International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 10 Issue 3, March, 2021, Impact Factor: 7.751

The Impact of Changing Technologies on Business Data Security: The Benefits and Challenges in the 21st Century

Dr. Erbynn Sefakor Bedzo

Aspen University:CAP-799, December 20, 2020

ABSTRACT

The study's research objective is to conduct a content analysis of business, journal, government, and other relevant publications to determine how changing technologies will impact business data security. The study also intends to examine the benefits of new technologies and their challenges in the 21st Century. The specific goals in the study include those of: (1) examining the current environment of new and rapidly advancing technologies; (2) examine the impact of new and changing technologies on business data security; and (3) examine the benefits and challenges that are associated with new technologies and business data security. Research has shown that new technologies are increasing, and the result is that business data security is facing new and unprecedented challenges. It is essential to identify the challenges of new technologies and to examine how businesses can best respond to the growth of threats to their data security.

INTRODUCTION

Introduction to the Study

According to Bissell et al. (2020), eighty-two percent of business leaders revealed spending over twenty percent of the company's information technology budget on advanced cyber-security technology investments. New and emerging technologies make cyber-security a key concern for business organizations because new and emerging technologies are presenting new challenges and opportunities for businesses. An examination of the sources of the committed cyberattacks revealed that nearly one-half of all security breaches are not direct, but rather are indirect as the bad actors make weak links in the business supply chain or ecosystem their targets (Bissel et al., 2020). There are estimations that indirect and direct cyberattacks will experience a twenty percent increase in 2021 (Bissel et al., 2020).

According to Maddox (2020), the top ten new and emerging technologies include those of: (1) artificial intelligence; (2) 5G; (2) IoT; (3) serverless computing; (4) biometrics; (6) augmented reality and virtual reality; (7) blockchain; (8) robotics; (9) natural language processing; and (10) quantum computing. Artificial intelligence or AI is algorithms that have been programmed to automatically parse information and apply knowledge and it the greatest force in all of the emerging technologies and is inclusive of sales applications and security for businesses (Maddox, 2020). 5G increases the power of wireless and computing connections by using power consumption that is intelligent and high device density and will support smart cities, augmented reality, and enable vehicles to be connected (Maddox, 2020). IoT or the Internet of Things works to combine information from connected devices and enable system analytics (Maddox, 2020). Serverless computing enables applications to be built and scaled in almost real-time for companies to help them respond to demand (Maddox, 2020). Biometrics uses authentication that is seamless, such as scanning the individual's face, pupil, or thumbprint (Maddox, 2020). Augmented and virtual reality will bring about transformation in the way that individuals engage with data, machines, and one another (Maddox, 2020). Blockchain technology increases transactions' security by managing challenges related to the supply chain and other data (Maddox, 2020). Robotics is being used to deliver and bring about changes in businesses and homes in a physical and virtual way (Maddox, 2020). Finally, quantum computing is reported as crucial to leveraging artificial intelligence power and machine learning (Maddox, 2020).

The entire globe is undergoing "a great informational change conducted by reshaping and redefining technological processes. The rapid growth of information technology (IT) has evolved worldwide security issues" (Mihaela, 2020, p. 352). The result is that information systems will have to be restructured, and companies will be forced to adopt strategies that are new in order to respond to the information security challenges (Mihaela, 2020). Although there are many benefits to the new technologies, including the quickness at which financial information can be presented and the benefits of automation for transactions and improvements in accuracy, there are higher risks of data being exposed, particularly corporate data that is sensitive (Mihaela, 2020). New and disruptive technologies have the potential to have a huge impact

on information security between 2020 and 2030 as quantum computing takes hold, along with wireless electricity, new interfaces, and as new communication protocols are developed and as new tools are used for productivity that is collaborative, such as Zoom meetings, new threats will be present (PWC, 2020). According to one cybersecurity expert, "smartphones are basically small PCs now, so all the current threats on a PC are simply transferred to the phone" (PWC, 2020, p. 10).

Research Objective

The objective of the research in this study includes examining the current environment of new and rapidly advancing technologies, examining the impact of new and changing technologies on business data security, and examining the benefits and challenges that are associated with new technologies and business data security. Toward that end, a content analysis of previously published studies will be conducted and will include a review of publications contained in such as business journals, various business publications, publications of the government, and any other published material that will contribute to the depth of the study. Included in the material reviewed will be business case studies of problems related to data security and how those situations were addressed.

Research Questions

The research questions that will be addressed in this study include those asking the following stated questions:

(1) What new and changing technologies exist or are expected to be ready for use in the near future?
(2) What benefits and challenges are associated with new technologies and business data security?
(3) How can businesses prepare their employees and security professionals to meet the challenge of data security presented by new and emerging technologies?

Statement of the Problem

According to Tawalbeh et al. (2020), security and privacy present the most significant challenges for the Internet of Things (IoT). IoT includes all types of connected devices linked across the Internet, whether they are wireless or wired devices. Industrial applications have been enabled across the Internet for business purposes for quite some time and assist businesses in acquiring and maintaining a competitive advantage. However, because of the "excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services" (Tawalbeh et al., 2020, p. 2). Organizations must ensure they use scanning and monitoring tools to ensure security threats are avoided. However, according to Khan et al. (2019), with the technological advances that are taking place, such as the 5G network, the attacks on business networks have increased in terms of their "complexity and strength" (p. 1). The result is that addressing those risks and ensuring sabotage is prevented has become a serious challenge (p. 1). According to Mihaela (2020), the use of information technology and particularly new technologies present more significant challenges in terms of data exposure risks being higher, sensitive corporate data is at risk, and challenges related to electronic fraud, phishing, and other risks increase. However, simultaneously, the Internet provides excellent benefits for businesses, yet, as digitization grows, so do the transformations wrought by new technologies. According to Mihaela (2020). "cybersecurity threats are not slowing down, and they have no boundaries" (p. 354). Moreover, the threats are increasingly becoming more complex and occurring more frequently at higher numbers in terms of their occurrence (Mihaela, 2020). For example, the WannaCry attack and the Not Petya attack resulted in serious repercussions, and growth has been seen in the use of skimming devices placed of ATM machines and other card reading stations where the information of users is being stolen, and fraudulent transactions are taking place (Mihaela, 2020). Not only are businesses negatively affected by the occurrence of data attacks and data breaches, but the entire market is also impacted, along with governments and other statutory bodies (Mihaela, 2020).

Background to the Study

According to Lange and Kettani (2019), across the history of humans, it has been the individuals and societies who have adapted the quickest to any shifts in technology that have managed to not only survive but to excel and those who fail to make the necessary adaptations "have fallen by the wayside" (p. 1002). In fact, there have historically been civilizations as well as large dynasties that have fallen because they lacked in the area of innovation (Lange and Kettani, 2019). The astronomical speed at which technology is being developed in contemporary times makes it very challenging to realize an edge technologically, and as the world grows more and more dependent on technology, the ability to stay abreast of technological development is essential. However, it is just as important to ensure that businesses can protect their data and the privacy of their clients. Research that was conducted and reported by Hewlett Packard found that three-fourths of IoT devices have vulnerabilities related to security (Lange and Kettani, 2019). However, the rate of speed at which many manufacturers and other businesses are adopting the technology may be to blame. However, despite the security risks presented by the new technologies, there are also many benefits (Lange and Kettani, 2019).

Tawalbeh et al. (2020) revealed that the Internet of Things (IoT) is used in various ways and for many purposes, including those of transportation, communication, education, as well as business development. The hyper connectivity concept was introduced by the Internet of Things, which works to enable communication between individuals, organizations, and with one another from locations that are remote with the ability to do so effortlessly (Tawalbeh et al., 2020). The Internet of Things is used in bringing about improvement in the activities of supply chains. Although IoT has improved individual's lifestyle with services that are automated, at the same time, the security and privacy challenges have increased, and by failing to change passwords and update devices, cybersecurity risks present along with the IoT system being at risk for malicious applications and loss of the sensitive data of the system (Tawalbeh et al., 2020).

However, it is necessary for business and security professionals to understand the dangers of IoT to the system when there are weak policies and protocols in place, making the system at risk to cyberattacks. Those considerations are especially relevant since hackers have worked in the development of various types of malware, as well as using phishing techniques that stimulate the sharing of data that is sensitive by employees (Tawalbeh et al., 2020). Failure to ensure data security can result in personal devices and workstations in the business being at risk to high-profile attacks; however, where the security experts conduct assessments of the potential for cyber threats in an accurate manner, they have a chance to develop mechanisms that are efficient in protecting from, prevention of, and neutralizing cyber threats (Tawalbeh et al., 2020).

Each day there are emerging and new technologies, or existing technologies being changed, and for example, the 5G network, which is

> "expected to play an essential role in the IoT systems and applications. It is getting the researchers' attention and curiosity about the possible security and privacy risks, with its high frequency and bandwidth. Yet, the short wavelength imposes a change in the infrastructure, hence the need for more base stations to cover the same area covered by other wireless technology. This new structure imposes more threats, such as fake base stations. It is essential to understand the security risks and potential solutions" (Tawalbeh et al., 2020, p. 2).

According to Lohrmann (2020), there are various trends that have been identified as of December 2020 that are likely to impact business cybersecurity in 2021, and the first of which is related to the great impacts on security for businesses due to the many employees who are working from home due to COVID-19. Lohrmann (2020) stated that as more attacks happen on the networks and computers of people's homes, it is expected that bad actors will make use of homes as types of criminal hubs as they take advantage of systems that are unpatched and any weakness to architecture businesses will likewise be impacted because the employees who are working from home. Secondly, Lohrmann (2020) stated that as the industry and individuals alike are rushing to put everything in the cloud, there will be challenges related to holes in security, outages, and misconfigurations.

