DOI: 10.5937/serbjph2502120T

ПРЕГЛЕДНИ РАД
REVIEW ARTICLE

ПСИХОЛОШКИ ЕФЕКТИ САЈБЕРБЕЗБЕДНОСНИХ ПОВРЕДА ПОДАТАКА КОД ОСОБА ИЗ НИГЕРИЈЕ

Сулејман Тојин, Бранка Стаматовић Гајић

Факултет здравствених и пословних студија, Ваљево, Србија

THE PSYCHOLOGICAL EFFECTS OF CYBERSECURITY BREACHES AMONG INDIVIDUALS IN NIGERIA

Sulaiman Toyin, Branka Stamatović Gajić

Faculty for Health and Business Studies, Valjevo, Serbia

Сажетак

Људска грешка је примарни узрок рансомвер напада, безбедносних повреда података и других сајбер претњи, и доводи до све већег броја сајбербезбедносних инцидената. Како системи информационе безбедности (сајбербезбедносни системи) постају све комплекснији, код људи све лакше долази до когнитивног преоптерећења и замора од упозорења, што може да утиче на учинак и да повећа вероватноћу грешке. Ово истраживање се бави психолошким ефектима сајбербезбедносних повреда података међу особама из Нигерије. Истраживање се ослања на теорију заштитне мотивације (енгл. *Protection Motivation Theory,* PMT*,* у даљем тексту ТЗМ) а податке преузима примарно из секундарних извора, укључујући часописе и чланке доступне на интернету. Подаци су квалитативно анализирани помоћу алата за анализу садржаја PQRS (енгл. *Preview, Question, Read, and Summarize*, прегледај, преиспитај, прочитај и резимирај), који је предложио Кохен (1990). Ова студија открива да сајбербезбедносне повреде података могу да доведу до општих кривичних дела и психолошке несигурности у Нигерији. Она закључује да дуготрајна изложеност штетном садржају са интернета може да утиче на когнитивне способности, укључујући решавање проблема и доношење одлука. Жртве могу да имају проблема са концентрацијом или доношењем рационалних одлука, што може потенцијално да утиче на њихов капацитет да се носе са својим свакодневним обавезама.

Кључне речи: сајбербезбедносне претње, дигитализација, појединац, психологија

Abstract

Human error is a primary cause of ransomware attacks, data breaches, and other cyberthreats, increasingly driving cybersecurity incidents. As cybersecurity systems become more complex, individuals are more prone to cognitive overload and alert fatigue, which can impair performance and raise the likelihood of errors. This study examines the psychological effects of cybersecurity breaches among individuals in Nigeria. The investigation is anchored on Protection Motivation Theory (PMT) and draws its data primarily from secondary sources, including online journals and articles. The data were qualitatively analyzed using the content analysis tool PQRS (Preview, Question, Read, and Summarize system), as proposed by Cohen (1990). This study reveals that cybersecurity breaches can lead to general crime and psychological insecurity in Nigeria. It concludes that long-term exposure to harmful internet content may affect cognitive abilities, including problem-solving and decision-making. Victims may struggle to concentrate or make sound decisions, potentially affecting their capacity to handle everyday obligations.

Keywords: Cyberthreats, Digitalization, Individual, Psychology

Увод

Дигитализација је идентификована као најзначајнији технолошки тренд који трансформише и друштво и привреду. Предузећа и појединци су данас под сталним притиском да користе дигиталне технологије [1]. Иако дигитализација доноси многе добробити, она подразумева и одређену цену [2]. Не може се порећи да је дигитализација остварила дубок утицај на друштво, обезбеђујући платформу за брзу комуникацију, пословање и повезивање широм света. Нажалост, како је растао значај информационог (сајбер) простора, тако су расле и количина и разноликост повреда података [3]. Повреде података могу да погоршају постојећа стања у

Introduction

Digitalization has been identified as the most significant technological trend transforming both society and business. Today, firms and individuals are constantly pressured to use digital technologies [1]. While digitalization offers many benefits, it also entails associated costs [2]. Undeniably, digitalization has profoundly influenced society, providing a platform for rapid communication, business, and connection worldwide. Unfortunately, as the significance of cyberspace grows, so has the quantity and diversity of data breaches [3]. Data breaches can exacerbate pre-existing mental health conditions by inciting feelings of worry, anxiety, and helplessness. The additional stress and men-

домену менталног здравља, покрећући осећаје забринутости, анксиозности и беспомоћности. Додатни стрес и ментални напор који проистекну из таквих повреда могу да погоршају постојеће проблеме.

Ово истраживање се бави оценом психолошких утицаја код особа након сајбербезбедносних повреда података и системима за подршку и интервенцијама који су доступни жртвама сајбербезбедносних повреда. Они се користе као конструкти за предвиђање психолошких ефеката (зависна променљива) информатичке безбедности на појединце (независна променљива).

У многим сферама живота, сајбербезбедносне повреде података могу да омету појединце да постигну своје циљеве, што је значајна ситуациона претходница негативних осећања. Неколико студија је претходно показало да постоји веза између сајбербезбедносних напада и негативних емоција као што су анксиозност, бес, туга и несигурност [4]. Утицај интернета на друштво је јасан, и како се информатички простор шири, расту и учесталост и разноврсност информатичких напада [3]. Већа је вероватноћа да ће јавност одреаговати на последице информатичког напада, него на сâм напад [5].

Значајан пример је сајбербезбедносни напад у коме би злонамерни софтвер (малвер) погодио електрану, остављајући хиљаде људи без струје. У овом сценарију, јавност се можда уопште не би интересовала за саму инфекцију малвером већ за њен исход, као што је губитак струје и последична немогућност да се кува или греје. Предвидиве бихејвиоралне и когнитивне тенденције, које су добро познати фактори у психологији људских фактора, обично доводе до људске грешке у области сајбербезбедности. Фишинг (енгл. *phishing*) и социјални инжењеринг су највеће слабости, које често наводе запослене да ненамерно открију своје креденцијале нападачима, због незнања или изостанка провере [6, 7]. Когнитивне пристрасности, као што је постављање једноставности поступка изнад безбедности, може се илустровати примером лоших пракси код одабира слабих лозинки, као што је поновна употреба истих креденцијала [8, 9, 10]. Према когнитивној психологији, појединци који развију навике у вези са лако запамтивим или често коришћеним лозинкама ће такве лозинке чешће користити на више платформи, што отвара могућности за хакере.

Додатни проблеми, као што су неправилна конфигурација и управљање привилегијама, илуструју колико недостаци менталне обраде података и превиди могу да доведу до несразмерних привилегија за приступ подацима, чиме се повећава могућност експлоатаци-

tal strain brought on by such violations may worsen existing problems.

This study assesses the psychological impacts experienced by individuals after cybersecurity breaches and examines the support systems and interventions available for victims of cybersecurity breaches, using these as constructs to predict the psychological effects (dependent variable) of cybersecurity on individuals (independent variable).

