, transaction systems were compromised and money fraud was performed without trace and recovery.

Despite of the Chief Commercial Officer of Naivas highlighting that stolen data did not contain customers personal data (banking details) and immediate actions were taken to contain the attack [16], the information is not sufficient to tell whether the systems are safe in future and whether there has been persistent mining of the customers shopping and transaction history, provided that a malware taken at least 182 days to be detected [9]. Checkpoint software technologies limited cyber security advisory report (checkpoint software 2022 security report) revealed shocking statistics in the Kenya cyber threats landscape with a hiked record of 278 million cyberattacks in the months of October, November, and December 2022. The Kenya National Cybercrime Center (NCC) reported that the cybercrime atmosphere in Kenya was worsening every single time with 200% cybercrime increase in the first quarter of 2022/2023 cyber calendar which is three times of the number of cyberattacks reported in the previous quarter [15]. Eastern and southern Africa nations are at a great risk of cyberattacks with major target to government agencies, insurance organizations, and finance sectors. According to the cyber security projection report of 2021 and 2022, Africa cumulatively experienced a high volume of cyberattacks worldwide. In the light of the unprecedented eruptive rise in cyberattacks organizations need to be vigilant about cyber threats in the digital landscape [17].

Nations all over the world have begun to realize the urgent need to have policy frameworks that deal with the security concerns of personal data; for example the Kenya data protection act 2019 [18] and the EU general data protection regulations act 2018 that include legal provisions about personal data [19]–[21].

The sensitivity of personal data or Personal Identifiable Information (PII) requires the data to be secured during transmission and storage using comprehensive security mechanisms since disclosure will cause direct harm to individuals [22]. According to NIST PII guide, Full name (if uncommon), face, home address, email, ID number, passport number, license plate number, driver's license, fingerprints or handwriting, credit card number, digital identity, date of birth, place of birth, genetic information, phone number, and login or screen name are all examples of personal data that hackers can be interested in mining[23] as illustrated in Figure 1 below.

Personal data should be given the top security priority as we want to attain total security [24]. Protecting personal data will not only useful to the individual, but also will ensure that the employee does not lose its reputation, undergo extreme expenses, provide low productivity and will minimize chances of widening the attacking points to the organization where an individual is working [24], Figure 2 below represents Graphical representation of the relationship between personal data and documents authenticity.

Nodes ‘P’ represents personal data (Full name (if uncommon), face, home address, email, ID number, passport number, license plate number, driver's license, fingerprints or handwriting, credit card number, digital identity, date of birth, place of birth, genetic information, phone number, login(s), SSN, account numbers, etc.), free spaces within the rectangles represent document text other than personal data and the lines connecting p(s) represent additional information needed to connect the texts and the personal data to make a document.

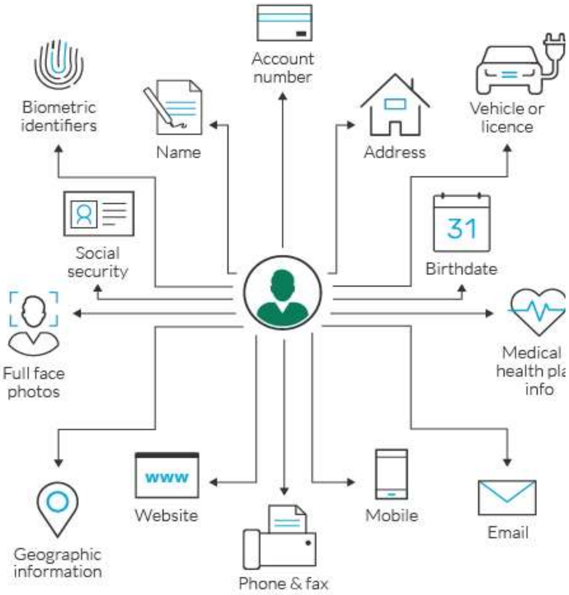

Fig.1. NIST: Personal Identifiable Information (PII) ([24])

Example: a financial bank statement: “P” is the ID number, Account number, Date of birth and physical address. “Free space” can be texts about deductions, gross salary, taxations, etc. the “lines of connection” can represent date of transaction, account balance, employees pin, etc.

The most appropriate way to promote data integrity is deploying multiple security mechanisms, which must be diligently and carefully applied to eliminate unnecessary complexities [25]. A concrete and coherent security system must be objective by ensuring integrity, confidentiality and availability of data [26]. To attain paramount internal and external security, this requires not only by extensive security techniques like hashing and encryption but also needs different information security guidelines and standards that must be adhered to [26].

In the following section, a detailed description of the security threats associated with personal data security will be presented.

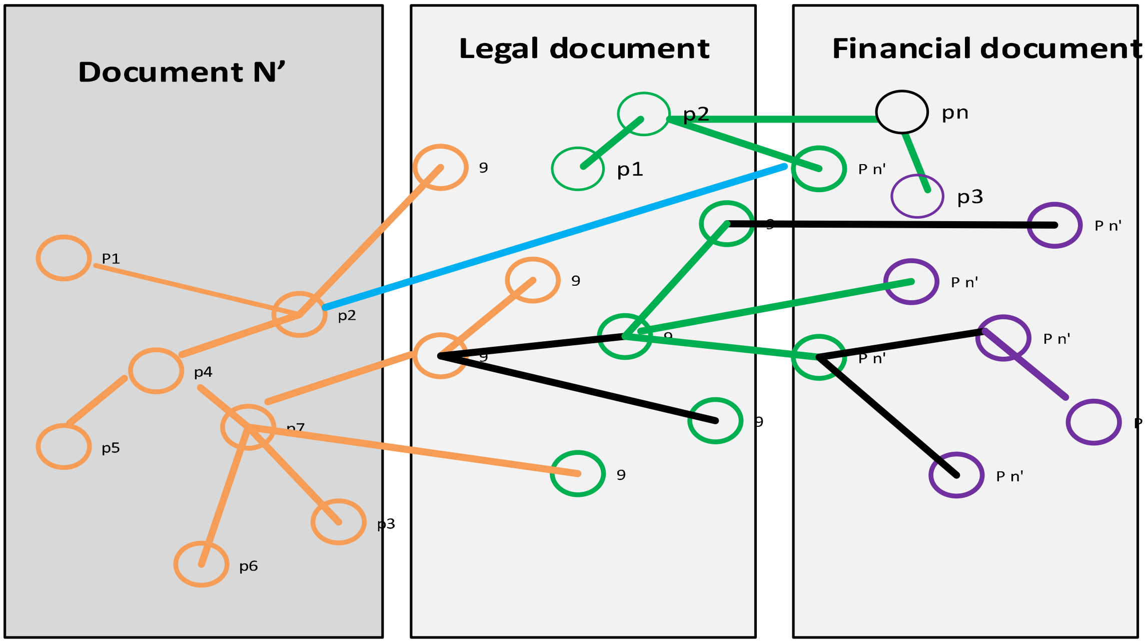

Fig.2. Relationship between personal data and critical records

III. Security Threats Associated With Personal Data Security

In the span of a few months since its inception in the summer of 2022, the "dandruff attack" has evolved rapidly from a basic mailing list to a sophisticated system with advanced methods of goal analysis. As of now, there are several generations of this attack that can be identified. The attackers have developed and refined their strategies over time to make the attacks more effective and harder to detect.