As the security industry experiences higher levels of growth along with new products, mergers, and acquisitions occurring in early 2021, there will be a growth in complexity issues in networks, problems with integration, and cyber teams will become overwhelmed (Lohrmann, 2020). Privacy is going to have issues and may become a complete mess, as users revolt and new laws are enacted, as well as failures in self-regulation and overall confusion (Lohrmann, 2020). Multi-factor authentication and identity will be issues as passwords are done away and overall create some disturbances in security. It is expected that ransomware will grow worse, characterized by new problems and data being stolen before it is even encrypted as well as malware packaging and additional threats with organizations being specifically targeted (Lohrmann, 2020).

Although 5G is being touted as remarkable, there will be many vulnerabilities with the growth of the technology. Moreover, Advanced Persistent Threats (APT) type attacks will be launched by criminal networks, as criminals purchase access into the corporate networks that are vulnerable (Lohrmann, 2020). Finally, new roles will be played by cryptocurrencies and criminals changing often in order to hide their advantages, and with the growth of digital transformation, many cybersecurity plans will implode with the growth in challenges related to security (Lohrmann, 2020).

Research Methodology

The research methodology that will be utilized in the present study is a qualitative content analysis of previously published research, including information contained in business journals, business publications, as well as other publications that shed light on the challenges and risks faced by businesses with the new and emerging technologies in relation to ensuring data security.

Organization of the Study

Chapter one has introduced the research in the study and has stated the research objective, research questions, statement of the problem, and the background of the study. The research methodology that will be used in the study has also been briefly described. Chapter two of the study will represent the largest part of the study and will review the information contained in business journals, business publications, and other various publications that will inform the study, representing the content that will be analyzed in the study. Chapter three will present a full account of the methodology of the study, and chapter four will present the analysis of the content reviewed in chapter two of the study. Chapter five will present the discussion, conclusions, and recommendations of the study.

LITERATURE REVIEW

Information Security Trends

According to a PriceWaterhouseCoopers (PWC) (2020) report, although information security has been a topic for some time now, it is, in fact, "an emerging sector that is undergoing significant change" (p. 2). The market research that is available does not yield a consensus on the exact size of the market of IT security; however, it is believed to be worth between four and five billion each year. Between 2020 and 2030, the requirements for information security will be affected by many factors at the macro-level, including such as climate change, globalization, evolving demographics, and regulation, all of which will serve to present risks and opportunities for business organizations as they cope with issues related to information security (PWC, 2020). Historically, information security has been held to include three specific components, including people, processes, and technology; however, organizations increasingly realize that people and processes are components that have been vastly overlooked in developing information security (PWC, 2020).

According to PWC (2020), research has identified seven specific key trends, all of which are interrelated, and that will serve to drive changes in the area of information security. The first three of the trends are related to technology changes, while the other three are related to the changes in the patterns of how technology is used by individuals and on the Internet. The seventh issue is identity and trust, which are interlinked with the other six trends (PWC, 2020). The first trends of infrastructure revolution are related to the following: (1) the increases in the penetration of wireless networks and broadband that is high speed; (2) the centralization of computing resources along with cloud computing being adopted widely; (3) the proliferation of the internet protocol devices that are connected and growing in terms of functionality; (4) the improvements of the infrastructure for global information and communications technology with increases in outsourcing; (5) the convergence of devices along with software components increased modularization; (6) the lines between the personal and work due to work-from-home remote working and the bring your own devices approach in information technology; and (7) user interface evolution and disruptive technologies emergence (PWC, 2020).

The second trend of data explosion will result in sensitive data being shared on a greater level between individuals and organizations, along with increases that are significant in visual data. As well, there are more individuals connected globally, and devices have more highly automated traffic. Devices are being multiplied, as are applications that generate traffic, and there is a need for data to be increasingly classified (PWC, 2020). The third trend of a world that is always connected has increased the level of connectivity between individuals due to social media networking along with other platforms requiring that devices be seamlessly connected. As well, there is a growth in information connectivity and mining of data along with increases in Critical National Infrastructure and connectivity for public services (PWC, 2020). The fourth trend, of the future finance trends, is characterized by levels of mobile and electronic commerce that are growing, including mobile banking as new banking models are being developed, growth occurring in new models for payment, and digital cash emerging (PWC, 2020).

The fifth trend of tougher standards and regulation is characterized by a growth in regulation, particularly related to privacy, an increase in information security standards, with net neutrality and globalization being opposing forces in the area of standardization and regulation (PWC, 2020). The sixth trend is one characterized by multiple internets and driving censorship that is greater along with new regional and state internets having political motivations. However, some internets are becoming more secure, and social networks are becoming closed, while paid content is experiencing growth (PWC, 2020). The seventh trend is related to new trust models and identity to address the presently used concepts, which are in decline. Identity will gain importance in relation to information-based security, all of which has resulted in the need to develop new models, devices, and infrastructure to address security (PWC, 2020). All of this information is shown in the following figure.

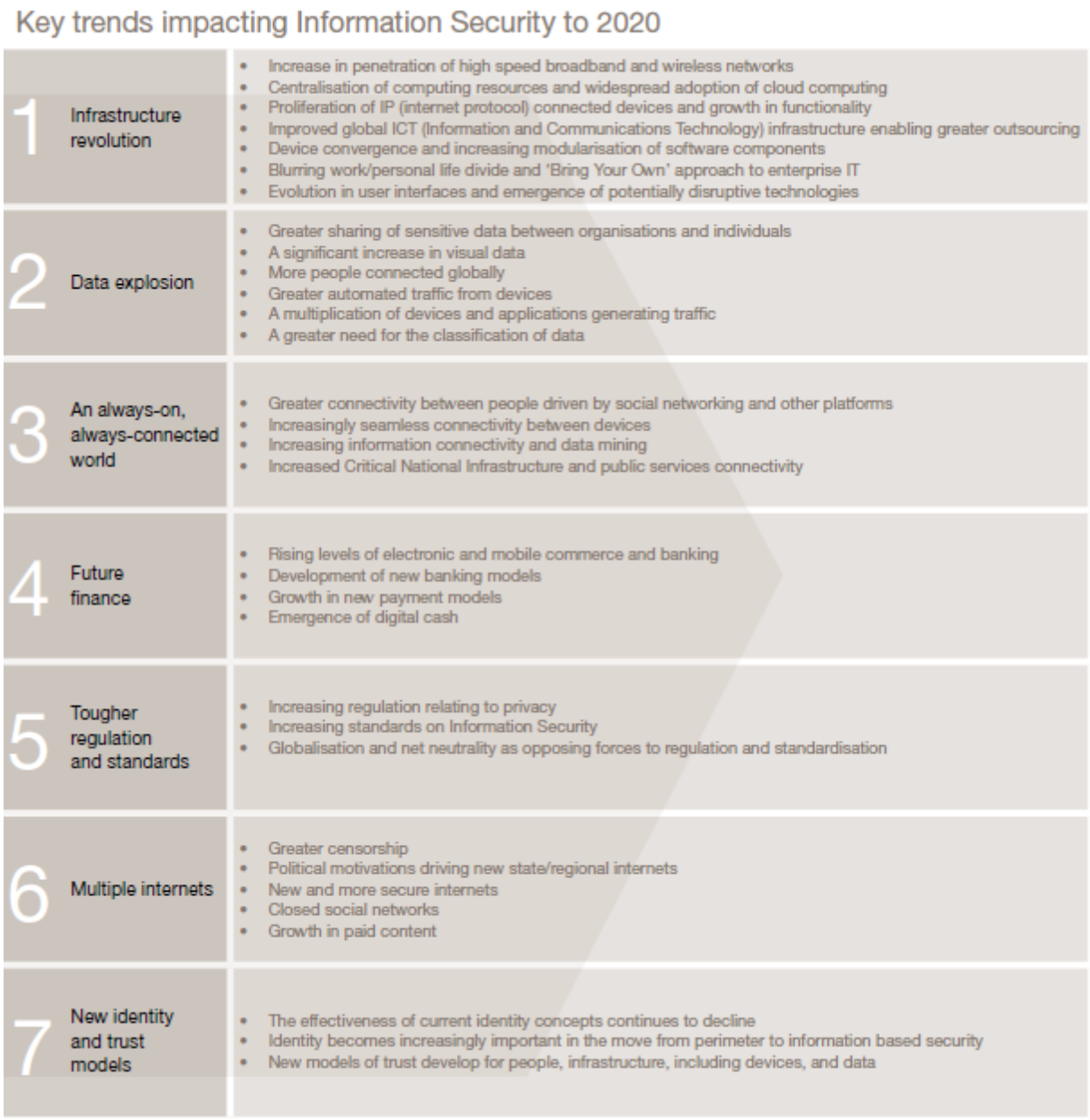

Figure 1. Information Security Trends 2020 and Beyond (Source: PWC, 2020)

According to PWC (2020), research that has been conducted has indicated that information security professionals, businesses, and other stakeholders must take an approach that is proactive due to the growth in the complexity and the number of threats. It will be essential that organizations make certain their approaches to information security are not only holistic in nature but are such that they take into consideration the processes, people, and technology aspects of information security. The approaches will need to be of the type that can adapt rapidly to the shift in threats and new technology, but that additionally meet the standards and regulations required (PWC, 2020). However, it will be crucial "that organizations also focus on aspects of information security that are not necessarily driven by regulation and standards, for example, protecting commercially sensitive information or intellectual property" (PWC, 2020, p. 6).