In many facets of life, cybersecurity breaches can impede individuals from realizing their goals, thus serving as a significant situational antecedent of negative feelings. Several studies have previously demonstrated a link between cybersecurity attacks and negative emotions such as anxiety, wrath, sadness, and insecurity [4]. The internet's impact on society is clear, and as cyberspace expands, so do the frequency and types of cyberattacks [3]. The public is more likely to respond to the outcomes of a cyberattack than to the attack itself [5].

A pertinent example is a cyberattack where malware compromises a national power plant, leaving hundreds of thousands without energy. In this scenario, the public might not be concerned with the malware infection itself but rather with the outcome, such as losing power and consequently being unable to cook or have heat. Predictable behavioral and cognitive tendencies, well-established in human factors psychology, typically cause human error in cybersecurity. Phishing and social engineering are major weaknesses, often leading to employees unintentionally revealing credentials to attackers due to ignorance or lack of verification [6, 7]. Cognitive biases, such as prioritizing convenience over security, can result in vulnerabilities, exemplified by weak password practices like reusing credentials [8, 9, 10]. According to cognitive psychology, individuals who develop habits around easily remembered or frequently used passwords are more likely to apply them across platforms, thereby creating opportunities for hackers.

Additional issues, such as improper configuration and rights management, illustrate how deficiencies in mental processing and oversight can lead to disproportionate access privileges, increasing the potential for data exploitation. Human factors psychology suggests that when individuals heavily rely on automated systems to prevent errors, a lack of routine checks and procedural safeguards can foster complacency [8, 9, 10]. Employees may neglect security concerns in favor of convenience, influenced by behavioral patterns. Furthermore, careless handling of removable media poses additional risks; users may fail to recognize the likelihood of malware transmission due to

је података. Психологија људског фактора указује да, када се особе снажно ослањају на аутоматске системе за спречавање грешки, недостатак рутинских провера и процедуралних безбедносних механизама може довести до осећаја уљуљканости [8, 9, 10]. Запослени могу да занемаре безбедносне аспекте, дајући предност једноставности поступка, на шта утичу обрасци понашања. Уз то, непажљиво руковање преносивим медијима представља додатне ризике; корисници могу да не препознају да постоји вероватноћа преноса малвера, услед недовољне обучености или навика у коришћењу таквих уређаја [6, 7]. Коначно, постављање приватних садржаја на друштвеним медијима наглашава информатичко-психолошке тенденције ка откривању сопственог живота и дељењу информација, при чему корисници могу погрешно да процене безбедност, али и домашај сопствених објава. Ови инциденти наглашавају неопходност проактивне културе информатичке безбедности која, када се споји са свеобухватном обуком у области информатичке безбедности и политикама будног праћења, може да појача отпорност на људске грешке [6, 7].

Алијанса за информатичке претње (енгл. *Cyber Threat Alliance*, CTA, у даљем тексту АИП) окупља познате компаније из области безбедности, са важним показатељима претњи који су раније дељени у силосима [11]. Са Мајклом Данијелом на челу, АИП има за циљ да „омогући висококвалитетно дељење информација о информатичким претњама у стварном времену, међу компанијама и организацијама које се баве информатичком безбедношћу, како би се побољшала информатичка безбедност наших глобалних дигиталних екосистема". АИП нуди досад невиђене увиде у криминалне тактике, кроз сарадњу преко 32 безбедносне организације које свакодневно сарађују у сагледавању ризика. Током 2017. године, установљена је Мрежа за подршку у области информатичког криминала (енгл. *Cybercrime Support Network*, CSN, у даљем тексту МПОИК), са циљем да се позабави значајним јазом у подршци жртвама информатичког криминала. МПОИК је поставила интернет сајт *fightcybercrime.org* и сарађује са федералним, државним и локалним властима у дељењу материјала милионима Американаца, у недостатку програма који би био подржан на националном нивоу [11].

МПОИК је такође пилотирала технику кол-центара у шест држава, заједно са интернет сајтом који омогућава власницима малих предузећа и клијентима да добију подршку у пријављивању, поновном успостављању и унапређењу њихових сигурносних система након инцидента. МПОИК је обучила специјалисте за рад у кол-центру да воде жртве кроз интернет сајт

inadequate training or habitual device usage behaviors [6, 7]. Finally, posting private content on social media highlights cyber psychology tendencies toward self-disclosure and information sharing, where users may misjudge the security and reach of their posts. These incidents underscore the necessity of a proactive cybersecurity culture, which, combined with comprehensive cybersecurity training and vigilant policies, can strengthen resistance to human error [6, 7].

The Cyber Threat Alliance (CTA) has brought together well-known security firms with important threat indicators that were previously shared in silos [11]. Led by Michael Daniel, the CTA aims to "enable near real-time, high-quality cyber threat information sharing among companies and Cybersecurity organizations in order to improve the cybersecurity of our global digital ecosystem." The CTA offers unparalleled insight into criminal tactics, with over 32 security organizations collaborating daily to discuss risk. In 2017, the Cybercrime Support Network (CSN) was established to address a significant void for cybercrime victims. CSN established fightcybercrime.org and collaborated with federal, state, and local governments to disseminate materials to millions of Americans in the absence of a nationally supported program [11].

CSN has also piloted a call-center technique in six states, alongside a website where small businesses and customers can get assistance with reporting, recovering, and bolstering their security after an incident. CSN trained Call Specialists to guide victims through the fightcybercrime.org website and provide support for reporting crimes to the FBI, FTC, or other appropriate authorities, utilizing the existing 211 human services referral lines run by United Way groups. Over 90% of callers reported being happy or very happy with the service [11].

Statement of the Problem

Human error is the primary cause of ransomware attacks, data breaches, and other cyberthreats, increasingly driving cybersecurity events [8, 9]. Studies indicate that human error accounts for over 80% of cybersecurity problems [8]. About 422 million people were affected by this increase as of 2022, and estimations suggest that by the end of 2023, up to 33 billion accounts may have been compromised [12, 13]. Cybersecurity Ventures estimated the global economic cost of cybercrime to be an alarming $8 trillion USD at the end of 2023, with an annual growth rate of 15%. By 2025, it could reach $10.5 trillion USD, more than tripling the reported $3 trillion USD cost in 2015 [14].

As cybersecurity systems become more complicated, in-

fightcybercrime.org и пружа подршку у пријављивању кривичних дела надлежним органима као што су FBI, FTC, и друга одговарајућа надлежна тела, користећи 211 телефонских линија за преусмеравање позива, са оператерима, којим управља компанија Јунајтед веј (енгл. *United Way*). Преко 90% корисника који су позвали центар су изјавили да су били задовољни или веома задовољни овом услугом [11].