The preservation of personal data security is paramount in today's interconnected digital landscape. However, this section delves into the various security threats that pose significant risks to the confidentiality, integrity, and availability of personal information. It explores the potential vulnerabilities that malicious actors exploit to compromise data security, such as ransomware attacks, advanced persistence attacks threats, phishing attacks, unintentional data exposure, and insider threats.. Understanding these security threats is essential for implementing robust protective measures and developing effective strategies to safeguard personal data from unauthorized access or misuse.

1) Ransomware attacks

Ransomware attack is one of the greatest threats to personal data, once an attacker gains access to the data, encrypts the data on the victim’s computer and in return asks for payment in order to decrypt the data [27]. It is reported that in the first half of the year 2021, $590 million ransomware related activities were performed which reflects an increase from $416 million cases in the year 2020 [28].

According to [29] analytics, 2 million files are infected daily due to ransomware attack. In addition, 37% of global large scale organizations reported ransomware attack in the year 2021 [28] . According to cyber threat landscape of 2022, companies are suffering from ransomware extortion since 80% of the companies which paid to retrieve their encrypted files experienced another attack after a short period [9]. Today ransomware is linked to geopolitical cold wars. Superpowers nations hires hackers to direct attacks to opposing superpower intelligence systems [30]. According to The Australian Cyber Security Center (ACSC), Russia sponsored ransomware attacks targeted the Australian critical infrastructure entities and sectors, including: healthcare facilities, financial markets, higher education organizations, research entities, and the energy sectors [31]. On the same context, the United Kingdom's National Cyber Security Centre (NCSC-UK) reported that ransomware attacks targeted the top UK sectors including the legal, businesses, charity centers, local governments and the healthcare sectors [32].

According to the US Treasury report of 2020, 78.5% of US ransomware attacks targeted personal data that are for financial identity [33]. Victims suffered from direct extortion as they had to pay for their encrypted data to be decrypted. Some personal data were used by attackers to fake credit cards and perform pseudo- transaction (money laundering) from the victim's bank account as illustrated in Figure 3. [33]. Figure 3 below highlights that protection of personal data is matter that should be given top priority. The figure represents a successful money laundry incident from a secure banking system. Although the bank system is protected, yet personal data (credit card identity numbers) is vulnerable to attack. Another research by a great cyber security researcher Andrew Morrison indicates that 42% of companies which lost their data have never recovered 95% of personal data even after payment [9].

2) Advanced persistence threats (APTs).

APTs are cyberattack activities where a threat actor establishes a sustained presence inside a compromised network in order to steal critical information on a regular basis [34]. According to the US Treasury FinCEN Advisory special report vol. 42, no. c, pp. 1–8, 2020, APT cyberthreats must constantly surpass the increasing sophistication of standard security controls in order to avoid detection [35] during the full APT attack life cycle (which could run for several years). The sophisticated attack techniques used by APT groups make it far more challenging to stop this cyber threat [17], [34] . For APT attack to be successful, an attacker needs to employ a number of systematic processes persistently known as APT attack life cycle as illustrated in figure 4 below.

Advanced persistent threat (APT) attacks are

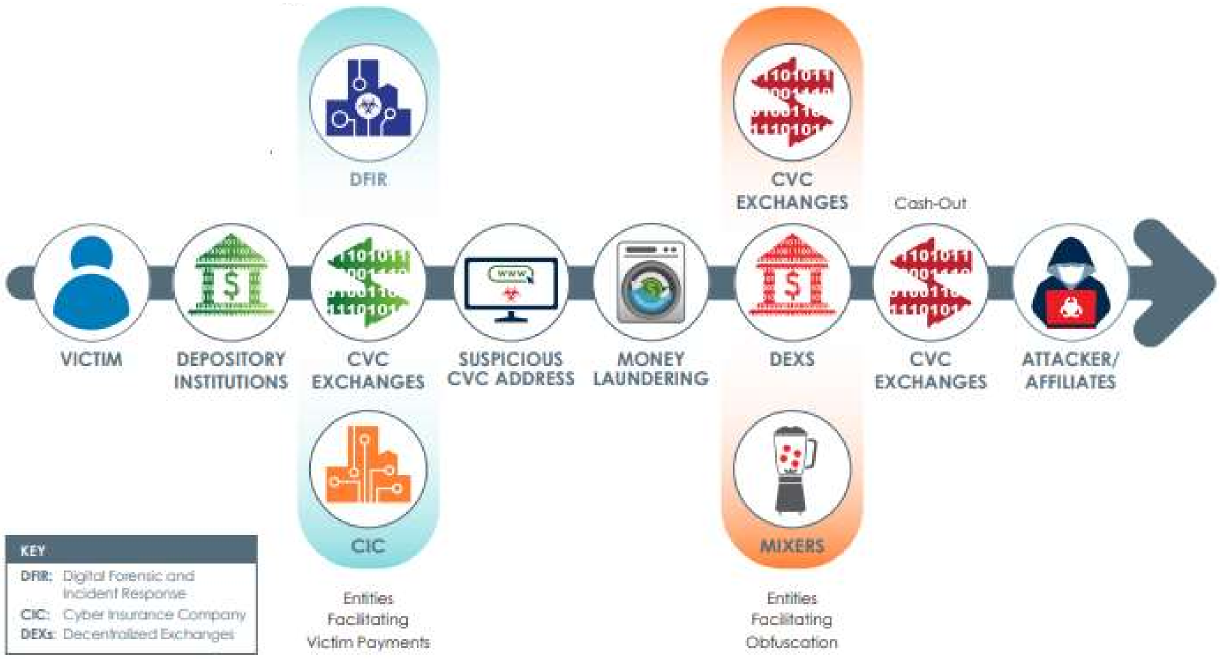
DFIR
CVC EXCHANGES
Cash-Out
VICTIM
DEPOSITORY INSTITUTIONS
CVC EXCHANGES
SUSPICIOUS CVC ADDRESS
MONEY LAUNDERING
DEXS
CVC EXCHANGES
ATTACKER/ AFFILIATES
CIC
MIXERS
Entities Facilitating Victim Payments
Entities Facilitating Obfuscation
KEY
DFIR: Digital Forensic and Incident Response
CIC: Cyber Insurance Company
DEXs: Decentralized Exchanges