New Technologies Challenges and Benefits

Cloud computing technology

As the very building blocks of technological communication are undergoing quick evolution, the change is evident as computers and televisions are connected via Wi-Fi without the need for cables, and broadband access is becoming faster (PWC, 2020). However, the implications for information security are quite significant. As computing resources become more centralized, reducing costs and improving functionality and services, businesses have for a large part been far too

slow to adopt information security for the cloud to address concerns about security. While the benefits of cloud computing are being enjoyed by businesses across the globe, the security concerns are those related to service reliability and availability, the privacy of data, classification of data, assets, and the need for compliance with regulatory requirements (PWC, 2020). According to Tony Dyhouse with Digital Systems Knowledge Transfer Network, "the driving force behind the cloud is economics. You simply get better economics from one size fits all. Security concerns, however, are the key blocker" (PWC, 2020, p. 9). The concept of cloud computing is stated to be:

> "the provision of IT as a service is such that storage, processes, software and even security are all provided as services. This has significant implications for organizations that adopt this model, but also for the IT and Information Security Industries which may need to adapt to this new ecosystem with new business models" (PWC, 2020, p. 9).

According to Ahmed and Hossain (2014), there are three particularly scenarios that are sensitive in the area of cloud computing, including: (1) personal sensitive data transmission that goes to the cloud server; (2) data that is transmitted from the cloud server to the computer of the clients; and (3) personal data of the client that is stored in the cloud server. Each of these areas is particularly prone to breaches of security (Ahmed & Hossain, 2014). Despite the challenges to cloud computing, it is reported as the fastest growing technology, although there are huge business concerns when using these technologies (Islam, 2017). The cloud computing architecture is shown in the following figure.

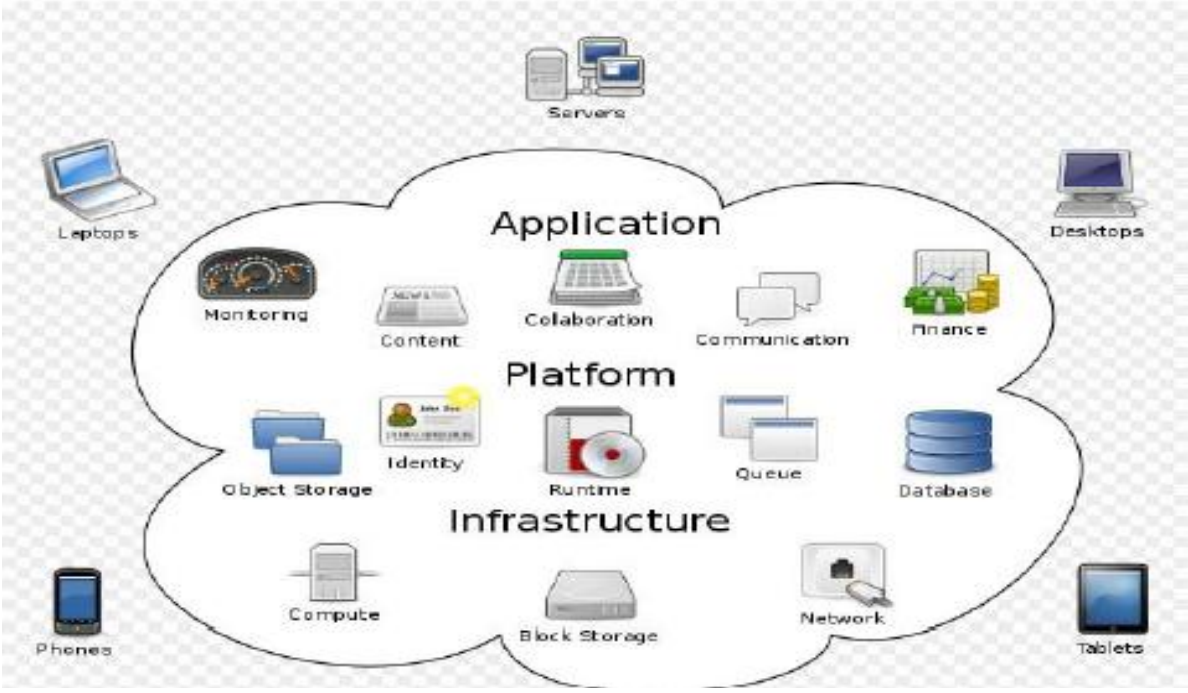

Figure 2. Cloud Computing Architecture (Source: Islam, 2017)

There are three types of services offered by cloud computing, and the first of which is Infrastructure as a Service (IaaS), which is a key service provision of the cloud offering many hardware resources, including a memory network, CPU, and others, which may be leased or rented by the user (Islam, 2017). Key examples of providers of cloud services are those of Google, Amazon, Microsoft, IBM, and Salesforce.com (Islam, 2017). The cloud offers virtualization and means that cloud consumers are able to meet any growth in the demand for resources. Virtualization is reported to be used very extensively in the IaaS cloud for the purpose of integrating or decomposing the physical resources and does so in an ad hoc manner and offers the ability of users to negate high investments for resources while enabling them to both manage and control the applications and software (Islam, 2017). The second type of cloud platform is Platform as a Service (PaaS). PaaS is described as a

> "development platform supporting the full 'software lifecycle' which allows cloud consumers to develop cloud services, along with applications directly on the PaaS cloud, it provides all services for developing, modifying, testing and running applications in a cloud environment without buying software" which is a huge benefit for those who use it (Islam, 2017, p. 225).

When using the PaaS, the user has no control over the operating system but however, can access development tools for the webserver, database, and others (Islam, 2017). The third type of cloud computing is 'Software as a Service' (SaaS), which enables the organization to run software applications across the Internet without having to install the software on its own computers, which saves money and time (Islam, 2017). Examples of SaaS include such as Microsoft Office 360, which enables multiple users to use the application through the cloud SaaS. However, cloud users do not possess any control over this type of service. Cloud computing has the benefits of achieving "economies of scale and optimization in terms of speed, security, availability, disaster recovery, and maintenance" (Islam, 2017, p. 225).

Specific benefits of cloud computing include, in addition to savings in terms of costs, the saving of time by not being required to install the software on every computer in the organization, and in the area of flexibility and scalability as the SaaS can be used by startups and larger corporations alike (Islam, 2017). Finally, backup and recovery are assisted because all of the company's data is effectively stored in the cloud, meaning that recovery of the information is very easy compared to if the information was stored on the organization's computing devices. Cloud computing helps the company maximize its resources by bringing about a reduction in the burden of needed information technology resources. Moreover, because the cloud can be accessed from mobile devices from home or work, then all the files can be accessed from anywhere, regardless of where the employees are (Islam, 2017). Another benefit of cloud computing is related to the ability to share applications and architectures among many users as the cloud works in a shared and distributed mode (Islam, 2017). Cloud computing additionally has the benefit of customization because it is a platform that allows for modification according to the needs and the ability to both create and amend applications so they can "address a diversity of tasks and challenges" (Islam, 2017, p. 226). Another benefit of cloud computing is the level of collaboration that can take place as "major projects of applications are delivering by the effort of multiple groups of employees working together" (Islam, 2017, p. 226). Cloud computing makes the provision of a method of working between people that is convenient as they work on common applications or projects and do so together in an effective manner (Islam, 2017). Additionally, cloud computing works in delivering services that are new such as those which multi-national companies such as Google, IBM, Amazon, Microsoft, and others provide, which means the companies can deliver any new product or application easily at the time it is released, and everyone is able to immediately access it (Islam, 2017). The improvements offered by cloud computing include efficiency, scalability, and flexibility, all while bringing about cost reductions and making the provision of the capacity to make certain of business continuity even in time of disruption that has not been anticipated (Islam, 2017). However, just as there are benefits of cloud computing, there are also challenges, which will be addressed in the following section.

According to Islam (2017), "security of data is the most tedious work in cloud computing. According to a survey…more than 70% of Chief Technical Officers believed the primary reason for not using cloud computing services is that of data security and privacy concerns" (p. 226). Particularly, the smaller organizations are those more hesitant to use cloud computing due to security issues as they are not prepared to simply get rid of their infrastructure and move immediately to the cloud (Islam, 2017). Data privacy is the primary concern, and organizations are hesitant to place their company's valuable data in the cloud; as well there is a lack of information among consumers concerning the location of the data and its transfer and other cloud operations. Consumers tend to have concerns in relation to the following:

1. Which are the other organizations sharing services?
2. How the creation and deletion of files are taking place?
3. What about backup of data?
4. Which type of consumers can access data?
5. What is the location of the data? (Islam, 2017, p. 226).

Data confidentiality is another huge concern with cloud computing and is linked to data privacy or making certain that the data is visible to just the users who are authorized. However, it is quite difficult because of the multi-tenancy properties and virtualization when multiple consumers are simultaneously sharing the software and hardware in a network that is distributed (Islam, 2017). The service provider is responsible for ensuring confidentiality, and generally, encryption is used as the most common of all solutions. There are various asymmetric and symmetric algorithms that are available to ensure data confidentiality; although decryption and encryption are the solutions to this issue, yet many questions remain, including those stated as follows:

1. Where are the encryption and decryption taking place (client side or cloud side)?
2. How can a search for data be done in an encrypted form?
3. What are the threats while transferring data from client to cloud?
4. Any misuse of data by the service provider?
5. Any misuse of keys by the service provider? (Islam, 2017, p. 226).