Формулација проблема

Људска грешка је примарни узрок рансомвер напада, безбедносних повреда података и других сајбер претњи, и доводи до све већег броја сајбербезбедносних инцидената [8, 9]. Студије указују да се људском грешком може објаснити преко 80% сајбербезбедносних проблема [8]. Од 2022. године, овим погоршањем је погођено око 422 милиона људи, док процене указују да је до 2023. године и до 33 милијарде налога можда компромитовано [12, 13]. Компанија Сајберсикјурити венчурес (енгл. *Cybersecurity Ventures*) процењује да је глобални економски трошак информатичког криминала узнемиравајућих осам билиона америчких долара до краја 2023. године, са годишњом стопом раста од 15%. До 2025. године, овај трошак би могао да досегне 10,5 билиона америчких долара, што је више него три пута више од пријављених три билиона долара трошка у 2015. години [14].

Како системи информационе безбедности постају све компликованији, код људи све лакше долази до когнитивног преоптерећења и замора од упозорења, што може да утиче на учинак и да повећа вероватноћу грешке [8, 9]. Претходне студије су испитивале психолошке ефекте сајбербезбедносних повреда података код појединаца, како помоћу квалитативних тако и помоћу квантитативних метода. Међутим, ниједна од ових ранијих студија није користила нити синхронизовала специфичне показатеље из ове студије, како би истражила психолошке ефекте сајбербезбедносних повреда података на особе из Нигерије, што је тачан циљ овог истраживања. Ова студија има за циљ да попуни тај јаз у знању и обезбеди одговоре на следећа истраживачка питања:

1. Који су уобичајени психолошки утицаји на особе из Нигерије након сајбербезбедносних повреда података?
2. Који системи за подршку и интервенције су тренутно доступни за жртве сајбербезбедносних повреда података у Нигерији, и колико су они делотворни?

dividuals are increasingly likely to experience cognitive overload and alert fatigue, which can impair performance and increase the likelihood of errors [8, 9]. Prior research has examined the psychological effects of cybersecurity breaches on individuals using both qualitative and quantitative methods. However, none of these earlier studies have used and synchronized the specific indicators of this study to investigate the psychological effects of cybersecurity breaches on individuals in Nigeria, which is the precise aim of this research. This study aims to fill this knowledge gap and provide answers to the following research questions:

1. What are the common psychological impacts experienced by individuals in Nigeria following cybersecurity breaches?
2. What support systems and interventions are currently available for victims of cybersecurity breaches in Nigeria, and how effective are they?

Conceptual Clarification

Digitalization

Digitalization has transformed nearly every aspect of life over the last few decades. Access to the internet, the increasing use of mobile phones, social media, and other ICT services have changed how people interact, communicate, learn, and work in almost every country [15, 16]. According to Schelenz and Schopp (2018) [16], "the term digitization refers to 'the action or process of digitizing; the conversion of analogue data (esp. in later use images, video, and text) into digital form.'" In a common sense, digitalization refers to the integration of digital technologies into everyday life across processes, organizations, businesses, and other societal domains. Often, the specific role of digitalization in business models is emphasized. In this context, digitalization focuses on the adoption and use of digital technology by key market players and other stakeholders, including distributors, producers, consumers, film practitioners, associations, policymakers, and politicians.

According to Parviainen et al. (2017) [17], the process of digital transformation involves the restructuring of many domains of social life around digital communication and media infrastructure. Since the emergence of the term digitalization, its effects on society have been central to discussion. The first modern use of the term digitalization in connection with computerization can be seen in an essay published in the *North American Review* in 1971. Wachal (1971), cited in Gorenšek & Kohont (2019) [18], describes the implications of digitalization for society in the context of countering objections to and the possibility of comput-

Појашњење концепта

Дигитализација

Дигитализација је трансформисала скоро сваки аспект живота у последњих неколико деценија. Приступ интернету, све већа употреба мобилних телефона, друштвени медији и други ИКТ сервиси променили су начин на који људи ступају у међусобну интеракцију, комуникацију, како уче и раде, у скоро свакој држави [15, 16]. Према Шеленцу и Шопу (2018) [16], израз дигитализација се односи на „радњу или процес дигитализовања; превођење аналогних података (посебно касније слика, видео снимака и текста) у дигитални облик". У општеприхваћеном смислу, дигитализација се односи на интеграцију дигиталних технологија у свакодневни живот у различитим процесима, организацијама, предузећима и другим друштвеним доменима. Често се наглашава специфична улога дигитализације у пословним моделима. У овом контексту, дигитализација се фокусира на усвајање и употребу дигиталних технологија од стране кључних играча на тржишту и других актера, укључујући дистрибутере, продуценте, потрошаче, филмске ствараоце, удружења, креаторе политика и политичаре.

Према Парвианену и сарадницима, (2017) [17], процес дигиталне трансформације укључује реструктурирање бројних домена друштвеног живота око инфраструктуре дигиталних комуникација и медија. Откако је дигитализација дефинисана као појам, њен утицај на друштво заузима централно место у расправама. Прва модерна употреба израза дигитализација у вези са комјутеризацијом (преласком на широку употребу рачунара) може се срести у есеју који је објављен у часопису „Северноамерички преглед" *(North American Review)* 1971. године. Вашал (1971), цитиран у публикацији Гореншек и Кохонт (2019) [18], описује импликације дигитализације по друштво у контексту могућности истраживања друштвених појава помоћу рачунара, и износи контрааргументе за приговоре на такву употребу. Проучавање и истраживање концепта дигитализације произвело је огромну количину материјала у литератури, наглашавајући како структуре дигиталних медија обликују и утичу на савремени свет. У овом контексту, дигитализација је почела да се бави структурирањем разноврсних области друштвеног живота око инфраструктуре дигиталних комуникација и медија. Гореншек и Кохонт (2019) [18] виде дигитализацију као једну од кључних, ако не и најважнију, одлику савременог света.

er-aided exploration of social phenomena. Studying and exploring the concept of digitalization has produced an enormous body of literature, highlighting how digital media structures shape and influence the modern world. In this context, digitalization has begun to address the structuring of diverse areas of social life around digital communication and media infrastructure. Gorenšek & Kohont (2019) [18] view digitalization as one of the key, if not crucial, features of the modern world.

Ethical Considerations in the Management of Cybersecurity Breaches

Analyzing the existing scholarly literature on ICT in general and cybersecurity particularly regarding moral values [19], one will find, among others, privacy and trust, freedom and (informed) consent, fairness, and equality, as well as dignity and solidarity [20]. While this list is by no means complete, it is clear that a wide range of moral values are involved in the development and use of ICT and the provision of cybersecurity. When considering ICT in healthcare as a paradigmatic use case, these values can be expanded to include the principles of Beauchamp and Childress (2019) [21]: autonomy, beneficence, non-maleficence, and justice. While these principles originate in biomedical ethics, they can be applied in professional domains beyond healthcare. Adherence to these values and principles must guide professional behavior because they constitute the core of the respective profession. They should guide the professional behavior of, for instance, physicians, computer scientists, or engineers – especially when they are concerned with ensuring cybersecurity. Yet, this means there may be circumstances in which the core moral values of a profession may compete or even conflict with technical or other requirements.