Fig.3. Ransomware money laundry incidence in a secure banking system

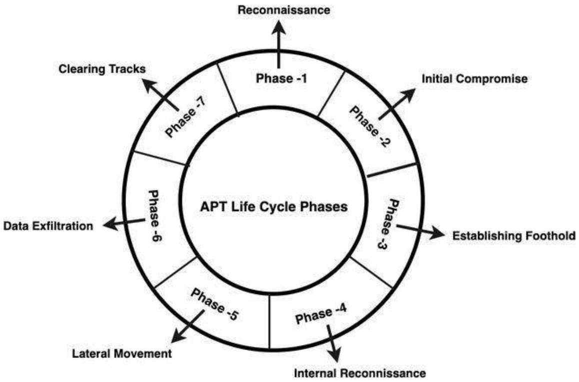

Fig.4. APT attack cycle

reportedly used by attackers to target important government infrastructures, financial institutions, legal entities, and huge organizations. While looking for sensitive internal information (personal data), intellectual property, and privileged credentials (administrator passwords and other credentials), APT is frequently utilized by the perpetrators. Governments and organizations also employ APT for espionage purposes (geopolitical advantage) in order to seek out information on political, military, and economic affairs as well as on the manufacturing of goods and marketing plans from other nations. [36], [37].

Some of the outstanding APT cyber-espionage are; the Chinese APT cyber espionage operation targeting US, Europe and Asia organizations to mine business and prominent peoples sensitive information is one of the top government sponsored APT espionage attack [38]. Hong Kong is also in the count of the victims of Chinese APT espionage whereby a persistent access was gained to the countries communication network, whereby DazzleSpy backdoor malware payload was launched into the pro-democracy radio station and critical personal information was stolen [39] . On the same note, the Twisted panda APT espionage where by the Chines government targeted the Russian defense research institutions [40]. The APT cyber-espionage landscape can't be complete without mentioning the BackTech cyber-espionage APT group that was sponsored by the Chinese government to spy and compromise with the Japan and Taiwan defense technology, media, and communication sectors [39].

On the top the landscape is the Russian state-sponsored APT attack targeting the US and the international critical infrastructure organizations with the aim of sabotaging and compromised with critical intelligence and prominent people personal data [8] .The Russian state sponsored APT attack is said to have been effectively planned and the attackers employed the full cycle of cyber kill chain [30]

Other threats and risks

3) Phishing attack

Phishing is the practice of a bad actor sending fraudulent message that looks to be from a trustworthy source, such as a bank or business, or from a person using the incorrect phone number. Phishing attacks can be sent via text, email, or social media. Usually, the intention is to install malware or coerce the victim into giving up personal information in order to steal information.

4) Unintentional data Exposure

A larger percentage of data breaches are brought on by the careless or unintentional release of sensitive data rather than a deliberate attack. Employees frequently share, allow access to, mishandle, lose, or share valuable data either accidentally or because they are unaware of security procedures.

Employee education as well as other methods like data loss prevention (DLP) technology and improved access controls can be used to solve this serious issue.

5) Insider threats

Employees who knowingly or unknowingly jeopardize the confidentiality of an organization's data are known as insider threats.

Insider risks are categorized into three i.e. Non-malicious insiders are users who may hurt others unintentionally, carelessly, or because they are not aware of security precautions. Insiders that intentionally try to steal data or hurt the company for their own gain are known as malicious insiders.

Insiders who have been hacked are people who are unaware that an outside attacker has obtained access to their accounts or credentials. The attacker can then carry out nefarious deeds while posing as a normal user.

IV. Mechanisms and Strategies for Enforcing and Enhancing Cybersecurity for Insurance Organizations

A. Integrating Digital Twin Capability for Cyber Security enhancement

Digital twin is a virtual representation of an object or system that spans its lifecycle, is updated from real-time data, and combines simulation, machine learning, and reasoning to aid decision-making. Digital twin technology connects real-world assets with real-world data to improve visualization. It is a potent data-driven technology [8].

Digital twin facilitates an accurate virtual representation of a physical object. The object being analyzed has a number of sensors attached to the critical working components. These sensors generate information about several facets of the functionality of the physical objects. After that, a processing system transfers this information and applies it to the digital copy. The virtual model can be used to run simulations, investigate performance problems, and produce potential upgrades, all with the aim of producing insightful data that can then be applied back to the original physical device.

Cross-functional teams can design, develop, test, deploy, and run complex systems in a collaborative, immersive manner using digital twins. With the help of digital twin's robust algorithms, businesses may synthesize historical data to comprehend the past, see the present, and anticipate difficulties in the future. Using sales and marketing insights, analysis, 3D visualization, modeling, and prediction, they assist in decision-making.

According to Australia 2020 defense strategic report, organization were advised to invest on intelligence and data driven technologies to address their cyber situation [12]. Today attackers have been enhancing their skills in that almost all attacks are artificial intelligence (AI) driven. In order for data organizations to be on the same page they should invest on AI and data driven security tools for the modern escalating cyber threats [12].

As we usher in the metaverse and fifth industrial revolution (5IR), the key secret is data about data to service data. Digital twin being a data driven technology it will be an effective tool to mitigate cyber security risks and thereby guaranteeing in depth defense [41]. Digital twin is expected to be an optimal way to promote cyber security. Digital twin will increase security scope visibility starting from anomaly detection, intrusion detection, identity vigilance, and prevention hence promote an active cyber defense posture.

The real time data analytics and behavior mining nature of digital twin gives it an upper hand for the implementation of a transformational and a comprehensive security framework. According to Krigsman [42], Kurt the CISO of Siemens USA argues that they have seen a significant cyber opportunity in the application real-time data, passive data, and digital twins, in threat detection from the internet, and data security. There is a significant opportunity to leverage digital twin in combating cyber related issues. Digital twin offers a simulated platform for discrepancy and anomaly detection hence reliable detection of an attack [43]. Digital twin will enhance visibility of cyber-attacks as follow;

i. Indicators of Compromise (IOC) search known-bad signs of compromise from a wide range of searches. Search for those signs in the network and host indicators from a variety of sources. Analyze outcomes for additional signs of malevolent behavior to eliminate the false positives.

ii. Pattern analysis - Examine data to find recurring patterns that may be caused by automated systems (such as malware or scripts) or regular human threat actor activity. Eliminate the regular activity data and analyze the remaining data to spot any unusual or harmful behavior [44]

iii. Anomaly Detection - Analyze the gathered artifacts to find errors based on the team's understanding of and experience with system administration. It reviews unique values for different datasets and, as necessary, conduct research on related data to look for aberrant behavior that might be a sign of threat actor activity [44], [45].