Another concern is that is data remanence or data that is stored in the cloud and which must be deleted following its lifecycle or the reformatting and recycling of the memory. However, when storage media is reformatted, it does not result in the removal of the data that was previously written, as it can be recovered or accessed from the media at a later time (Islam, 2017). There is not yet a standard that is clear on the recycling of the storage media, and the result is that "data remanence makes difficult the vacation of hardware resources from the cloud. Most consumers are unknown to allotted resources and storage space, due to the issue consumers are locked in one service provider" (Islam, 2017, p. 226). However, there are some different techniques that have been specifically developed to counter the data remanence, including sanitizing, purging, cleaning, and destruction, as well as degaussing, overwriting, media destruction, and encryption (Islam, 2017). Another key challenge of cloud computing is related to data integrity, and specifically that of ensuring that no data is lost and that it is preserved and protected from any modification by users who are not authorized (Islam, 2017). There are many organizations that share the same platform or application, and due to multi-tenancy, many consumers may share data that an unauthorized user might impact and result in failure of the integrity of the data. Another challenge is related to the transmission of data; in that, the majority of the time, the data will be

> "transferring between consumer and cloud. Initially, data is sent from the client site to the cloud; data is returned from the cloud to the client after queries. Encryption is used to provide protection during the transmission of data. Most of the time, data is transferred without encryption" because of the required time for encrypting and decrypting the data (Islam, 2017, p. 227).

The result is that the attacker might, during the transfer of the data, work to trace the communication, and then disrupt the transfer of data and misuse the data (Islam, 2017). However, a homomorphic algorithm enables data to be processed in a form that is encrypted; however, there is still a chance that there will be an interruption in the data transfer or that the data may be changed during the transfer. Another serious issue may arise due to data breaches, particularly since the environment of the cloud is shared among multiple organizations and users globally, should any problem arise on the cloud, then the sensitive data or the organizations and users may be exposed. For example, when customers are using the various applications on the virtual machines, then the sharing of the same database could occur, and the data could be corrupted, affecting all of the others who are sharing that database (Islam, 2017).

Artificial Intelligence (AI) and Business Data Security

Artificial intelligence was reported by Lazic (2019) to offer many benefits to businesses in protecting their data and ensuring data security. In just 2016, more than three billion was invested in nearly 300 cybersecurity startups, with those specializing in machine learning and AI being the companies to receive the largest of all investments. It is estimated that "machine learning in cybersecurity will boost spending in big data intelligence and analytics, reaching as much as US$96 billion by 2021" (Lazic, 2019, p. 1). The buyers of AI and machine learning technology include those particularly vulnerable to be on the receiving end of cyberattacks, including banking, defense, and government; however, due to the exceptionally strong interest in the use of AI and machine learning for detecting threats, it is likely that all types of businesses will become interested in acquiring the technology (Lazic, 2019). Cyberattacks often involve huge economic damage where there is extortion for payments that are anonymous in the form of Bitcoin, and when any type of critical infrastructure is affected, then the rule of law along with international security comes under threat. However, businesses operating in the aviation and shipping sectors are also at a huge risk because it has been shown that the ship tracking systems can be hacked through ISPs and the AIS data altered to change the information about the ship location and other information resulting in loss of cargo and even loss of the lives of employees if the ship becomes wrecked or left flailing in the open seas (Lazic, 2019). However, machine learning, which is one component of artificial intelligence, has benefits, including the ability to examine the information as it is constantly learning and improving its strategies and functions across time. As AI learns more about the normal behavior of users, it develops the capacity to identify very small variations from patterns, and for example, should an employee login from Hong Kong rather than their usual location of New York, then a threat would be identified (Lazic, 2019). Artificial intelligence then has the capacity to use that information to improve and enhance its own functions and fine-tune its strategies, so they are improved. The importance of artificial intelligence is that if a human being were asked to filter such huge amounts of information, including computer usage, logins, and the systems infrastructure, it would be impossible for them to keep up. However, artificial intelligence has the capacity to attend to it all and to do so "quickly, effortlessly, and on a 24/7/365 basis" (Lazic, 2019, p. 3).

Businesses in the private sector, along with larger corporations, have already begun to deploy artificial intelligence systems, and it is noted that even some governments globally are using artificial intelligence. The reason is clear when the benefits are considered that include the savings of money and time since structured data can be examined rapidly, along with artificial intelligence' ability to read comprehensively, learn unstructured data, including that of words, phrases, and statistics (Lazic, 2019). The real benefits of artificial intelligence for protecting business data security is revealed in the following statistics: (1) 35 percent of all attacks are fileless, which means they are immune to any anti-virus programs; (2)

40 percent of all industrial business type sites have at least one if not more connections to the Internet; (3) 49 percent of companies who were on the receiving end of attacks that were significant were attacked again and successfully so within twelve months of the first attack; (4) 84 percent of industrial business sites have one or more device that can be accessed remotely (Lazic, 2019). However, despite the promise of artificial intelligence and the fact that it is the hottest and latest new trend, there are those who disagree with relying on artificial intelligence because even with the use of artificial intelligence, there are still some loopholes existing, and hackers are always working on figuring out how it is they can commit data attacks (Lazic, 2019). However, artificial intelligence does have the capacity to simply "sit back, collect data, and wait for a hacker to get messy" (Lazic, 2019, p. 3). In order to integrate artificial intelligence effectively into a businesses' technology, there must be a great deal of planning followed by training and preparation of the business systems and employees to ensure it is used to the full advantage. However, artificial intelligence can be integrated with a businesses' existing cybersecurity as follows:

1. Creating more accurate, biometric-based login techniques
2. Detecting threats and malicious activities using predictive analytics
3. Enhancing learning and analysis through natural language processing
4. Securing conditional authentication and access (Lazic, 2019, p. 4).

The benefits that companies are realizing from the use of artificial intelligence include that artificial intelligence has lowered the costs of detecting and responding to breaches, and artificial intelligence enables organizations to respond faster to any data breaches (Lazic, 2019). According to Lazic (2019), the reasons for using artificial intelligence for business data security are compelling and include the following:

- Three out of four executives say that using AI allows their organization to respond faster to breaches.
- Three in five firms say that using AI improves the accuracy and efficiency of cyber analysts.
- A majority of organizations say that AI lowers the cost of detecting and responding to breaches by 12%, on average, building a roadmap for implementing AI in cybersecurity (Lazic, 2019, p. 6).

Specific actions that must be taken to effectively institute the use of artificial intelligence includes the following: (1) data sources should be identified and platforms created so as to operationalize the artificial intelligence and may involve either building or buying a data platform that makes provision of the data in a consolidated view; (2) it is important to ensure the selection of the right use cases so that benefits are accelerated and maximized, and importantly, Lazic (2019) identified five specific use cases that yielded the highest benefits and the less complexity in implementation, including those of: (1) detection of malware, intrusion, risk scoring for network operational technology; (2) detection of fraud for IT and behavioral analysis for the user and machine for IoT; (3) external collaboration will enhance the threat intelligence, and could be collaboration across crowd-sourced planforms so that the organization is kept abreast of the new threats that are presenting via collaboration with other security professionals; (4) it is necessary to ensure the deployment of security, orchestration, automation, and response, also known as SOAR so that security management can be improved since SOAR makes AI use more effective by supporting response that is rapid to any threats that are detected; (5) training cyber analysts to be prepared for the use of artificial intelligence and ensuring they possess the knowledge of the key processes of AI; and (6) finally, necessary is the installation of AI governance in the cybersecurity of the organization so that long-term improvement can be realized (Lazic, 2019).

5G Networks and Technologies and Business Data Security

According to Ahmad et al. (2019), 5G wireless networks will make provision of data rates that are extremely high with much higher coverage. The benefits will include improved 'Quality of Service' (QoS) along with latency that is extremely low. In addition, the benefits of 5G wireless networks include affordable and reliable access to broadband access in any location, and this is not just for small hand-held devices but includes communication of Machine-to-Machine (M2M), Cyber-Physical systems (CPs), and the Internet of Things (Ahmad et al., 2019). There are, however, inherent security challenges as well as benefits to 5G wireless networks. In order to examine the security issues of the network, it is important to know that the network architecture has three tiers related to security, including: (1) access networks; (2) backhaul network; and (3) the core network (Ahmad et al., 2019). Security threats for the 5G networks include those of: (1) attack on DoS and signaling plane; (2) hijacking attacks; (3) signaling storms; (4) access that is not authorized; (4) attacks on configuration; (5) penetration attacks; (6) theft of user identity; (7) man-in-the-middle attack; (8) TCP level attacks; (9) key exposure; (10) session replay attacks (11) IP spooling and reset attacks; (12) scanning attacks; (13) IMSI catching attacks; (14) channel prediction attacks; (15) jamming attacks; (16) active eavesdropping; (17) passive eavesdropping; (18) NAS signaling storms; and (19) IoT traffic bursts (Ahmad et al., 2019). The following table displays each of the stated security threats along with the potential targets and the segments of the networks that may be affected by those security threats.

Security threats	Potential targets	Affected network segments		
		HetNet Access	Backhaul	Core Network
DoS attack on signaling plane	Centralized control elements			✓
Hijacking attacks	SDN controller, hypervisor	✓	✓	
Signaling storms	5G core network elements			✓
Un-authorized access	Low-power access points	✓		
Configuration attacks	Low-power access points	✓		
Saturation attacks	Ping-pong behavior in access points, and MME	✓		✓
Penetration attacks	Subscriber information			✓
User identity theft	User information data bases			✓
Man-in-the middle attack	Un-encrypted channels, e.g. in IoT	✓		
TCP level attacks	Gateways, router and switches		✓	
Key exposure	Radio interfaces	✓		
Session replay attacks	Session keys in non-3GPP access	✓		
Reset and IP spoofing	Control channels	✓		
Scanning attacks	Radio interfaces interfaces	✓		
IMSI catching attacks	Roaming and UE	✓		
Jamming attacks	Wireless channels	✓		
Channel prediction attacks	Radio interfaces	✓		
Active eavesdropping	Control channels	✓		✓
Passive eavesdropping	Control channels	✓		✓
NAS signaling storms	Bearer activation in core network elements			✓
Traffic bursts by IoT	Saturation of GTP end-points		✓	✓

Figure 1. 5G Network Security Threats, Targets, and Segments Affected (Source: Ahmad et al., 2019)

However, the security challenges for 5G do not end there, as there are security issues present in the primary 5G technologies as well, which include those of: (1) DoS attacks; (2) hijacking attacks; (3) signaling storms; (3) resource or slice theft; (4) configuration attacks; (5) saturation attacks; (6) penetration attacks; (7) theft of user identity; (8) SPIDAS DoS attacks; (9) TCP level attacks; (10) man-in-the-middle attacks; (11) IP spoofing and reset; (12) scanning attacks; (13) data leakage; (14) cloud intrusion; (15) active eavesdropping; (16) passive eavesdropping, and (17) VM manipulation (Ahmad et al., 2019). The security threats, along with the element of the network that could be targeted and the technology that would be impacted, are shown in the following figure.