A comprehensive cybersecurity strategy includes more than just technical elements, as concluded by Christen et al. (2017) [20]. It must encompass aspects of leadership, societal, and corporate culture and include larger economic and even sociopolitical elements (e.g., national security). Cybersecurity must be understood as a multi-dimensional task. Without claiming to be exhaustive, one can identify moral values, technical requirements, and other factors that influence ICT design and thus profoundly impact the conditions under which cybersecurity can be provided. The provision of cybersecurity depends on numerous values, aims, and requirements that are interrelated but also in competition or even conflict with each other.

Literature Review

This section reviews material pertinent to the research's

Етичка разматрања код управљања безбедносним повредама података

Анализа постојеће академске литературе о ИКТ уопштено, те о информатичкој (сајбер) безбедности посебно, у погледу моралних вредности [19], доводи, између осталог, до питања приватности, поверења, слободе и (информисаног) пристанка, праведности и једнакости, као и достојанства и солидарности [20]. Иако овај списак ни у ком случају није исцрпан, јасно је да је у развој и употребу ИКТ, као и у пружање информатичке безбедности, укључен широк спектар моралних вредности. Када се разматра ИКТ у здравству, као парадигматски пример употребе, ове вредности се могу проширити да обухвате начела Бошама и Чилдреса (2019) [21]: аутономије, доброчињења, нешкодљивости и правде. Иако ова начела потичу из биомедицинке етике, могу се применити и у стручним доменима изван здравства. У својим поступцима, стручњаци се морају усмеравати управо овим вредностима, јер они представљају окосницу својих професија. Ове вредности би требало да усмеравају професионално одношење, на пример, лекара, информатичара или инжињера, посебно када је реч о обезбеђивању информатичке безбедности. Ипак, то значи да би могле да постоје околности у којима би централне моралне вредности неке професије могле да дођу у компетицију или чак и конфликт са техничким и другим захтевима.

Свеобухватна стратегија информатичке безбедности не обухвата само техничке елементе, као што су закључили Кристен и сарадници (2017) [20]. Она мора да обухвати аспекте лидерства, друштвене и корпоративне културе, и да укључи шире економске, па чак и друштвено-политичке елементе (нпр. државну безбедност). Информатичка безбедност се мора разумети као вишедимензионални задатак. Не тврдећи да је сачињен исцрпан списак, могу се идентификовати моралне вредности, технички захтеви и други фактори који утичу на дизајн ИКТ, и тиме остварују снажан утицај на услове под којима се може осигурати информатичка безбедност. Осигурање информатичке безбедности зависи од бројних вредности, циљева и захтева који су међусобно повезани, али су некада међусобно конкурентни, или чак у конфликту једни са другима.

Преглед литературе

Овај део рада се бави прегледом материјала који су релевантни за циљ овог истраживања, уз одавање признања ауторима за њихов значајан допринос овој научној области.

goal, acknowledging the authors for their robust contributions to this field of study.

Common Psychological Impacts Experienced Following Cybersecurity Breaches

Bada and Nurse (2020) [15] examined an employee's feelings following a cyberattack at their company. The study explored how workers cope with a cyberattack on an emotional and psychological level. The study found that senior management plays a critical role in changing employees' emotional and coping abilities through their support and intervention. Numerous studies have shown that empathy is a fundamental leadership trait; however, it is rarely displayed in the workplace, particularly following catastrophic circumstances. This is especially true for security specialists who defend their organizations' organizational and business data on the front lines of conflict. The study supports the conceptual challenges that affect employee well-being. It clearly showed that cybersecurity assaults have serious psychological repercussions that need to be addressed in addition to becoming a barrier for engineers. While some individuals are more likely to have a strong negative affective stress reaction and neglect to take the necessary actions, others are more likely to react proactively and positively, reducing the negative consequences of the cybersecurity breach. Psychological problems and possibly psychosis may be identified, especially for these individuals. Although this current study focuses on the psychological consequences of cybersecurity breaches on individuals, the reviewed study's initial goal is pertinent as it explored how employees deal emotionally and psychologically with a cyberattack.

Bada and Nurse (2020) [15] also examined employees' emotional responses and coping mechanisms in the event of a cyberattack. The study investigated how employees react emotionally and cope with a cyberattack. Data was gathered using a comprehensive case study technique involving 24 semi-structured interviews at a multinational manufacturing organization, alongside primary observations and a collection of secondary materials. Technology Threat Avoidance Theory (TTAT) was used to enhance the grounded approach to data analysis through an emotion-theoretic lens. The study's conclusions, based on structural appraisal theory, show that the IT security team in the case study alternated between negative emotion-focused coping and positive problem-focused coping. Senior management empathy and resource mobilization were important explanatory factors or turnaround mechanisms that mediated this oscillation. A conceptual model known as the Transformation of Coping via Empathic Leadership (T-CEL) is developed by building on these studies. Through their support and intervention, senior manage-

Уобичајени психолошки утицаји до којих долази након сајбербезбедносних повреда података

Бада и Нурс (2020) [15] су испитивали осећања запослених након сајбербезбедносне повреде података у њиховим предузећима. Студија је истраживала како радници превладавају безбедносне повреде података на емоционалном и психолошком нивоу. У студији је пронађено да више руководство, кроз подршку и интервенције, игра критичну улогу у промени емоционалних и способности превладавања код запослених. Бројне студије су нагласиле емпатију као фундаменталну особину у лидерству; међутим, она се ретко испољава на радном месту, посебно након катастрофалних околности. Ово је посебно тачно за специјалисте у области безбедности, који бране организационе и пословне податке својих организација на првим борбеним линијама конфликта. Студија подржава концептуалне изазове који утичу на добробит запослених. Она је јасно показала да сајбербезбедносни напади имају озбиљне психолошке последице којима се мора позабавити, уз то што постају баријера за инжињере. Иако неки појединци показују већу вероватноћу снажне негативне афективне реакције на стрес и не предузимају неопходне радње, за друге је вероватније да ће позитивно и проактивно реаговати, чиме се смањују негативне последице информатичких повреда података. Могу се идентификовати психолошки проблеми, а могуће и психозе, посебно код ових појединаца. Иако се тренутна студија фокусира на психолошке последице сајбербезбедносних повреда података код појединаца, почетни циљ студије која је предмет овог прегледа је значајан, јер се она бавила испитивањем како се запослени емоционално и психолошки носе са сајбербезбедносним нападима.