The monitoring, simulation, optimization and prediction of cyber outcome are among the potential ways digital twin will enhance security posture. The virtual replica of the defense mechanism will significantly assure additional security to the data, system and users [46]. The paradigm shift in attack mechanisms has resulted in further exposure of data assets. Hackers have upgraded their use of AI and data driven techniques to perform their attack hence they can penetrate easily even in protected systems, thus there is a need to upgrade the security postures [41]. Digital twin will enhance the visibility of not only data items but also behavior of the personal data processing. In a case where anomaly data behavior is detected significant out bound security protocols will disable outflow of data and any instances. The inbound security protocols will conduct signature filtration and separate the data from malicious signatures. Cryptography algorithms will be employed during data exchange to ensure that that on transit is encrypted.

V. Technical and Legal Frameworks for Safeguarding Personal Data

Scholars and cyber security organizations and agencies have engaged in extensive research to recommend for effective ways to enhance personal data security. ENSA under contract number ENISA P/18/12/TCD Lot 2 established an advisory consortium committee that was tasked with the responsibility to come up with recommendation report about "the cryptographic measures for security personal data" [47]. The report significantly highlighted the cryptographic techniques applied to safeguard sensitive/personal data. In addition to the technical cryptographic recommendation ENSA emphasized that legal provisions must also parallel applied[18]. The National Institute of Standards and Technology (NIST) on its special publication number 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" has highlighted out provisions for personal data security. A framework for protecting PII should highlight not only legal policies and procedures but also should incorporate technical mechanisms [23].

A. Legal frameworks review

Legal frameworks play a vital role in highlighting the rules and regulations for handling cyber related crimes. In the cyber projection statistics, it's highlighted that in the present cyber security landscape its recorded that there has been a significant increase in cyber insider threats. Employees are said to be acting maliciously against employer once they quit their jobs due to unfair work expectations [13]. Toby Lewis the head of threat analysis at DarkTace affirmed that, Internal employees have access to information systems and in one way or the other they always monitor the system behaviors, there is a likelihood once the employees quite the jobs they might use their previous system credentials to perform malicious activities [48].There is a trend where criminal groups recruited insiders by offering the large amount of money to enable them gain access to critical/personal information in the organizations databases [49], [50]. The above scenarios indicate that there is an essence to incorporate legal frameworks to enable conviction and judging cybercrime related issues both insider and external.

Based on this, Kenya makes reference to legal frameworks (treaties, statues, parliamentary acts and by laws) have been promulgated in Kenya and internally to protect personal data.

1) The Data Protection Act 2019 of Kenya, part IV, section 30 has highlighted out the principles for safeguarding personal data [15].

2) The Kenya data protection bill 2018, part II clause 23, highlights out the legal conviction procedure for whoever found with an offence of interference with personal data [21].

3) The general data protection regulation (GDPR 2018) chapter 4, article 32 has reinforced a provision for the protection of personal data (both in context and substance) and extended the responsibility to data processors(both private, public and individuals) to give personal data a top priority in the security pyramid [51].

4) The 2010, National Institute of Standards and Tech-

nology (NIST) "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" [23]

VI. Technical Mechanisms for the Protection of Personal Data

Technical mechanisms provide direct data security related concerns. Researchers have found out that personal data is more exposed and vulnerable to attacks. The research conquers with UpGuard technologies on their remarks about an optimal, comprehensive personal data security the following should be applied.; cryptography, Pseudonymization and anonymization, Hashing and critical data de-identification, Typosquating protection, data masking and ethical walls.

1) Pseudonymization techniques

Pseudonymization is a data protection technique which aims at protecting the identity of individuals by substituting their identifiers by pseudonyms [52], [53].

Following the adoption of the General Data Protection Regulation (GDPR), Article 4(5) Employment of Pseudonymization techniques to hide personal data both in the databases and in the user's portable devices has gained additional attention and relevance by cyber security organization and organizations that deal with personal data.

According to the European Data Protection Board report of 2021, Pseudonymization is only one possible technique and must be combined with a thorough security risk assessment for the protection of personal data. Data controllers and processors should engage in data pseudonymization, based on a security and data protection risk assessment and taking due account of the overall context and characteristics of personal data processing. This may also comprise methods for data subjects to pseudonymize personal data on their side (e.g. before delivering data to the controller/processor) to increase control of their own personal data [53].

Security concerns more so to personally identifiable information (personal data) and maintaining the primary significant value of personal data should be given top priority [54]. Personal data such as; name of the person, age of the person, account number, social security numbers, biometric data, and IP addresses should be hidden/di-identified from the public view since their exposure to the public might result to security risks [52]. The regular interaction and access to personal data subject the data to extensive vulnerabilities which might result to cyber risks, the portability of the personal data even within personal devices like; mobile phones and flash drives should be comprehensive in order to restore the confidentiality, integrity and access of such data.

2) Data masking and ethical walls

Through the use of data masking, a decoy copy of your organizational data that you can use for software testing, training, and other activities that don't require the real thing. When a functional substitute is required, the aim is to secure data while offering it. An ethical wall is a screening tool that safeguards users from a conflict of interest by prohibiting or restricting the exposure of information to specific workers who represent other clients or interests that might conflict with or benefit from the information [55] hence the critical data is di-identified.

While changing the values, data masking preserves the data's type. Encryption, character rearranging, and character or word substitution are just a few methods for altering data. Regardless of the method you select, the values must be altered in a way that prevents them from being backwards-engineered [56].

3) Cryptographic techniques (Encryption of Data)

The process of transforming data from a readable format (plaintext) to an unintelligible encoded format (ciphertext) is known as data encryption. The data cannot be read or processed until the encrypted data has been decrypted using the decryption key [56].

The sender and recipient each have their own keys, which are combined to conduct the encryption operation in public-key cryptography systems. This eliminates the need to share the decryption key [57]. This is more secure by nature.

Hackers may be prevented from gaining access to sensitive data using data encryption. The majority of security plans depend on it, and many compliance standards related to protection of personal data require the integration of such techniques.