Security Threat	Target Point/Network Element	Effected Technology			
		SDN	NFV	Cloud	MIMO
DoS attack	Centralized control elements	✓	✓	✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓		
Signaling storms	5G core network elements			✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓	✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓		
Saturation attacks	SDN controller and switches	✓			
Penetration attacks	Virtual resources, clouds	✓		✓	
User identity theft	User information data bases			✓	
SPIDAS DoS attacks	Cyber-Physical clouds			✓	
TCP level attacks	SDN controller-switch communication	✓			
Man-in-the-middle attack	SDN controller-switch communication	✓			
Reset and IP spoofing	Control channels	✓			
Scanning attacks	SDN controller interfaces	✓			
Insider attacks	Cloud and virtual systems		✓	✓	
Data leakage	Cloud storage systems			✓	
Cloud intrusion	Overall cloud systems			✓	
Active eavesdropping	Control channels	✓			✓
Passive eavesdropping	Control channels	✓			✓
VM manipulation	Clouds and virtual systems		✓	✓	

Figure 2. 5G Technologies Challenges for Security (Source: Ahmad et al., 2019)

However, despite the overwhelming numbers of security challenges related to 5G wireless networks and technology, there are solutions for security, which are shown in the following table.

Solution	Security type	Effected Technology			
		SDN	NFV	Cloud	MIMO
Controller Replication	Control plane security through scalability	✓			
SEFloodlight	Control plane access authorization	✓			
DoS detection	DoS and DDoS detection techniques	✓		✓	
NetServ	Self-protection of control plane from DoS attacks	✓	✓	✓	
FRESCO	Composable security for SDN	✓			
PermOF	Application authorization in SDN	✓			
FlowChecker	Flow rules verification in SDN switches	✓			
VeriFlow	Flow rules verification in SDN switches	✓			
Flow admission	Flow-based access control in SDN	✓			
Resonance	Control access to SDN and core network elements	✓			
Splendid Isolation	Ensures traffic isolation for VNFs and virtual slices		✓		
TLS protocol	Provide security to control channels	✓			
IBC protocol	Provide security to control channels	✓			
Capacity sharing	Security in sharing of resources	✓		✓	
DDoS Defender	Defence from IP spoofing and DDoS	✓		✓	
OpenHIP	User identity verification for roaming and clouds services	✓		✓	
ECOS	Privacy and trust in offloading	✓			
OF-RHM	Ensure identity security of users	✓			
mMIMO security	Active attack detection methods				✓
OSPR	Active eavesdropping detection				✓
Physical layer security	Passive eavesdropping detection				✓
Security principles	NFV security challenges and best practices		✓		
Policy manager	NFV security configurations		✓		
Xoar	NFV and VM security platform		✓		
OpenVirteX	NFV hypervisor security		✓		
SecMANO	NFV orchestration and MVNO security		✓		
NFVITP	MVNO security principles and practices	✓	✓		
Security proposals	Integrity verification, security of data and storage systems			✓	
ENDER	HX-DoS mitigation Security for cloud web services			✓	
Secure protocol	Service-based access control security	✓		✓	
CSA proposal	Cloud Security Alliance (CSA) proposal for security			✓	

Figure 3. 5G Security Solutions (Source: Ahmad et al., 2019)

Despite the security challenges and issues related to 5G wireless networks and technologies, the benefits of the technology are incredible but will require a:

> "paradigm shift in security as well. The development in computing paradigms, such as quantum computing, will compel us to design new robust security architecture leveraging powerful computing to strengthen network security. The basic idea is that the diversity and growth of computing and communication technologies must be matched with novel security systems" (Ahmad et al., 2019, p. 25).

It is related that machine execution of automation and functions that are complex will be useful for the acquisition of information, implementation of action and decision selection, as well as implementing action to ensure reliability and accuracy; however, there will still be some requirements to manually configure some of the aspects of security (Ahmad et al., 2019). However, it is noted that more research is needed to address the security challenges that exist in relation to 5G as it is combined with cloud computing technologies.

Blockchain Technology and Business Data Security

According to Demirkan, Demirkan and McKee (2020), "blockchain is essentially a decentralized digital ledger that consists of blocks of transactions between parties" (p. 2). Blockchain has also been described as a "distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties" (Crosby et al., 2016, p. 8). However, there is not a central control for the blockchain, and there are many huge possible benefits for many of the businesses and industries. The high level of security in the blockchain is based on its efficiency because in order for anything to change in a blockchain, required is that the majority of all parties to any transaction and those in the following blocks contained in the chain have to be an agreement with any change (Demirkan et al., 2020). Companies and organizations can form private blockchains for a specific industry or business sector requiring authentication for its use and can make provision of software solutions for businesses that are trustworthy (Demirkan et al., 2020). For example, the Hyperledger is described as:

> "an enterprise-based ledger that is based on blockchain technology and is used to support all the blockchain-based distributed ledgers. Hyperledger is designed for enterprise-level blockchain applications and introduces member management services ensuring data security and trust among users. The goal of the Hyperledger is to support blockchain technology and transform and advance global business transactions" (Demirkan et al., 2020, p. 3).

Blockchain accounting enables the business professional to track orders that are arranged in blocks in a manner that is very secure and enables transactions to be not just recorded but also verified, and no intermediary is needed because it is completely automated. The automation eliminates errors and cuts out unnecessary intermediaries. In addition, it is easy to see the transactions, and everything is transparent and verified in real-time by computers (Demirkan et al., 2020). However, cybersecurity is an issue even with Blockchain technology, so it is necessary to ensure employees receive training on cybersecurity awareness even when using blockchain. Yet, blockchain is a secure technology compared to others with less in the way of threats to security and is, in fact, "emerging as one of the more reliable and powerful technologies for cybersecurity" (Demirkan et al., 2020, p. 8). However, due to the rapid development of blockchain technology, there is not yet enough in the way of history and use of the technology in relation to executive business decisions. However, blockchain will likely be very useful in adaptation to the supply chains and enabling more secure and accurate transactions, as well as supporting reporting that is more accurate (Demirkan et al., 2020). Blockchain makes it possible to improve the security of the business system both backward and forward in terms of supply chain linkages since everything in the supply chain will be traceable, and issues of security can be easily identified (Demirkan et al., 2020). Blockchain's Distributed Ledger Principles enable the following:

1. There is no trusted third party required instead; the network is peer-to-peer.
2. New transactions are time-stamped and hashed onto an ongoing chain of transactions.
3. The hash algorithm is designed to provide a proof-of-work.
4. The record, the hashed chain of transactions, cannot be changed without redoing the proof-of-work.
5. The proof-of-work is accomplished by a pool of CPUs from the peer-to-peer network through computation.
6. The longest chain (block of transactions) includes the latest transaction and requires the most CPU work to create the hash; therefore, it takes the most time, to date, to compute the hash.
7. The system works as long as the majority of peer-to-peer nodes are not cooperating to subvert the chain since they represent the majority of the computing power and so can compute the hash faster than any other group (Demirkan et al., 2020, p. 12-13).

These components enable anyone who is auditing the system to easily identify issues with data security and reliability.

Business Data Security Case Studies

Small Business Impact of Fraud

There are many ways that businesses can face security issues, and according to the National Cybersecurity Alliance (2020a), one of those ways can involve the use of business credit cards. In a situation involving one business that was a business consulting firm that sent a ten-person team to South America to attend to a project for a client, one of the company's employees used the business debit card at a South American ATM. One month later, the business began receiving overdraft notices from the bank. There were fraudulent withdrawals in the amount of $13,000.00, all of which were from South America, along with a $1,000.00 fee for overdrafts (National Cybersecurity Alliance, 2020a). The attack was launched by criminals by installing an ATM skimmer device on the ATM machine that recorded the debit card credentials and then manufactured fraudulent cards and used them all around South America. Once the company realized that the fraud had occurred, the company initiated contact with the bank and closed down the account that had been hacked, but the bank refused to reimburse the company, and the business cut its ties with the bank. The company updated its

protocols for travel and banned employees from using the debit cards provided by the company requiring that employees prepay electronically or use cash or a major credit card if needed (National Cybersecurity Alliance, 2020a). The lessons learned by the company were to use major credit cards since they have more protection than business debit cards, and there should be a better grasp of the policies of the bank about losses due to fraud and recovery. Although the amount would appear to be small to a ten-person firm, the amount lost was impactful on the business.

Keylogger Strikes Business

The National Cybersecurity Alliance (2020b) reported the event in which a construction company that used online banking extensively along with ACH transfers was attacked by a keylogger. Although the employees used a login with the company that had a user-specific ID along with a password, the company received notification that a $10,000.00 transfer had been initiated by a source that was unknown. However, upon contacting the bank, the company discovered that cybercriminals had conducted a total of six transfers in the amount of $550,000.00 in just one week. The cybercriminals had managed to install malware directly on the computers of the company and had been using a keylogger to capture the credentials for using the company's banking functions. Although the bank managed to retrieve less than half of the money that was stolen, the company was left with $350,000.00 missing. Unfortunately, the company did not have an effective cybersecurity plan and learned they needed to gain the assistance of a cybersecurity forensic firm to assist them in reviewing their systems, identifying the source of the problem, and upgrade the security software (National Cybersecurity Alliance. 2020b).