Бада и Нурс (2020) [15] су такође испитали емоционалне одговоре и механизме превладавања запослених у случајевима информатичких напада. Студија је испитала како запослени емоционално реагују и како се носе са сајбербезбедносним нападом. Подаци су прикупљани помоћу свеобухватне технике студије случаја, у којој су коришћена 24 полуструктуирана интервјуа у мултинационалној производној организацији, заједно са примарним опсервацијама и прикупљањем секундарних материјала. Теорија избегавања технолошких претњи (енгл. *Technology Threat Avoidance Theory*, TTAT) је примењена како би се унапредио рационални приступ анализи података кроз призму емоционално-теоретског приступа. Закључци студије, на основу теорије структурне оцене, показују да је тим за ИТ безбедност у посматраној студији случаја алтернирао између негативног превладавања фокусираног на емоције и позитивног превладавања фокусираног

ment can significantly improve employees' emotional and coping skills. Because it examines workers' emotional and coping reactions to a cyberattack, this study is relevant to the first objective of this present research, which focuses on the psychological effects of cybersecurity breaches on individuals in Nigeria.

Support Systems and Interventions Currently Available for Victims of Cybersecurity Breaches

Bada and Nurse (2020) [15] also examined the emotional experiences of victims of cybersecurity breaches. The study specifically investigated emotional responses to cybersecurity breaches. A context-specific tool was developed based on the studied literature. 145 participants who had experienced a cybersecurity breach reported on their assessments, action tendencies, bodily reactions, expressions, subjective feelings, and regulation attempts. The tool employs a thorough approach to evaluate emotional reactions to cybersecurity threats and offers an effective method for identifying potentially problematic reactions. A distinct three-dimensional structure emerged from a principal component analysis of 75 emotion responses. Thus, the study concluded that to combat cybersecurity concerns, emotional support systems must be developed in addition to technological advancements to prevent detrimental long-term psychological effects. Since the current study focuses on the psychological impact of cybersecurity breaches on individuals, the study's objective, which examined emotional reactions to such breaches, is relevant to current procedures for providing assistance and interventions to victims of cybersecurity breaches in Nigeria.
Canetti et al. (2017) [4] examined how people felt about and trusted autonomous vehicles after cybersecurity events, investigating the different elements that support this trust in light of such incidents. The study employed a dual-methodological approach. A cohort of 151 individuals completed structured questionnaires to collect quantitative data, while in-depth semi-structured interviews with specialists in AV technology and cybersecurity provided qualitative data. The key factors influencing public trust from the perspective of research participants were then identified through rigorous structural equation modeling of the quantitative data. The study concluded that cyber-attacks undoubtedly reduce public trust in AVs and emphasized the significance of perceived safety, incident severity, regulatory frameworks, and business legacy in forming public trust. Therefore, the report advises all parties involved, from legislators to AV manufacturers, to map out the path for effective future AV integration. Although the current study focuses on the psychological impacts of cybersecurity breaches on individuals, Canetti et al.'s study [4] is relevant to the second objective of this research, as it examines elements

на проблем. Емпатија вишег руководства и мобилизација ресурса били су важни фактори којима се може објаснити ово осцилирање, и утицали су на преусмеравање ових осцилација. Концептуални модел познат као трансформација превладавања помоћу емпатичног вођства (енгл. *Transformation of Coping via Empathic Leadership*, T-CEL) развијен је управно надоградњом на ове студије. Својом подршком и интервенцијом, више руководство може значајно да унапреди емоционалне и вештине превладавања код запослених. Због тога што испитује емоционалне и реакције превладавања запослених на информатички напад, ова студија је релевантна за први циљ овог истраживања, које се фокусира на психолошке ефекте сајбербезбедносних повреда података код појединаца у Нигерији.

Тренутно доступни системи подршке и интервенције за жртве безбедносних повреда података

Бада и Нурс (2020) [15] су такође испитивали емоционална искуства жртава сајбербезбедносних повреда података. Студија је специфично испитивала емоционалне одговоре на сајбербезбедносне повреде података. Развијен је инструмент специфичан за овај контекст, на основу проучене литературе. Они који су искусили сајбербезбедносну повреду података (145 учесника), известили су о својим оценама, тенденцијама ка одређеним радњама, телесним реакцијама, изражавању, субјективним осећањима и покушајима регулације. Овај инструмент користи детаљан приступ за оцењивање емоционалних реакција на сајбербезбедносне претње и нуди делотворан метод за идентификацију потенцијално проблематичних реакција. Из анализе главних компоненти 75 емоционалних одговора проистекла је јасна тродимензионална структура. Тако је студија закључила да је, у циљу борбе против сајбербезбедносних претњи, неопходно развити системе за емоционалну подршку, уз технолошке напретке, како би се спречили дуготрајни штетни психолошки ефекти. С обзиром да се ова студија фокусира на психолошке утицаје сајбербезбедносних повреда података на појединце, циљ студије, која је испитивала емоционалне реакције на такве повреде података, релевантан је за тренутне процедуре пружања подршке и интервенције за жртве сајбербезбедносних повреда података у Нигерији.

Канети и сарадници (2017) [4] су посматрали шта људи осећају и колико имају поверења у аутономна возила (АВ) након сајбербезбедносних догађаја, испитујући различите елементе који подржавају ово поверење у светлу таквих догађаја. У студији је примењен приступ двоструке методологије. Група од 151 особе је попунила структуиране упитнике како би се прикупили ко-

that support trust in the setting of cybersecurity events, concerning the efficiency of Nigeria's current procedures for providing assistance and interventions to victims of cybersecurity breaches.

Theoretical Framework

No single theory has gained ascendancy as an explanatory model for all types of psychological effects related to cyberattacks. Perhaps the diversity of their impact on individuals in Nigeria poses an inherent barrier to such a global theory, adding complexity to its construction and challenging the emergence of a unifying explanatory theory. This study is anchored on the Protection Motivation Theory (PMT) [22] to underpin the research.

Protection Motivation Theory (PMT)

Rogers (1975) [22] developed the Protection Motivation Theory (PMT), which posits that human and environmental factors combine to create a potential threat. Risk triggers two cognitive processes: threat appraisal and coping appraisal. The threat appraisal process evaluates the elements of the action that may pose a risk, such as the degree of danger, the individual's sensitivity to the threat, and the intrinsic and extrinsic motivations surrounding the acts. The coping appraisal process compares the costs (or efforts) associated with protective behavior (response cost) with an individual's ability to manage and avoid the presented danger (self-efficacy and reaction efficacy). How vulnerable a person feels to a hazard is related to their risk assessment. Various factors influence vulnerability to cyberattacks [23].

The most common indicator of protective motivation is the measurement of the "intention" to engage in the recommended preventive activity. The fact that people do not appear to view malicious cyberattacks as a threat to themselves, and if they do, believe there is nothing they can do to prevent them, is another important factor in understanding how the public responds to these attacks. Rather than the cyberattack itself, the public is more likely to respond to the event (such as a disruption of service). Adaptive intentions or behaviors were often made possible by increases in threat intensity, threat vulnerability, response efficacy, and self-efficacy.