The technical measures when adopted independently they only address a niche problem, but joint adoption solves only the technical related issues of data protection. Adoption of technical and legal frameworks for the protection of personal data independently does not provide the comprehensiveness and the robustness required for the personal data security. Based on the literature findings with significance reference to the rational choice theory the cyber atmosphere for the personal data is compromised and gets more sophisticated every time [58], [59], hence need for insurance organization to adopt cyber vigilance measures as discussed below.

VII. Cyber Vigilance

Entails the integration of threat data, IT data and critical data with context-rich intelligence to proactively detect and manage cyber threats and respond more effectively to cyber incidences. It includes: advanced threat readiness and preparation, cyber risk analytics, SOC and threat intelligence [8].

Cyber vigilance through data leak detection, privilege control and monitoring, credentials exposure detection, will further make security posture more comprehensive and strong[60]

Cyber intelligence is a systematic process as highlighted below.

i. Credentials exposure detection

Credential exposure is state or a situation where individual's credentials (username, passwords or SSN are revealed either accidentally or intentionally. Credentials exposure detection is the process or a technique at which a response is given automatically in a case where credentials have been exposed[61]. The data breach investigation report (DBIR) indicates that 67% of data breach incidences in 2020 were as a result of credentials theft [62].

Attivo Networks (2021), "Improving cyber hygiene by remediating exposed credentials" study was done concerning the log in credentials exposure and a conclusion was made that automated system for credentials exposure detection is the only strategy to remediate the issue.

Further experimental study was conducted using threat path solution and it was found that 80% of network users use a common password [63].

ii. Privilege Control and Management (PCM)

Privilege control refers to cybersecurity techniques and tools used to impose control over elevated ("privileged") access and permissions for users, accounts, systems, and processes throughout an IT environment [64]. Privilege control management will ensure that stolen credentials cannot be used to access onto the system [65].

PCM had three pillars of effectiveness (visibility, knowledge and action) [66], PCM strategies enables reporting of credentials exposure hence visibility of point of attack and a coherent action is taken for disabling access [67]. PCM allow specific access rights to be given to specific users while barring other users from accessing the services. ManageEngine proposed a ranking pyramid framework for management of personal data security, where at the top is the "most privileged users" who play critical risky role in cyber vigilance of the organization and process and control personal data, at the middle "power users" and at the bottom "the standard users" [68] this is illustrated in figure 5. Microsoft reported that

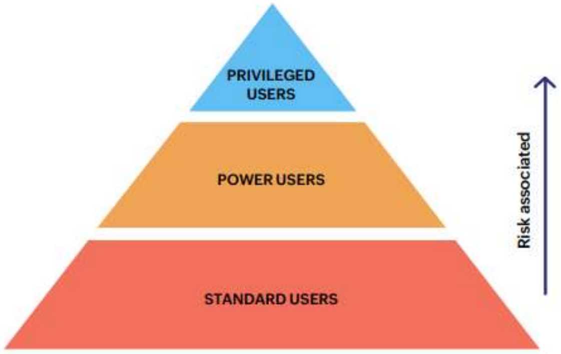

Fig.5. pyramid of data handlers' risks

in 2014, 80% of reported incidences of personal data mutilation was due to credentials exposure and malicious people gained access to individuals computers stole and mutilated the data [67].

PCM is made even more possible and effective through the integration of machine learning (ML), Artificial intelligence(AI), data mining and Digital twin [44], [45] hence an automated method for privilege control and management [69]. ML enable an automated supervised learning that learn from users behaviors and once a suspicious users are detected their privileges are systematically suppressed [44].

iii. Data anomaly and outlier detection

ML enhances visibility of malicious activities by the perpetrators, learning the users behavior on a database and enable detection of anomaly activities [44] .

IV. Data Leak Detection and Prevention

A. Theoretical review

The study is strongly grounded on the following two theories; Cloud Access Security Broker (CASB) and the rational choice theory

1) Cloud Access Security Broker (CASB) model.

Cloud Access Security Broker (CASB) is placed between cloud service users and cloud applications of cloud computing to ensure security enforcement of cloud-based software CASB is also used to manage the dimensionality, heterogeneity, and ambiguity associated with cloud services [70]. Cloud Access Security Broker (CASB) is a framework for securing data end to end. Unlike other security models and frameworks that focus on SaaS, CASB is a comprehensive tool for both IaaS, SaaS and private cloud applications [71]. It was predicted that 85% organizations offering cloud service were to rely on CASB by 2020 for implementation of security postures which is an increase from 5% in 2015. Giant cloud service companies like Microsoft, sales force, and Amazon Web Services (AWS) are among the organizations that have adopted CASB [72].

Despite the significant contribution the model has made into the cloud security it has failed to address the issue of in-house security policies and postures integration. Streamlined dynamic security posture that are interdependent will make it easy for the organization to conduct security analytics and streamline with the policy frameworks of the organizations [73]. CASB model has addressed data security issues in the cloud [74] but it fails to address the security issues associated with data exchange process outside the cloud.

The model sets an architectural base outlay of defense in-depth that will be incorporated in further studies to come up with a comprehensive and dynamic model that address both cloud issues, internet and offline personal data processing issues.

2) Rational choice theory.

Human being are assumed to be rational in nature hence their utilitarian believe such as financial gain even from deviant actions [75]. Rational choice theory gives presumption that people are driven by a desire for financial gain and opportunities of making profit [76]. The theory converge all the human actions towards the psychological force [77]. Criminal decision making is a rational process, if the cost and risk to be taken is low compared to profit benefit out of crime then a person will commit a crime [78], [79].

Criminal behavior in cyber space are inevitably based on criticality of data and the comprehensiveness of the available security mechanisms [80]. Rational choice theory in cyber criminology asserts that if there are high chances of difficulty in accessing a system and high chances of being caught will discourage the hackers from engaging in deviant actions [81].

The theory sets a strong foundation for cyber legal frameworks for intra-cybercrime and extends it further on the need of strong security mechanisms. The theory sets a base for the study by trying to advocate for incorporation of strong security measures that makes it difficult for attackers to access critical data (personal data).

B. Empirical review

Irwin attesed that cyber predictions are difficult but emphasized on cyber insurance policies popularity and comprehensiveness in combating cybercrimes [82]. He failed to clarify on how cyber insurance will enhance cyber threat prediction.

Denise on the Majesco blog highlighted that data driven opportunities Insurance companies are incorporating metadata driven design approach to cope with huge data velocities. The study revealed that investment on AI [83], and metadata driven technologies (data warehousing, data mining, BI, customer relationship management, enterprise application integration, and knowledge management) will enable insurance companies to reduce time needed to implement new data sources and enhance automation [84]. The study findings also revealed that it will be easy for insurance companies to handle large customers effectively.