Dark Web Attack

A government contracting firm's CEO received a notification, according to the National Cybersecurity Alliance (2020c), that there was an auction of the business data of the firm on the dark web and eventually tracked the issue to a malicious email attachment that had been downloaded by a senior employee who believed they could trust the source. The attack was a phishing attack, which is one in which malware is sent in an email attachment. The company responded by the IT management shutting off communications immediately with the server that had been impacted, and the system was taken offline. Cybersecurity scans were run on the network so that any potential breaches or additional ones could be identified. Fortunately, the firm had a cybersecurity forensics firm already onboard, and every agency that had been affected was immediately notified. However, the impact financially and operationally of the breach was significant and extensive, and cost in excess of one million dollars (National Cybersecurity Alliance, 2020c). The company had to keep its system offline for quite a few days, and business was disrupted while a new server and security software licenses were installed. The lessons learned from the security breach included that no company is too small to become a target for cybercriminals, staff must necessarily be highly trained in cybersecurity, even when that is not their direct job, anti-virus, and firewalls, along with information encryption tools, must be installed to scan for and counteract anything harmful, and there must be ongoing testing for vulnerability and the conduction of risk assessments (National Cybersecurity Alliance, 2020c).

Capital One Data Breach

According to Neto, De Paula, and Borges (2020), Capital One "works in a highly regulated industry, and the company abides to existing regulations" (p. 5). However, despite the fact that Capital One invested strongly in IT infrastructure, in 2019, it disclosed that an individual external to the organization had accessed customer data that was sensitive. A total of 106 million individuals in the United States and Canada were affected (Neto et al., 2020). However, the company did have a Responsible Disclosure Program, which meant that the incident was discovered quicker than if the regular cybersecurity operations had discovered the incident. The FBI became involved, and a woman was arrested for the hack. It was discovered that she had worked for a cloud server and had hacked into 30 additional companies (Neto et al., 2020). The individual arrested is reported to have "created a scanning software tool that allowed her to identify servers hosted in a cloud computing company with misconfigured firewalls, allowing the execution of commands from outside to penetrate and access the servers" Neto et al., 2020, p. 7). The Capital One hack by the individual was enabled due to a configuration failure in the company's Web Application Firewall (WAF). Capital One failed in the implementation of security controls that were proper and should have used the NIST Framework in mitigating the attack. The ISO and NIST frameworks both should be followed to ensure security, and lack of the standards or lack of training on adhering to the standards can result in situations such as those experienced by Capital One (Neto et al., 2020).

ISO and NIST Frameworks

Both ISO 27001 and the NIST framework are concerning the establishment of controls for information security (Compliance Council, 2020). ISO 27001 is reported as a standard with a focus on keeping stakeholder and customer information secure and the maintenance of integrity by ensuring no unauthorized modification takes place. The National Institute and Standards of Technology or NIST framework is a voluntary cybersecurity framework that is available for companies that oversee any critical infrastructure, and has the selfsame goals of ISO 27001 but emphasizes the identification, evaluation, and management of risks deemed acceptable for information systems (Compliance Council,

2020). The NIST Framework sets out the principles of identification of cybersecurity risks, protection of the company, early detection of threats, response to the attack when it occurs, and recovery from the attack (Compliance Council, 2020). The ISO 27001 framework has a focus on the context of the organization, the organizational leadership, and their commitment to information security, planning, support, operation, evaluation of performance, and improvement (Compliance Council, 2020).

The following lists the principles of the ISO 27001:

1. Context of the organization: The company examines the environment in which it is working along with all systems that are involved and its goals, including the relevant parties and the assets that fall within the system.
2. Leadership and Commitment: Information security is such that it comes from the top of the organization and goes downward. When leadership is actively involved with ensuring they are following the requirements and make provision of guidance, it is much more likely that success will be realized.
3. Planning: It is necessary for businesses to have methods for identifying cybersecurity risks and for treating those that are most concerning while discovering new opportunities. Required is a risk management process that involves the organization preparing for cybersecurity assessment and threats as they evolve.
4. Support: Cybersecurity measures that are successful are those that are provided with sufficient resources. The organization should ensure the provision of the necessary budget, infrastructure, communications, and people to achieve success.
5. Operation: This involves the organization doing what they need to in order to act on their protection and data security planning.
9. Performance evaluation: After the plan has been deployed, companies should ensure they track the plan's effectiveness in order to make any needed adjustments.
10. Improvement: The organization should conduct a regular evaluation to ensure any improvements needed are made (Compliance Council, 2020).

Training and Education for Employees

Despite the fact that employees use the Internet and computers on a regular basis in the workplace and have some level of awareness concerning security risks, the truth is that for the largest part, most employees are not certain of the measures required to ensure they "achieve the confidentiality, integrity, and availability of information in cyberspace" (Kovacevic and Radenkovic, 2020, p. 1). Although employees may have heard the term phishing, they generally do not know how to recognize it when it occurs, and even if they do realize what it is do not know how to react in an appropriate manner. The Pew Research Center revealed that only slightly more than one-half of employees could correctly identify the phishing attacks (Kovacevic and Radenkovic, 2020). Moreover, a report by the Ponemon Institute revealed that human being carelessness was the primary reason for nearly 80 percent of all cyberattacks, indicating the need for businesses to ensure their employees are properly educated and trained on cybersecurity issues. The first step is to increase security awareness, which requires training to teach employees how to recognize any IT security issues and concerns and provide an appropriate response. However, security awareness training is not a one-off event but instead is ongoing in nature and continuous since there are new attacks appearing on a constant basis (Kovacevic and Radenkovic, 2020). Achieving awareness requires three levels, including: (1) perception, or recognizing the attributes, status, and dynamics of elements that are related in the environment; (2) comprehension, which is a synthesis of the various and separate perceptual elements using evaluation and analysis based on data collected; and (3) projection or a prediction of the information analyzed (Kovacevic and Radenkovic, 2020).

Parry and Battista (2020) also noted how emerging technologies would be affecting the work of employees and revealed that the function of HR is going to be impacted by those emerging technologies. For example, the digital platforms that are used commonly in the workplace and central to online marketing include e-Bay and Amazon, while labor market platforms such as Freelancer.com and Uber, along with AI, robotics, machine learning, and augmented and virtual reality, will play strong roles in many industries, including those of construction, healthcare, oil and gas, as well as aerospace (Parry and Battista, 2020). This means that the type of skills, knowledge, and abilities that organizations require will be undergoing continuous change, and while the need for the general manual and cognitive skills are on the decrease, the workforce will need various skills, along with increases in creative, social, and new cognitive and technical skills (Parry and Battista, 2020).

The human resources (HR) plays a role that is critical in the recruitment and the development of the needed competencies for the organization and will need to ensure the design of programs for leadership development that take the newly needed skills and associated challenges into consideration (Parry and Battista, 2020). HR will have to focus on managing the organizations' employees in a modern environment that serves to coordinate machines and humans (Parry and Battista, 2020). It will be important that human resources personnel are adept at using automation and digitalization in searching for

new talent with the needed skills to function in the highly technological workplace. There are recommendations stated, revealing that "companies should develop a competency model which incorporates bot its corporate values and also the specific requirements for individual's jobs" (Deloitte, 2017, p. 46). The competencies that are required should be firstly identified, then quantified in excess of what is the current case and used in recruiting new staff and evaluating the performance of already existing staff to understand what training or education is needed to enable employee competencies (Deloitte, 2017). Digitalization can be used in the optimization of employee training and to ensure the company stays abreast of changes in technology. Required will be an embedding in the company culture the acknowledgment of the need to stay current with the ability to use new technologies (Deloitte, 2017). Therefore, the company must ensure it promotes and encourages ongoing training and to guide employees with self-directed learning, and by creating digital spaces, the organization could "enable deep learning to take place and new competencies to be acquired" (Deloitte, 2017, p. 48). The culture of learning in the organization will require the inclusion of business data security learning that informs employees how to identify threats to the organization's data. There are many various data security training programs available for employees to get a company started with training; however, it is important that the training for data security is ongoing (Media Pro, 2020). The primary aspect of training for security awareness is equipping employees with the needed knowledge to combat any such threats. Employees will not understand the threats that exist and much less so what actions to take without proper training. The majority of employees have no knowledge about security threats, and others are confused or misinformed about what behaviors are risky (Media Pro, 2020). No matter which type of training program the company chooses, it should be such that it makes the provision of actionable, concise advice that is memorable concerning the reduction of information technology and cybersecurity risks (Media Pro, 2020). Recommended aspects of data security training should cover such as phishing, social engineering, safety using the Internet and social media, mobile computing, insider threats, which may be such as an employee inserting an infected USB into the organization's computer system, incident reporting, relevant regulations and laws, and practices to ensure data privacy (Media Pro, 2020).