Relevant Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) [22] is one of the often-used theories in behavioral information systems (IS) security research, a critical part of the information systems security field. Applications of protection motivation the-

лективни подаци, док су детаљни полуструктуирани интервјуи са специјалистима у области технологије АВ и информатичке безбедности донели квалитативне податке. Кључни фактори који су утицали на поверење јавности из перспективе учесника истраживања су потом идентификовани ригорозним моделовањем структурних једначина за квантитативне податке. Студија је закључила да су информатички напади несумњиво смањили поверење јавности у АВ и нагласила значај перципиране безбедности, озбиљности инцидента, регулаторних оквира и пословне заоставштине при формирању поверења јавности. Стога је извештај сугерисао свим укљученим странама, од законодаваца до произвођача АВ, да израде мапу пута за делотворну будућу интеграцију АВ. Иако се актуелна студија фокусира на психолошке утицаје сајбербезбедносних повреда података на појединце, студија Канетија и сарадника [4] је релевантна за други циљ овог истраживања, јер испитује елементе који подржавају поверење у окружење око сајбербезбедносних догађаја, што је релевантно за ефикасност актуелних процедура Нигерије за пружање помоћи и интервенција жртвама безбедносних повреда података.

Теоретски оквир

Ниједна теорија се није издвојила као модел који објашњава све врсте психолошких ефеката у вези са информатичким нападима. Можда разноликост њихових ефеката на појединце у Нигерији представља структурну баријеру таквој глобалној теорији, што чини њену конструкцију додатно комплексном и представља изазов за појављивање јединствене теорије којом би се све могло објаснити. Ова студија се ослања на Теорију заштитне мотивације (ТЗМ) [22], на коју се надограђује ово истраживање.

Теорија заштитне мотивације (ТЗМ)

Роџерс (1975) [22] је развио теорију заштитне мотивације (ТЗМ), по којој се људски фактор и фактор окружења удружују како би створили потенцијалну претњу. Ризик покреће два когнитивна процеса: процену претње и процену превладавања. Процес процене претње оцењује елементе радње који могу да представљају ризик, као што су степен опасности, осетљивост датог појединца на претњу, као и унутрашња и спољна мотивација у вези са тим радњама. Процена превладавања пореди цену или напор који се доводи у везу са заштитним понашањем (цена одговора) са способношћу појединца да управља и избегне представљену опасност (самоефикасност и ефикасност реакције). Осећај осетљиве особе у вези са опасношћу има везе са њеном проценом ризика. Различити фактори утичу на осетљи-

ory in information systems research have recently been examined by information systems studies [24]. Years of PMT studies in psychology provide many more important insights on information systems security research. This study may be able to comprehend why people do (or do not) adhere to information systems security measures by using the protection motivation theory insights that have not previously been examined in information systems security. For instance, research in psychology demonstrates that appeals that seek to evoke both fear and empathy increase the efficacy of threat messages when the targeted individual is accompanied by others at risk. Therefore, messages that encourage people to think about other people's perspectives might help them better understand why they should keep their data and information safe. Additionally, the insights from Protection Motivation Theory (PMT) may be used to develop effective treatments that improve people's information systems security behavior.

Method

This study examines the psychological effects of cybersecurity breaches on individuals in Nigeria. The data were collected through secondary sources and analyzed qualitatively using the PQRS (Preview, Question, Read, and Summarize) system of content analysis, as proposed by Cohen in 1990 [25].

Ethical Considerations

Research ethics standards were carefully adhered to throughout this study. The authors of the relevant literature used are mentioned in in-text citations and are properly referenced. The literature reviewed is all in line with the objectives of this research.

Discussion of Findings

Cybersecurity breaches can lead to psychological imbalance. While the effects of cybersecurity breaches are significant, their psychological impact on groups and individuals are also recognized as important. Bada and Nurse (2020) [15] revealed that through their support and intervention, senior management plays a critical role in changing employees' emotional and coping abilities during cybersecurity breaches. Their study also used Technology Threat Avoidance Theory (TTAT) to enhance the grounded approach to data analysis through an emotion-theoretic lens. The study's conclusions, based on structural appraisal theory, showed that the IT security team in the case study alternated between negative emotion-focused coping and positive problem-focused coping.
Literature on cybersecurity breaches has numerous meth-

вост на информатичке нападе [23].

Најчешћи показатељ заштитне мотивације је мера „намере" да се предузме препоручена превентивна активност. Чињеница да људи, наизглед, не виде информатичке нападе као претњу по себе саме, а и ако их виде тако, сматрају да ништа не могу да учине против њих, јесте још један значајан фактор у разумевању тога како јавност одговара на ове нападе. Већа је вероватноћа да ће јавност одговорити на последични догађај (као што је прекид неких услуга) него на сâм информатички напад. Адаптивне намере и понашања често су последица повећања интензитета претње, осетљивости на претњу, ефикасности одговора и самоефикасности.

Релевантна теорија заштитне мотивације (ТЗМ)

Теорија заштитне мотивације (ТЗМ) [22] је једна од често коришћених теорија у бихејвиоралним истраживањима безбедности информационих система (ИС), што представља критичан део информатичке безбедности. Примена теорије заштитне мотивације у истраживањима информационих система недавно је била предмет испитивања у студијама информационих система [24]. Године ТЗМ студија у психологији доносе многе додатне важне увиде у истраживања безбедности информационих система. Ова студија би могла да дође до одговора зашто се људи придржавају (или не) мера безбедности информационих система, применом увида из теорије заштитне мотивације који претходно нису били испитивани у области безбедности информационих система. На пример, истраживања у психологији показују да апели који имају за циљ да изазову и страх и емпатију повећавају ефикасност порука о претњама, када је особа којој су ове поруке намењене у друштву других који су такође под ризиком. Стога, поруке које охрабрују људе да размишљају о перспективама других могу да им помогну да боље разумеју зашто би требало да чувају безбедност својих података и информација. Уз то, увиди из теорије заштитне мотивације (ТЗМ) могу да се искористе за развој делотворних третмана којима се унапређују понашања људи у вези са информационом безбедношћу.

Метод

Ово истраживање се бави психолошким ефектима сајбербезбедносних повреда података међу особама из Нигерије. Подаци су прикупљени из секундарних извора и квалитативно анализирани применом алата за анализу садржаја PQRS (енгл. *Preview, Question, Read, and Summarize*, прегледај, преиспитај, прочитај и резимирај), који је предложио Кохен (1990) [25].

odological and definitional issues; 'cybersecurity breaches' have broad categories, such as Cyber Terrorism, Ransomware, Phishing, Cyberbullying, Cyber-stalking, etc. Research focusing on one manifestation of cybersecurity breaches (e.g., Cyber Terrorism) should not assume that the process is applicable to other types of cybersecurity breaches, such as Cyber Fraud. Perpetrators of cybersecurity breaches have varying motives, targets, demands, structures, and arenas of operations. Where an individual fails to properly manage their password, the chances that the perpetrator of cybersecurity breaches would hijack the system and gain access to data is very high, and the purpose of personal security will be defeated. Adhering to information systems security measures, using the Protection Motivation Theory insights as propounded by Rogers (1975) [22], becomes more important, especially in Nigeria.