The study advocates for technology to accommodate more users in insurance companies but fails to address the security issues and concerns on the customers data. The study has not tackled on how metadata technology can promote data security of the customers data.

According to the research that was conducted by Veselovská and Jančíková in 2018, on new trends in insurance information technology security, using qualitative data, synthesis and comparison to identify technological innovations in insurance companies' information systems. The research findings revealed that Insurance information technology is embracing AI, robotics, block chain for fast data processing and to improve customers' experience. Also it was revealed that cyber security is a major concern that insurance companies should look from both the service provide perspective and the client side perspective [85].

Despite the study's attempt to address the security metrics associate with insurance company's insurance information systems there are no clarifications on security frameworks for guaranteeing personal data safety.

VIII. Conclusion

In conclusion from the study findings and the literature cited truly the cybercrime landscape is getting worse day by day. Personal data have a unique characteristic of individual identification of specific people hence they are not only exposed to direct threats but also to indirect threats since they can be used to fake actions and activities. The personal data value has reached another extent where they are considered to be valuable assets to hackers who get access to them either through extra filtration or purchase from the dark web market like SSNDOB. There is an urgent need to refocus on the data security models and prioritize personal data security more so in the insurance companies that are tasked with the responsibility to process personal data min large quantity. There is need to adopt intelligence mechanism in the data protection frameworks in the insurance companies to embrace robustness and comprehensiveness in the personal data security.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] A. Paro, “Hackers Leaked 22 Million Records on the Dark Web in 2020 - Security Boulevard,” securityboulevard blog, 2021. https://securityboulevard.com/2021/01/hackers-leaked-22-million-records-on-the-dark-web-in-2020/ (accessed Jul. 16, 2022).

[2] Kaspersky, “Ransomware WannaCry: All you need to know,” Kaspersky, 2017. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (accessed Jul. 16, 2022).

[3] NCCIC, “What is WannaCry?,” National Cybersecurity and Communications Integration Center. 2020. [Online]. Available: https://www.avast.com/c-wannacry

[4] BBC News, “Lithuania urges people to throw away Chinese phones - BBC News,” 2021. https://www.bbc.com/news/technology-58652249 (accessed Jul. 16, 2022).

[5] C. Rosch, “A massive cyberattack in Costa Rica leaves citizens hurting - Rest of World,” Rest of worlds news , Jun. 01, 2022. https://restofworld.org/2022/cyberattack-costa-rica-citizens-hurting/ (accessed Jul. 16, 2022).

[6] B. Crothers, “Conti Ransomware Group Attacks Costa Rica, U.S. Responds With $15 Million Bounty | Venafi,” venafi. Inc, May 2022. https://www.venafi.com/blog/conti-ransomware-group-attacks-costa-rica-us-responds-15-million-bounty (accessed Jul. 16, 2022).

[7] Heimdal Security, “Threat Report 2023: A 2022 Review of the Cyber-Threat Landscape and Prediction for 2023,” 2023.

[8] CISA, FBI, and NSA, “Understanding and Mitigating Russian State- Sponsored Cyber Threats to U . S . Critical Infrastructure,” Jt. Cyber Secur. Advis., 2022.

[9] A. Morrison, “Cyber Security Landscape 2022,” no. February, 2022.

[10] P. O. Magutu, G. M. Ondimu, and C. J. Ipu, “Effects of Cybercrime on State Security : Types , Impact and Mitigations with the Fiber Optic Deployment in Kenya,” J. Inf. assuarence cyber secuirty, vol. 2011, no. 1, p. 21, 2017, doi: 10.5171/2011.618585.

[11] A. Ertan, K. Floyd, P. Pernik, and T. Stevens, Cyber Threats and NATO 2030: Horizon Scanning and Analysis. 2020. [Online]. Available: www.ccdcoe.org

[12] C. Cubbage, D. Matrai, and S. Babi, “Invest in intelligency now to prepare Australia’s utilities for the future,” Cyber risk Leaders: magazine for secuirty and technology professionals, no. 2, p. 52, 2020.

[13] L. Irwin, “9 cyber security predictions for 2022 - IT Governance UK Blog,” IT Governance Blog, Feb. 15, 2022. https://www.itgovernance.co.uk/blog/9-cyber-security-predictions-for-2022 (accessed Jul. 20, 2022).

[14] Business Daily, “Kenya cyber attacks up by half to 37m in one quarter - ,” Business Daily, 2020. https://www.businessdailyafrica.com/bd/economy/kenya-cyber-attacks-up-by-half-to-37m-in-one-quarter-2285138 (accessed May 14, 2023).

[15] Business Today, “Kenya Records 278 Million Cyberattacks In 3 Just Months,” Business Today, Feb. 07, 2023. https://businesstoday.co.ke/kenya-records-278-million-cyberattacks-in-3-just-months/ (accessed May 14, 2023).

[16] W. Musalia, “Ransomware: Naivas Supermarket’s System Hacked, Data Stolen - Tuko.co.ke,” Tuko news, Apr. 24, 2023. https://www.tuko.co.ke/business-economy/technology/503268-ransomware-naivas-supermarkets-system-hacked-data-stolen/ (accessed May 14, 2023).

[17] Mandiant Investigator, “Global Perspectives on Threat Intelligence Report | Mandiant,” Mandiant, 2023. https://www.mandiant.com/resources/reports/global-perspectives-on-threat-intelligence (accessed May 05, 2023).

[18] European information commisisioners office, “Guide to the General Data Protection Regulation (GDPR),” 2021.

[19] V. C. Kanji and R. Njenga, “The Kenya Data Protection Act 2019,” A.B. Patel Patel Advocates, vol. 37, no. 4, pp. 161–163, 2021, [Online]. Available: https://abpateladvocates.com/data_protection_act_2019_kenya.php

[20] Govornment of Kenya (GoK), The Data Protection Act 2019, vol. 41, no. 4. 2019, pp. 145–147. [Online]. Available: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

[21] Government of Kenya (GoK), “the Data Protection Bill, 2018 Arrangement of Clauses Part Ii-Objects and Principles of Protection of Personal Data,” pp. 309–331, 2018, [Online]. Available: http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf

[22] Imperva softwares, “What is Personally Identifiable Information; PII Data Security ,” Imperva, 2021. https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/ (accessed Jul. 27, 2022).

[23] E. Mccallister, K. Scarfone, and T. Grance, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Recommendations of the National Institute of Standards and Technology,” Comput. Secur. Div. Inf. Technol. Lab. Natl. Inst. Stand. Technol., vol. 800, no. 122, p. 59, 2010.