Chapter Three: Methodology

The research methodology of this study is qualitative and in the form of a content analysis of previously published materials located in journal articles, business publications, and any other publications that would inform the study. According to Gheyle and Jacobs (2017), content analysis is a methodology in research used to make sense in an unstructured way of message contents and might be in the form of texts, which is the case in the present study. Content analysis is held to be "distinct for several reasons, as can be noticed in the one often-cited definition: it is a research technique for making replicable and valid inferences from text to the constructs of their use" (Gheyle and Jacobs, 2017, p. 2). Qualitative content analysis is interpretive in nature and is focused on context and meaning (Gheyle and Jacobs, 2017). Qualitative content analysis is an approach that makes the requirement of a process that is analytical and is based on the formulation of research questions and sampling material that is previously published (Gheyle and Jacobs, 2017). Content analysis is inductive and has no predefined categories but instead asks open questions. Evidence is collected in the content analysis from materials that will inform the study. The evidence is of key importance and analyzed through what has been called a hermeneutic loop, which involves an ongoing contextualization, reinterpretation, and redefinition of the research (Gheyle and Jacobs, 2017). The content analysis that will be conducted in this study will not specifically involve any type of coding but instead will be focused on gaining meaning from the entirety of the sources reviewed and identifying themes that emerge in the research. According to Vaismoradi and Snelgrove (2019), qualitative content analysis and thematic analysis have many elements in common. In both types of analysis, there is a search for any hidden meaning in the data. Qualitative content analysis is enhanced by intuition, creativity, and innovation and are elements critical to developing themes (Vaismoradi and Snelgrove, 2019). The primary focus of qualitative content analysis is the provision of a simple yet in-depth reporting of the similarities and differences that exist in the data (Vaismoradi and Snelgrove, 2019).

CHAPTER FOUR: ANALYSIS

Introduction

The objective of the research in this study was to examine the current environment of new and rapidly advancing technologies, the impact of new and changing technologies on business data security, and the benefits and challenges associated with new technologies and business data security. The specific research questions this study sought to answer were those of: (1) what new and changing technologies exist or are expected to be ready for use in the near future? (2) what benefits and challenges are associated with new technologies and business data security? and (3) how can businesses prepare their employees and security professionals to meet the challenge of data security presented by new and emerging technologies? As noted in the introduction to the study, security and privacy present the most significant challenges for the Internet of Things (IoT), which includes all types of connected devices linked across the Internet, whether they are wireless or wired devices (Tawalbeh et al., 2020). The majority of today's businesses are linked to the Internet in some way, whether it is via their computers, their accounting software, their banking apps, or other types of Internet support and enabled applications. It is important that businesses use scanning and monitoring to ensure that their business data is secure

and that any security threats are avoided. However, as technologies are rapidly expanding and emerging, new threats are constantly being introduced into the business via various new computing methods and technology. The result is that there are more significant challenges relating to data exposure risks and sensitive corporate data being at risk (Mihaela, 2020). Not only are threats to data security becoming more common, but they are also becoming more complex. However, businesses can only survive if they keep up with new technology, and although there are many security risks, it is certain that there are also many benefits to the new and emerging technology (Lange & Kettani, 2019). Additional security risks have been posed most recently since so many employees are working from home due to the situation with the COVID-19 pandemic (Lohrman, 2020). The use of home networks and computers have increased the potential problems with business data security, and when added to the placing of so much information in the cloud, the threats increase due to holes in security, outages, and misconfigurations. It is certain that as the security industry experiences growth at much higher levels accompanied by new products along with mergers and acquisitions in the earlier part of 2021 that there will also be an increase in the complexity of issues in integration problems, network issues, and which may well overwhelm cybersecurity teams.

As noted in the literature reviewed in this study, information security is undergoing a change that is significant and will be impacted between the present and 2030 by various macro-level factors, including globalization, evolving demographics, and regulation, all of which will impact business organizations in terms of opportunities and risks.

Cloud Computing

Seven trends identified in the study included the increase in the penetration of wireless networks and high-speed broadband, centralization of computing resources and wide adoption of cloud computing, the rapid growth of internet protocol devices with increased functions and connections, infrastructure improvements for communications technology and information globally and outsourcing increases, the convergence of devices along with software components and increased modularization, and the lines between personal and work life being blurred with remote working, and bring your own devices approach in information technology. Finally, user interface evolution is growing, along with disruptive technologies emerging (PWC, 2020). With the explosion of data comes the sharing of data that is sensitive on a greater scale between organizations and individuals and particularly social media networking requiring seamless connections between devices.

Information security professionals, along with businesses and many other stakeholders, will be required to use an approach that is proactive in addressing business data security due to the growth in the complexity of threats and the number of threats. Required will be that organizations ensure their approaches to information security take into consideration the processes, people, and technology aspects of information security and that those approaches enable rapid adaptation as there is a shift in the threats and as new technology is adopted.

However, the benefits of new technology are clear, and despite the quick evolution, changes such as Wi-Fi enable connections to computers without the need for wires or cables. However, at the same time, while reaping the benefits of cost reductions, improvements in functionality and services, businesses have been far too slow to adopt information security, particularly for the cloud computing technology. Cloud computing enables businesses to access such as Microsoft Office online without having to install the programs on every computer the business owns, and IT as a service enables processes, software, storage, and security as services. However, in cloud computing, there are three specific scenarios in which business data security may be endangered, including when sensitive personal information is sent to the cloud server when data is transmitted from the cloud service to the business computer, and when the personal data of the business or its clients is stored in the cloud server (Ahmad & Hossain, 2014). As shown in the study, cloud computing offers three services, including Infrastructure as a Service, Platform as a Service, and Software as a Service (Islam, 2017).

Infrastructure as a Service enables a business to use the cloud for its hardware resources, including a memory network, CPU, and others that can be either rented or leased and enables the business to meet any growth in its demand for resources and to do so saving the costs that would otherwise be required. Platform as a service enables the business to run its applications directly on the cloud and enables modification, development, testing, and the running of an application without the requirement of purchasing software. Cloud computing has the primary benefits of the achievement of economies of scale, as well as optimization in relation to security, speed, availability, recovery from any disaster, and maintenance, and moreover, the ability to backup all of the company's data in the cloud. Backing up data in the cloud is a huge benefit as compared to where the computers of the business, storing all the company's data have the potential to crash and lose all of the data. Another reported benefit of cloud computing is the ability to share applications and architectures among many users, as well as to enhance the potential for customization, and makes all the company's data available in a location that can be accessed by all employees, ensuring that work is streamlined, and collaboration is effective between various employees.

Specific concerns with cloud computing are related to data privacy security issues and data confidentiality, requiring that the data be only visible to authorized users, which can be very difficult, and since the service provider is responsible for ensuring confidentiality, the business may not have complete control over security; however, it can address some of those concerns by ensuring data encryption is undertaken and being very careful about what cloud services, the company uses.

Artificial Intelligence

The second issue and technological advance that may impact business data security identified in the present study is that of artificial intelligence, which has many benefits for data security protection. However, companies that use artificial intelligence and machine learning technology may be especially vulnerable to cyberattacks (Lazic, 2019). Cyberattacks can cost a business huge sums of money and may even involve extortion. However, at the same time, the benefits of artificial intelligence will mean that it is adopted by many companies. Therefore, the necessary precautions should be taken when using the technology. The benefits of artificial intelligence include savings of money and time because structured data can be examined quickly, and artificial intelligence has the capacity to read and examine data in a comprehensive manner. However, artificial intelligence has some shortcomings in terms of protecting business data, including that some of the attacks will not be identified by antivirus programs, companies who are attacked may be followed by another attack, and overall, some loopholes still exist with data security when artificial intelligence is used. Businesses that use artificial intelligence have to make certain they create better techniques for employee login, such as those which are biometric-based and ensuring they secure conditional authentically and access. Artificial intelligence, when used properly, can assist businesses to lower costs associated with detecting and responding to data breaches and enable a faster response.

5G Technology

The benefits of 5G are clear in that the networks will make provision of affordable and reliable broadband access and for all types of devices, including Machine to Machine, Cyber-Physical systems, and the Internet of Things (Ahmad et al., 2019). The 5G network has three security tiers, including the access networks, the backhaul network, and the core network. Specific security threats for 5G networks are those related to a DoS attack, hijacking attacks, unauthorized access, signaling storms, configuration type attacks, and penetration attacks. Other security issues include those related to user identity theft, man-in-the-middle type attacks, TCP attacks, key exposure attacks, session replay attacks, IP spoofing and reset, as well as scanning IMSI catching, channel prediction, jamming, active and passive eavesdropping, NAS signaling storms, and IoT traffic bursts.

Blockchain

Blockchain is a decentralized digital ledger in which transactions between various parties are recorded in a block form (Demirkan et al., 2020). No central control exists for Blockchain technology. There are great benefits for businesses due to the high level of security that exists in blockchain, which cannot be modified without the agreement of the majority of parties to a transaction. Blockchain is a peer-to-peer network that can be used to eliminate costs and cut out unnecessary intermediaries, and the transactions are secure and verified. Everything in the blockchain is transparent and verified in real-time by computers. However, there are still some cybersecurity risks requiring that employees receive training when the use of blockchain is implemented. Even with the concerns, blockchain technology is much more secure than are other technologies. Blockchain will enable more accurate reporting and will be useful for the supply chains, as well as enabling transactions that are more secure. Ultimately blockchain will enable the improvement of the business security system in both directions in terms of traceability.

Theme Three: Businesses of All Types and Sizes Are at Risk for Business Data Security Breaches

The case studies reviewed in the present study revealed that businesses of all types and sizes are at risk of data breaches and cyberattacks. From the small business with only ten people who had their company credit cards hacked to Capital One that experienced a major data breach, the dangers are present for any business. Keylogger attacks, such as that which occurred and was inflicted on a construction company, can cost companies huge sums of money, and in that specific case, the attack cost more than one-half million dollars. Attacks such as the keylogger attack involve malware being installed directly on computers, but other attacks can occur across the Internet in the form of cybersecurity attacks. Whether the attacks are in the form of dark web attacks such as the case study reviewed in which a server was attacked using phishing or an employee inserts an infected flash drive into the company computer, the results are the same, in that the company will lose time, money, and oftentimes the trust of their clients and customers due to the attacks. It is important that companies are up to date on their knowledge and alignment to the ISO and NIST frameworks.