Failure to adhere to information systems security measures can affect a nation's security and prosperity. The findings of Bada and Nurse (2020) [15] concluded that to combat cybersecurity concerns, emotional support systems must be developed in addition to technological advancements to prevent detrimental long-term psychological effects. Canetti et al. (2017) [4] examined how people felt about and trusted autonomous cars and concluded that cyberattacks undoubtedly reduce public trust in AVs, emphasizing the significance of perceived safety, incident severity, regulatory frameworks, and business legacy in forming public trust. Research in cognitive psychology and cyber psychology shows that high workloads and short deadlines necessitate quick decisions, which raises the risk of mistakes including missed alarms, misconfigured systems, and delayed threat responses [26]. Drawing from this background, human factors psychology suggests that by dividing mental demands, techniques like task-sharing and decision-support systems can reduce cognitive fatigue and avoid mistakes caused by an excessive amount of information [10].

Conclusion

This study aims to contribute insights into the psychological effects of cybersecurity breaches among individuals in Nigeria. In summary, a clear understanding of the differences among the literature reviewed, theoretical framework, and conceptual framework provides better guidance on the psychological effects of cybersecurity breaches among individuals in Nigeria.

This study reveals the existence of cybersecurity breaches that can lead to general crime and psychological insecurity in Nigeria. There are indications that cybersecurity breaches can have significant psychological effects on individual

Етичка разматрања

Током целе студије, етички стандарди истраживања су строго поштовани. Аутори релевантне литературе се наводе и у цитатима у тексту, као и у правилно наведеним референцама. Литература која је део овог прегледа усклађена је са циљевима овог истраживања.

Дискусија о резултатима

Сајбербезбедносне повреде података могу да доводу до психолошке неравнотеже. Иако су ефекти безбедносних повреда података значајни, њихов психолошки утицај на групе и појединце такође је препознат као значајан. Бада и Нурс (2020) [15] су открили да више руководство, кроз своју подршку и интервенције, игра критичну улогу у промени емоционалних и способности превладавања запослених током безбедносних повреда података. Њихова студија је такође применила теорију избегавања технолошких претњи (енгл. *Technology Threat Avoidance Theory*, TTAT) како би унапредила рационални приступ анализи података кроз призму емоционалне теорије. Закључци студије, на основу теорије структурне оцене, показују да је тим за ИТ безбедност у посматраној студији случаја алтернирао између негативног превладавања фокусираног на емоције и позитивног превладавања фокусираног на проблем.

Литература о безбедносним повредама података има бројне методолошке и проблеме у вези са дефиницијама; информациона (сајбербезбедносна) повреда података има широке категорије, као што су сајбер тероризам, рансомвер (*малициозни софтвер који захтева од жртве уплату новца/откупа како би омогућио поновни приступ подацима,* прим. прев), фишинг, сајбер-насилништво, сајбер-прогањање итд. Истраживања која су усмерена ка једном појавном облику сајбербезбедносне повреде података (нпр. сајбер-тероризму) не треба да претпоставе да се исти процес може применити на друге врсте безбедносних повреда података, као што је сајбер-превара. Починиоци сајбербезбедносних повреда података имају различите мотиве, циљеве, захтеве, структуре и области у којима оперишу. Када појединац не успе правилно да заштити своју лозинку, постоји велика шанса да починилац сајбербезбедносне повреде података отме систем и добије приступ подацима, чиме је поражена намена мера личне безбедности. Придржавање безбедносних мера у информационим системима, помоћу примене увида из теорије заштитне мотивације које је изнео Роџерс (1975) [22], добија на значају, посебно у Нигерији.

Непридржавање мера безбедности унутар информационих система може да утиче на безбедност и про-

victims in Nigeria.

This study therefore concludes that long-term exposure to harmful internet content might affect cognitive abilities, including problem-solving and decision-making. Victims may struggle to concentrate or make wise decisions, which may affect their capacity to handle everyday obligations. Furthermore, being targeted online can cause trust issues, leading people to lose faith in others and online platforms, making them reluctant to use social media or communicate online. This hesitation may cause them to become even more isolated from support networks.

сперитет целе државе. Бада и Нурс (2020) [15] у својој студији закључују да је, у циљу борбе против сајбербезбедносних претњи, неопходно развити системе за емоционалну подршку, уз технолошке напретке, како би се спречили дуготрајни штетни психолошки ефекти. Канети и сарадници (2017) [4] су испитивали колико људи имају поверења, и шта осећају у вези са аутономним возилима, и закључили су да информатички напади несумњиво смањују поверење јавности у АВ и нагласили значај перципиране безбедности, озбиљности инцидента, регулаторних оквира и пословне заоставштине при формирању поверења јавности. Истраживања у когнитивној психологији и сајбер психологији показују да високо радно оптерећење и кратки рокови захтевају брзо доношење одлука, што повећава ризик од грешака, укључујући пропуштена упозорења, погрешно конфигурисане системе и одложене одговоре на претњу [26]. Надограђујући на ово, психологија људског фактора указује да би подела менталног напора, технике као што су дељење задатака и системи за подршку при доношењу одлука, могли да смање когнитивни замор и доведу до избегавања грешака до којих долази услед прекомерне количине информација [10].

Закључак

Ово истраживање је намењено стицању увида у психолошке ефекте сајбербезбедносних повреда података међу особама из Нигерије. Укратко, јасно разумевање разлика између прегледаних студија, теоретског оквира и концептуалног оквира доноси боље смернице у погледу психолошких ефеката сајбербезбедносних повреда података код особа из Нигерије.

Ова студија открива да постоје сајбербезбедносне повреде података које могу да доведу до општих кривичних дела и психолошке несигурности у Нигерији. Постоје индиције да безбедносне повреде података могу да имају значајне психолошке ефекте на појединачне жртве у Нигерији.

Ова студија, стога, закључује да дуготрајна изложеност штетном садржају са интернета може да утиче на когнитивне способности, укључујући решавање проблема и доношење одлука. Жртве могу да имају проблема са концентрацијом или доношењем паметних одлука, што може потенцијално да утиче на њихов капацитет да се носе са својим свакодневним обавезама. Даље, напади на интернету могу да доведу до проблема са поверењем, што наводи људе да изгубе веру у друге људе и интернет платформе, те стога да оклевају да користе друштвене медије или да комуницирају путем интернета. Ово оклевање може да доведе до њихове даље изолације од мрежа подршке.