[24] Computer Solution East, “Protecting Your Data Is the Top Priority for Professional Services! We Get It,” Computer Solution East, Aug. 26, 2020. https://www.computersolutionseast.com/blog/managed-security-services/protecting-your-data-is-the-top-priority-for-professional-services-we-get-it/ (accessed Jul. 27, 2022).

[25] S. D. Dorairaj and T. Kaliannan, “An Adaptive Multilevel Security Framework for the Data Stored in Cloud Environment,” Sci. World J., vol. 2015, 2015, doi: 10.1155/2015/601017.

[26] M. Qingxiong, A. C. Johnston, and J. M. Pearson, “Information security management objectives and practices: A parsimonious framework,” Inf. Manag. Comput. Secur., vol. 16, no. 3, pp. 251–270, 2008, doi: 10.1108/09685220810893207.

[27] S. Gittlen, “The Complete Guide to Ransomware,” 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/Guide-to-preventing-phishing-and-ransomware

[28] S. M. Kerner, “Ransomware Trends, Statistics and Facts in 2022,” TechTarget, Feb. 2022. https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts (accessed Jul. 18, 2022).

[29] Virustotal, “Ransomware i a global context,” Virustotal Report, no. October. 2021.

[30] FBI, CISA, NSA, ACSC, and NCSC-UK, “2021 Trends Show Increased Globalized Threat of Ransomware,” 2022.

[31] McGrathNicol Technology, “Ransomware epidemic continues to rise in 2022 The Rise in Ransomware Attacks,” 2022.

[32] S. Alder, “CISA, FBI, NSA Warn of Increased Threat of Ransomware Attacks on Critical Infrastructure,” HIPAA J. , vol. 3, no. 2, Feb. 2022, Accessed: Jul. 19, 2022. [Online]. Available: https://www.hipaajournal.com/cisa-fbi-nsa-warn-of-increased-threat-of-ransomware-attacks-on-critical-infrastructure/

[33] US Treasury, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” FinCen Advis., vol. 42, no. c, pp. 1–8, 2020.

[34] E. Kost, “Advanced Persistent Threat (APT) | A Definition by UpGuard,” UpGuard, 2022. https://www.upguard.com/glossary/advanced-persistent-threat-apt (accessed May 05, 2023).

[35] Financial Crimes Enforcement Network (FinCEN), “Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic Financial Red Flag Indicators of Cybercrime and Cyber-Enabled Crime Exploiting COVID-19,” FinCen Advis., vol. 1, no. FIN-2020-A005, pp. 1–8, 2020.

[36] Iiviu Arsena, “Anti-malware research:PT Hackers for Hire Used for Industrial Espionage,” Bitdefender anti-malware research, Aug. 20, 2020. https://www.bitdefender.com/blog/labs/apt-hackers-for-hire-used-for-industrial-espionage/ (accessed Jul. 20, 2022).

[37] Bitdefender, “More Evidence of APT Hackers-for-Hire Used for Industrial Espionage,” 2020. [Online]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

[38] T. Keary, “Experts discover a Chinese-APT cyber espionage operation targeting US organizations | VentureBeat,” VentureBeat technologies , Mar. 03, 2022. https://venturebeat.com/2022/05/03/experts-discover-chinese-cyber-espionage-operation/ (accessed Jul. 20, 2022).

[39] C. Kime, “Advernced Persistant threat (APT) attack and prevention.” esecurity planet, p. 10, 2022.

[40] A. Ribeiro, “Chinese APT espionage operation Twisted Panda targets Russia’s state-owned defense institutes - Industrial Cyber,” Industrial Cyber News, May 23, 2022. https://industrialcyber.co/vulnerabilities/chinese-apt-espionage-operation-twisted-panda-targets-russias-state-owned-defense-institutes/ (accessed Jul. 20, 2022).

[41] D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal, and H. Janicke, “Digital Twins and Cyber Security - solution or challenge?,” 6th South-East Eur. Des. Autom. Comput. Eng. Comput. Networks Soc. Media Conf. SEEDA-CECNSM 2021, no. September, 2021, doi: 10.1109/SEEDA-CECNSM53056.2021.9566277.

[42] M. Krigsman, “Improve Security with Real-Time Data and Digital Twins | Redis,” The data economy podcast , Redis, 2021. Accessed: Jul. 19, 2022. [Online]. Available: https://redis.com/the-data-economy-podcast/episode-5/

[43] Siemens USA Technologies, “Trends and innovation in cyber security: AI, quantum computing and digital twins. ,” Ingenuity by Siemens, Jul. 05, 2022. https://ingenuity.siemens.com/2022/07/ai-quantum-computing-and-digital-twins/ (accessed Jul. 19, 2022).

[44] C. K. Wee and R. Nayak, “A novel machine learning approach for database exploitation detection and privilege control,” J. Inf. Telecommun., vol. 3, no. 3, pp. 308–325, 2019, doi: 10.1080/24751839.2019.1570454.

[45] A. Outchakoucht, A. A. El Kalam, H. Es-Samaali, and S. Benhadou, “Machine learning based access control framework for the internet of things,” Int. J. Adv. Comput. Sci. Appl., no. 2, pp. 331–340, 2020, doi: 10.14569/ijacsa.2020.0110243.

[46] K. Alshammari, T. Beach, and Y. Rezgui, “Cybersecurity

for digital twins in the built environment: Current research and future directions," J. Inf. Technol. Constr., vol. 26, pp. 159–173, 2021, doi: 10.36680/j.itcon.2021.010.

[47] European Union Agency for Network and Information Security (ENISA), "Recommended cryptographic measures for securing personal data," 2013.

[48] T. Lewis, "The future of cyber security: 2022 predictions from Darktrace - Darktrace Blog," Darktrace Holdings Limited, Jan. 07, 2022. https://darktrace.com/blog/the-future-of-cyber-security-2022-predictions-from-darktrace (accessed Jul. 20, 2022).

[49] S. Poremba, "Ransomware Gangs are Recruiting Your Employees - Security Boulevard," Security Boulevard , Jan. 31, 2022. https://securityboulevard.com/2022/01/ransomware-gangs-are-recruiting-your-employees/ (accessed Jul. 20, 2022).

[50] W. Shannon, "The Great Resignation will drive cyber attacks in 2022," Security Brief Australia, Dec. 17, 2021. https://securitybrief.com.au/story/the-great-resignation-will-drive-cyber-attacks-in-2022 (accessed Jul. 20, 2022).

[51] The European Parliament And The Council Of The European Union, "Regulation (Eu) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement," Off. J. Eur. Union, vol. 61, 2018.