Theme Four: Employee Training is Key Ensuring Business Data Security

The fourth theme identified in the material reviewed in the present study is the necessity for employee training on business data security issues because employees, although having some level of awareness about security risks, are not certain of

what they should and can do to ensure they take the necessary action to ensure the security of business data (Radenkovic, 2020). As noted by the Pew Research Center, employees do not know how to identify phishing attacks, and as already mentioned, an employee could unknowingly insert a flash drive that is infected with a virus into the business computer resulting in disaster for the company. The increasing complexity of the methods used by criminals who commit cyberattacks and other business data attacks makes training on security for the business of incredible importance. In light of the new and emerging technologies, businesses will have to ensure employees across the organization receive training on information security prevention measures, how to respond if a threat is detected, and who in the information technology department to contact when a threat is detected. In other words, business data security can no longer be the information technology departments' sole domain because all employees will have to be proactively involved in ensuring business data security. As noted in the present study, the human resources department will have to be involved in hiring employees with the necessary knowledge and skills but will also be responsible for training the existing employees since the domain of HR is involved in connecting computers and human beings in various functions across the organization. Today's businesses and the various actors and departments will all have to be focused on ensuring employees are trained in information security prevention, detection, and response practices, and it cannot be just a one-off event because the training will need to ongoing on a regular basis and ever-evolving to match the emergent technologies that will be used in the business setting. Training for employees should cover, such as phishing, social engineering, Internet and social media safety, insider threats, incident reporting, and any laws that are relevant.

Adoption of NIST and ISO 27001 Frameworks is Critical for Businesses

The fifth and final theme identified in the study is that the adoption of the NIST and ISO 27001 frameworks will be critical for organizations. Each of these frameworks sets out the principles for the business in terms of prevention, identification, response, preparation of employees using training, and recovery from any attack on the businesses' data and information security breaches. When leadership in the company strictly adheres to the frameworks and offers guidance to those being led, any information security program will be much more effective and successful. Employees require guidance and training on the NIST and ISO 27011 framework, along with other cybersecurity and information security training.

DISCUSSION

The information reviewed in the study has revealed that new and emerging technologies offer huge benefits to companies, including cost savings, savings in time, and ultimately a higher level of data security but only if employees are properly trained using the NIST and ISO 27001 frameworks so they can properly identify, respond to, and work in a concentrated manner that mitigates the potential for attacks on business data. Business data security is a huge concern for businesses as it is not just the business that may suffer huge losses when attacks on the business data occur, but the clients and customers may also be affected, giving the business a bad name. The promises of cloud computing, artificial intelligence, 5G networking, and blockchain technology will certainly result in companies using those technologies to drive business growth and to streamline many business processes, including the supply chain, accounting, and many other aspects of the business that will be enabled by the new technologies. The question is not whether new technologies will emerge, but how soon the next new and improved technologies will emerge, and for that reason, companies are going to have to stay on their game with employee training that is continuous and organizational-wide.

CONCLUSION

The conclusion of this study is that new and emerging technologies are offering powerful solutions to businesses and will enhance business growth and productivity by connecting them with their customers and one another in a collaborative way that enhances work processes from the supply chain to accounting and in terms of customer relationship management. However, the new and emerging technologies also come with serious challenges that must be addressed in relation to ensuring business data security. Training of employees in the area of business data security and information security measures will be critical for businesses, and they will need to ensure that training is ongoing, includes all employees and departments of the organization, puts plans in place to identify and respond to information security threats. It will be necessary that the training of employees follows the NIST and ISO 27001 framework to ensure the organization's plan for information security is sound. Both the NIST framework and ISO 27001 set out the methods for organizational identification, response, and recovery from any type of attacks on a businesses' information security, whether the attack occurs at the physical location of the company or in the area of cybersecurity.

RECOMMENDATIONS

The recommendations that have arisen from the research conducted in the present study include those stated as follows:

1. Companies should research the latest technologies and identify the benefits and challenges before adopting the technologies.
2. Companies should adopt the NIST and ISO 27001 frameworks.
3. Companies should train everyone in the organization and in every department about business data security using the NIST and ISO 27001 frameworks so that the employees can effectively be proactive in preventing threats and properly respond to threats.
4 Companies should develop a culture of information security and cybersecurity awareness in the organization, which will be enhanced by training, leadership guidance, HR processes and practices, interaction with the information security team and department, and an ongoing process of updating the training to respond to new and emerging technologies.

REFERENCES

[1] Ahmed, M. & Hossain, M.A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security and Its Applications (IJNSA), 16*(1), 25-35. https://www.researchgate.net/publication/276199301_Cloud_Computing_and_Security_Issues_in_the_Cloud
[2] Bissel, K., Lasalle, R.M., Dal Cin, P. (2020). *Innovate for cyber resilience: Lessons from leaders to master cybersecurity execution*. 1-48. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
[3] Compliance Council (2020). ISO 27001 vs NIST Cybersecurity Framework. https://blog.complia ncecouncil.com.au/blog/iso-27001-vs-nist-cybersecurity-framework.
[4] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.
[5] Deloitte (2017). *What key competencies are needed in the digital age? The impact of automation on employees, companies, and education*, 1-60. https://www2.deloitte.com/content/dam/ Deloitte/ch/Documents/innovation/ch-en-innovation-automation-competencies.pdf.
[6] Demirkan, S., Demirkan, I. & McKee, A. (2020). Blockchain technology in the future of business cybersecurity and accounting. Journal of Management Analytics, 1-20. https://www.researchgate.net/publication/339509334_Blockchain_technology_in_the_future_of_business_cyber_secu rity
[7] Gheyle, N. & Jacobs, T. (2017). *Content analysis: A short overview*. Internal Research Note, 1-17. https://www.researchgate.net/publication/321977528_Content_Analysis_a_ short_overview
[8] Islam, N. K.V. (2017). Review on benefits and security challenges of cloud computing. *International Journal of Computer Science and Information Technologies, 8*(2), 224-228. http://ijcsit.com/docs/Volume%208/vol8issue2/ijcsit2017080219.pdf
[9] Khan, R., Kumar, P., & Jayakody, D.N.K. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *Journal of LATEX IEE Communications Surveys and Tutorials*, 1-55. https://www.researchgate.n et/publication/3 34644935_A_Survey_on_Security_and_Privacy_of_5G_Technol ogies_Potential_Solutions_Recent_Advancements_and_Future_Directions
[10] Lange, T. & Kettani, H. (2019). On security challenges of future technologies. *Journal of Communications, 14*(11), 1002-1007. https://www.researchgate.net/publication/336567 832_On_Security_Challenges_of_Future_Technologies
[11] Lazic, L. (2019). Benefit from AI in Cybersecurity. The 11th International Conference on Business Information Security (BISEC-2019), 18 October 2019, Belgrade, Serbia, 1-9. https://www.researchgate.net/publication/336826190_BENEFIT_FROM_AI_IN_CYBERSECURITY
[12] Lohrmann, D. (2020). *The top 21 security predictions for 2021*.https://www.govtech.co m/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html
[13] Maddox, T. (2020). Top 10 emerging technologies of 2020: Winners and losers. https://www.te chrepublic.com/article/top-10-emerging-technologies-of-2020-winners-and-losers/
[14] Media Pro (2020). Security awareness training: What is it and why it's critical. https://www.mediapro.com/security-awareness-training/
[15] Mihaela, C.L. (2020). Current security threats in the national and international context. *Accounting and Management Information Systems, 18*(1), 351-378. https://www.re searchgate.net/publication/342905154_Current_security_threats_in_the_national_and_international_context
[16] National Cybersecurity Alliance (2020a). A business trip to South America goes south, 1-1. https://www.nist.gov/system/files/documents/2020/09/30/Cybersecurity-Case-1.pdf
[17] National Cybersecurity Alliance (2020b). A construction company gets hammered by a keylogger, 1-1. https://www.nist.gov/system/files/documents/2020/09/30/Cybersecurity-Case-2.pdf

[18] National Cybersecurity Alliance (2020c). A dark web of issues for a small government contractor, 1-1. https://www.nist.gov/system/files/documents/2020/09/30/Cybersecurity-Case-5.pdf

[19] Neto, N.N., Madnick, S., De Paula, A.M., & Borges, N.M. (2020). *A case study of the capital one data breach*. [Cambridge: MA: MIT Sloan], 1-25. http://web.mit.edu/smadnick/ww w/wp/2020-07.pdf

[20] Parry, E. & Battista, V. (2020). The impact of emerging technologies on work: A review of the evidence and implications for the human resource function. *Emerald Open Research, 1*(5), 1-13. https://emeraldopenresearch.s3.amazonaws.com/manuscripts/13973/9 daba8b5-b5a3-4028-8725-e652a0c18c68_12907_-_emma_parr.pdf? doi=10.12688/emeraldopenres.12907.1&numberOfBrowsableCollections=5&numberOfBrowsableInstitutionalCollections=0&numberOfBrowsableGateways=6

[21] PriceWaterhouseCoopers (PWC) (2020). Revolution or evolutions? Information Security 2020, 1-44. https://www.pwc.com.au/consulting/assets/risk-controls/revolution-or-evolution-2010.pdf

[22] Tawalbeh, L., Muehidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences, 10*(4102), 1-17. https://www.mdpi. com/2076-3417/10/12/4102/pdf

[23] Vaismoradi, M. & Snelgrove, S. (2019). Theme in qualitative content analysis. Forum *Qualitative Social Research, 20*(3)(23). https://www.qualitative-research.net/index.php/fqs/article/view/3376/4470

[24] Vaismoradi, M. & Snelgrove, S. (2019). Themes in qualitative content analysis and thematic analysis. *Forum: Social Research, 20*(3) (23), 1-15. https://www.researchgate.net/publication/336085326_Theme_in_Qualitative_Content_Analysis_and_Thematic_Analysis