Литература / References

1. Baum A, Newman S, Wienman J, West R, McManus C, editors. Cambridge handbook of psychology, health and medicine. Cambridge: Cambridge University Press; 1997. 660p.
2. Kohli R, Melville NP. Digital innovation: a review and synthesis. Inform. Syst. 2019; 29(1):200–23. https://doi.org/10.1111/isj.12193
3. Ahmad M, Murray J. Understanding the connect between digitalisation, sustainability and performance of an organisation. IJBEX. 2019; 17(1):83–96. https://doi.org/10.1504/IJBEX.2019.10017927
4. Canetti D, Gross M, Waismel-Manor I, Levanon A. How cyber-attacks terrorize: cortisol and personal insecurity jump in the wake of cyber-attacks. Cyberpsychology Behavior, and Social Networking. 2017; 20(1):72–7. https://doi.org/10.1089/cyber.2016.0338
5. Verizon. 2018 Data Breach Investigations Report. 11th ed. [Internet]. New York (NY): Verizon; 2018 [cited 2025 May 10]. Available from: https://www.verizon.com/business/resources/reports/DBIR_2018_Report.pdf
6. Minei, E., Matusitz, J. Cyberterrorist messages and their effects on targets: A qualitative analysis. Journal of Human Behaviour in the Social Environment, 2011; 21 (8): 995–1019. https://doi.org/10.1080/10911359.2011.588569
7. Hadlington L. The “Human Factor” in Cybersecurity: Exploring the Accidental Insider. In: McAlaney J, Frumkin L, Benson V, editors. Psychological and Behavioral Examinations in Cyber Security [Internet]. Hershey (PA): IGI Global; 2018. p. 46–63. https://doi.org/10.4018/978-1-5225-4053-3.ch003
8. Nobles C. Botching Human Factors in Cybersecurity in Business Organizations. HOLISTICA – Journal of Business and Public Administration. Sciendo, 2018; 9(3): 71–88. https://doi.org/10.2478/hjbpa-2018-0024
9. Nobles C. Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. HOLISTICA – Journal of Business and Public Administration. 2022; 13(1):49–72. https://doi.org/10.2478/hjbpa-2022-0003
10. Nobles C. Establishing human factors programs to mitigate blind spots in cybersecurity [Internet]. MWAIS 2019 Proceedings. 2019;22. [cited 2025 May 10]. Available from: https://aisel.aisnet.org/mwais2019/22.
11. Judge K. Who is Helping Cybercrime Victims? [Internet]. Baltimore (MD): US CyberSecurity Magazine. Summer 2021. [cited 2025 May 10]. Available from: https://www.uscybersecurity.net/csmag/who-is-helping-cybercrime-victims/.
12. Palatty NJ. 90+ Cyber Crime Statistics 2025: Cost, Industries & Trends [Internet]. New Delhi (IN): Astra Security; 2025 Jun 16 [cited 2025 Jun 17]. Available from: https://www.getastra.com/blog/security-audit/cyber-crime-statistics/#2_Cyber_Crime_Statistics_By_Year.
13. Vujinović I. More than 70 cybercrime statistics – a $6 trillion problem [Internet]. DataProt; 2023 [cited 2025 May 10]. Available from: https://dataprot.net/statistics/cybercrime-statistics/.
14. Morgan S. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics [Internet]. Sausalito (CA): Cybersecurity Ventures; 2023 [cited 2025 May 10]. Available from: https://cybersecurityventures.com/cybersecurity-almanac-2023/
15. Bada M, Nurse JRC. The social and psychological impact of cyberattacks. In: Benson V, McAlaney J, editors. Emerging Cyber Threats and Cognitive Vulnerabilities [Internet]. London (UK): Academic Press; 2019. p. 73–92. https://doi.org/10.1016/B978-0-12-816203-3.00004-6
16. Schelenz L, Schopp K. Digitalization in Africa: Interdisciplinary Perspectives on Technology, Development, and Justice [Internet]. International Journal of Digital Society. 2018; 9(4):1412–20. [cited 2025 May 10]. Available from: https://infonomics-society.org/wp-content/uploads/ijds/published-papers/volume-9-2018/Digitalization-in-Africa.pdf.
17. García-Peñalvo FJ, Conde MA, Alier M, Casañ MJ. Tackling the digitalization challenge: how to benefit from digitalization in practice. International Journal of Information Systems and Project Management. 2017; 5(1):63–77. https://doi.org/10.12821/ijispm.

18. Gorenšek T, Kohont A. Conceptualization of digitalization: Opportunities and challenges for organizations in the Euro-Mediterranean area [Internet]. International Journal of Euro-Mediterranean Studies. 2019; 12(2):93–115. [cited 2025 May 10]. Available from: https://emuni.si/wp-content/uploads/2020/01/IJEMS-2-2019_93–115.pdf.
19. Christen M, Gordijn B, Weber K, van de Poel I, Yaghmaei E. A review of value-conflicts in cybersecurity: an assessment based on quantitative and qualitative literature analysis [Internet]. Orbit Journal. An Online Journal for Responsible Research and Innovation in ICT. 2017; 1(1):1–19. https://doi.org/10.29297/orbit.v1i1.28.
20. Weber K, Kleine N. Cybersecurity in health care. In: Christen M, Gordijn B, Loi M, editors. The ethics of cybersecurity [Internet]. Cham (CH): Springer; 2020. p. 111–30. https://doi.org/10.1007/978-3-030-29053-5_7
21. Beauchamp, T. L., Childress, J. F. Principles of Biomedical Ethics. Am J Bioeth. 2019; 19(11):9–12. https://doi.org/10.1080/15265161.2019.1665402
22. Rogers RW. A protection motivation theory of fear appeals and attitude change. J Psychol. 1975; 91(1):93–114. https://doi.org/10.1080/00223980.1975.9915803
23. Burrell DN. Understanding cognitive and behavioral psychological factors that lead to cybersecurity breaches in healthcare [Internet]. RAIS J Soc Sci. 2024; 8(2):43–53. [cited 2025 May 10]. Available from: https://journal.rais.education/index.php/raiss/article/view/234
24. Wall JD, Buche MW. To Fear or Not to Fear? A Critical Review and Analysis of Fear Appeals in the Information Security Context. CAIS. 2017; 41(1):277–300. https://doi.org/10.17705/1CAIS.04113
25. Cohen G. Memory. In: Hayes N, editor. Introduction to Psychology [Internet]. 1st ed. Hove (UK): Psychology Press; 1991. p. 570–620. [cited 2025 May 10]. Available from: https://www.taylorfrancis.com/chapters/edit/10.4324/9781315785127-12/memory-gillian-cohenp
26. Triplett WJ. Addressing human factors in cybersecurity leadership. Journal of Cybersecurity and Privacy. 2022; 2(3):573–86. https://doi.org/10.3390/jcp2030029

Примљено / Received
13. 5. 2025.
Ревидирано / Revised
10. 6. 2025.
Прихваћено / Accepted
11. 6. 2025.

Кореспонденција / Correspondence

Сулејман Тојин – Sulaiman Toyin
toyinsulaiman8@gmail.com