[52] K. Limniotis and M. Hansen, Recommendations on shaping technology according to GDPR provisions : an overview on data pseudonymisation., 1st ed., no. November. European Union Agency for Network and Information Security, 2018. doi: 10.2824/74954.

[53] ENISA, Data Pseudonymisation: Advanced Techniques and Use Cases, no. JANUARY. 2021. [Online]. Available: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

[54] P. Štarchoň and T. Pikulík, "GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones," Procedia Comput. Sci., vol. 151, no. April, pp. 303–312, 2019, doi: 10.1016/j.procs.2019.04.043.

[55] Thomson Reuters, "Ethical wall | Practical Law," Thomson Reuters Practical Law, 2022. https://uk.practicallaw.thomsonreuters.com/0-201-9413?contextData=(sc.Default)&transitionType=Default&firstPage=true (accessed May 05, 2023).

[56] T. Vernon, "Data protection," Fire Risk Manag., no. SEPTEMBER, pp. 43–44, 2009.

[57] E. Guanabara, K. Ltda, E. Guanabara, and K. Ltda, "Introduction to the hash function as a personal data pseudonymisation technique." European Data Protection Supervisor, p. 31, 2019.

[58] C. Testart, "Understanding the Institutional Landscape of Cyber Security," SSRN Electron. J., no. August, pp. 1–42, 2018, doi: 10.2139/ssrn.2756608.

[59] S. Dzazali, A. Sulaiman, and A. H. Zolait, "Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations," Gov. Inf. Q., vol. 26, no. 4, pp. 584–593, 2009, doi: 10.1016/j.giq.2009.04.004.

[60] A. T. Tunggal, "What is Personally Identifiable Information (PII)? | UpGuard," UpGuard, May 01, 2022. https://www.upguard.com/blog/personally-identifiable-information-pii (accessed Jul. 20, 2022).

[61] Attivo Networks company, "Identity Threat Detection and Response (ITDR)," 2022.

[62] Verizon, "DBIR Data Breack Investigation Report 2008-2022," 2022.

[63] Attivo Networks, "Improving cyber hygiene by remediating exposed credentials," 2021.

[64] BeyondTrust, "What is Privileged Access Management (PAM)," BeyondTrust, Jan. 22, 2021. https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam (accessed Jul. 27, 2022).

[65] Beyondtrust, "Privilege Management for desktops Multiple Deployment Options: Install Privilege Management for Windows," 2019. [Online]. Available: https://www.beyondtrust.com/docs/privilege-management/windows/admin/install-upgrade/install-pm-windows.htm

[66] NIST, "NISTIR 7657 A Report on the Privilege (Access) Management Workshop NIST IR 7657 A Report on the Privilege (Access) Management Workshop," in Privilege (Access) Management Workshop, 2010, p. 48.

[67] BeyondTrustSoftware, "Seven Steps to Complete Privileged Access Management," 2017.

[68] ManageEngine, "Privileged access management 101 : A comprehensive guide to building a sound PAM strategy for your enterprise," ManageEngine. pp. 1–14, 2019.

[69] M. W. Sanders, “Automated methods for generating least privilege access control policies,” Colorado School of Mines, 2019.

[70] S. Ahmad, S. Mehfuz, F. Mebarek-Oudina, and J. Beg, “RSM analysis based cloud access security broker: a systematic literature review,” Cluster Comput., vol. 3, no. 6, p. 31, 2022, doi: 10.1007/s10586-022-03598-z.

[71] Bitglass, “The Definitive Guide to Cloud Access Security Brokers.” Amazone, Silcon valley, p. 14, 2015.

[72] C. Lawson, N. MacDonald, B. Lowans, B. Reed, and Gartner, “The Definitive Guide to Cloud Access Security Brokers.” Bitglass, 2015. [Online]. Available: https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/Bitglass_WP_Definitive_Guide_to_CASB.pdf

[73] C. Yambari, “Drawbacks of CASBs (Cloud Access Security Brokers) in the Remote World | Zluri,” zluri technologies, Mar. 02, 2022. https://www.zluri.com/blog/casb-drawbacks/ (accessed Jul. 19, 2022).

[74] Versa Networks, “Cloud access security broker (CASB),” 2022. [Online]. Available: https://www.netskope.com/es/security-defined/what-is-casb%0Ahttps://umbrella.cisco.com/products/cloud-access-security-broker-casb

[75] J. C. Roberts and B. Bersani, “Human Trafficking as a Cybercrime: A Rational Choice Theory Perspective,” University of Maryland, College Park, 2021.

[76] J. Scott, “Rational Choice Theory,” no. 1920, pp. 1–15, 2000.

[77] D. Satz and J. Ferejohn, “Rational Choice and Social Theory,” J. Philos., vol. 91, no. 2, pp. 71–87, 1994.

[78] R. L. Akers, “Rational Choice , Deterrence , and Social Learning Theory in Criminology : The Path Not Taken Not Taken *,” J. Crim. Law Criminol., vol. 81, no. 3, p. 25, 1991.

[79] B. McCarthy and A. Chaudhary, “Rational Choice Theory,” Encyclopedia of Criminology and Criminal Justice. Springer, New York, NY, New York, NY, pp. 4307–4315, 2014. doi: 10.1007/978-1-4614-5690-2_396.

[80] M. Bachmann, “What Makes Them Click ? Applying The Rational Choice Perspective To The Hacking Underground,” University of Central Florida, 2008.

[81] G. E. Higgins, “Digital Piracy , Self-Control Theory , and Rational Choice : An Examination of the Role of Value,” Int. J. Cyber Criminol., vol. 1, no. 1, pp. 33–55, 2007.

[82] L. Irwin, “9 cyber security predictions for 2022 - IT Governance UK Blog,” IT Governance Blog, Feb. 2022.

[83] F. Daniel, “Artificial Intelligence in Insurance – Three Trends That Matter | Emerj Artificial Intelligence Research,” emerj AI research and advisory company , Mar. 14, 2020. https://emerj.com/ai-sector-overviews/artificial-intelligence-in-insurance-trends/ (accessed Jul. 25, 2022).

[84] G. Denise, “Catch and keep more customers with a digital insurance platform,” Majesco, Dec. 10, 2020. https://www.majesco.com/platform-technologies-that-belong-in-your-tech-portfolio/ (accessed Jul. 25, 2022).

[85] S. Veselovská and E. Jančíková, “New Trends in Insurance Information Security Technologies,” Conf. Proc. 2nd Int. Sci. Conf. ITEMA 2018, vol. 2, no. 10, pp. 652–659, 2018, doi: 10.31410/itema.2018.652.