Journal of Business and Environmental Sciences
Volume: : 2 (2): Page:303-329
https://doi.org/10.21608/JCESE.2023.206861.1030
ISSN: 2974-3117
E-ISSN: 2974-3125

Research article

The Impact of Data (Cyber) Security on Business Continuity "Applied Case Study on Telecom Egypt"

Amr Hassan [1], Walid Taha [2] *

[1] Sinai Higher Institute for Specific Studies, Egypt; amr.hassan.std@iesr.asu.edu.eg

[2] Telecom Egypt; mero11111@yahoo.com

* **Correspondence:** amr.hassan.std@iesr.asu.edu.eg.

Abstract: Purpose: Telecom Egypt seeks to improve the performance of cyber data security, so the research aimed to show the impact of cyber data security on business continuity. The survey and implementation of the survey list directed to the sample items, which amounted to 384 items, and statistical analysis was used using the spss program in order to verify the validity of the research hypotheses.

Results: The research reached to The Main hypothesis accepted “There is a Significant Impact of data (Cyber) Security on business continuity in the Egyptian telecommunication sector”- The study showed that cyber security has a role in achieving business continuity, The results of the research showed that cybersecurity has a very positive impact on the comprehensive understanding of the way the organization works at Telecom Egypt.

Recommendations: The most important recommendations are: The researchers recommends the necessity of increasing the updates of special applications in the field of cybersecurity and making a comprehensive plan with specific time periods to be circulated to all branches of Telecom Egypt, the necessity of giving a greater role in the field of cyber security training to all sectors and departments within the company to support the role of cyber security in formulating a business continuity strategy in Telecom Egypt- The necessity of increasing attention to the privacy of customer data, due to its significant impact in the study on business continuity; In order to improve the level of performance in the related companies.

Keywords : (Cyber) Security - Business Continuity - Telecom Egypt.

APA Citation: Hassan. A., Taha. W., (2023). The Impact of Data (Cyber) Security on Business Continuity Applied Case Study on Telecom Egypt. Journal of Business and Environmental Sciences, 2(2), 303-329.

Introduction

Telcos have been collecting customer data for decades, but recent interest in big data continues to draw significant attention to customer data collection processes. Customers are not only concerned

Received: 19 April 2023; **Revised**: 15 May 2023; **Accepted:** 1 June 2023; **Online:** 4 June 2023
The Scientific Association for Studies and Applied Research (SASAR)
https://jcese.journals.ekb.eg/

with how this information is collected, but also with which data points are tracked and for what purpose.

Regardless of the industry, data security has a significant impact on both the business and the customer, as data breaches remain one of the top threats to consumer safety and business continuity. That's why it's important to keep your data collection strategies transparent to maintain trust and loyalty. Customers understand that telecom brands collect information for billing purposes. However, as these methods become more detailed, all of these companies must offer clear privacy policies to consumers who want to control their personal information. (Järveläinen, 2015)

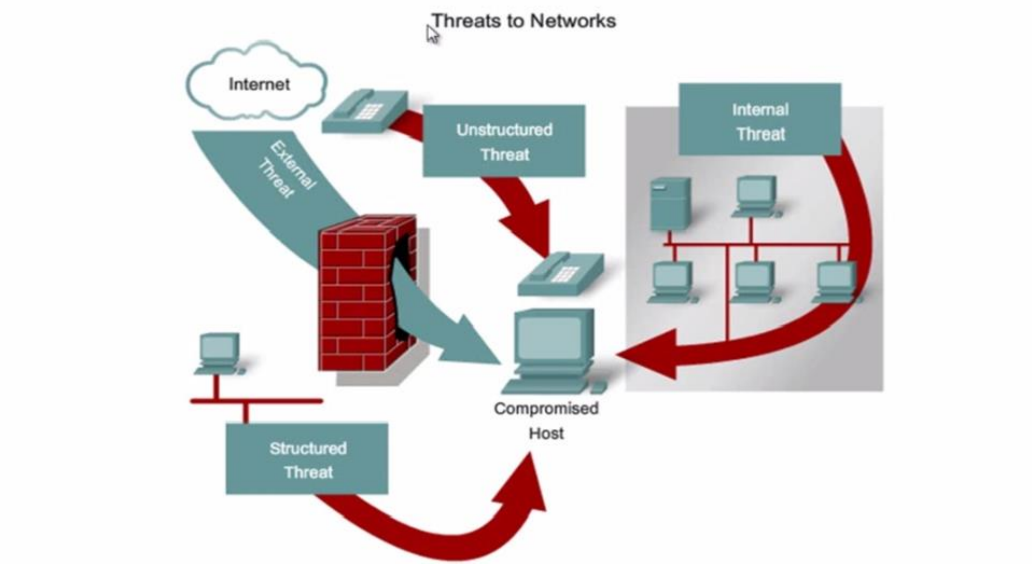

Figure 1. Threat to Network

Accurate data (cyber) security starts with a comprehensive strategy and risk assessment. This allows you to see what threats you are facing and what could happen if your valuable data is lost due to theft, malware infection or system failure. Other potential threats you want to identify. (Järveläinen, 2015)

These include:

1) Physical hazards such as fire, power failure, theft, or intentional damage.
2) Human error, such as incorrect handling of information, unintentional deletion of data or input errors.
3) Corporate espionage exploits and other malicious activities.

Now it can identify sensitive areas and develop strategies to protect data and information systems. There are several aspects to consider here:

1) Who has access to which data?
2) Who uses the Internet and postal systems and how do they access them?
3) Who has access and who is restricted?
4) Whether to use passwords and how to store them.

5) Which firewalls and anti-malware solutions should you implement?
6) Train staff properly and ensure data security.

The increasingly faster data generated permeates every aspect of our lives. This situation requires intensifying the data security practices of all stakeholders (individuals, governments and companies). Data loss or theft is becoming a major financial burden as “more business functions are moved online and more businesses and consumers around the world go online.”(Lewei Dong, 2021).

The causes of data security incidents vary. This includes but is not limited to system failures, virus or malware infections, theft or fraud by personnel, or attacks by unauthorized third parties. Traditionally, companies whose business models are geared towards monetizing data storage and processing are most at risk. As a result, IT service providers and resellers who handle large volumes of customized information were the main victims or targets of data breaches. (David W Chadwick, 2020).

Research Importance

The researcher believes that this research contributes to making an applied assessment of the relationship between data (Cyber) Security and improving the Business Continuity of Telecom Egypt as the research provides the possibility to clarify the causal relationship between the general variables of the data (Cyber) Security .

1.Academic knowledge

The lack of scientific literature on data security (cyber) in Egypt to the researcher's knowledge makes the present study relevant.

2.Researchers

- The researcher believes that the field is interesting because it deals with a new and sought-after field that is suitable for application to many organizations.
- This study could also help enrich the researchers' knowledge of data (Cyber) Security subjects and Business Continuity.

Problem and Research Questions

The problem

Cybercrime is now a global problem affecting many areas of human life. Police officers around the world have to learn how to deal with this type of crime, safety classes for children prepare them for the dangers of the digital world... and of course, big companies that have every reason to keep their data secret and intact are investing incredible amounts of money to increase digital security in the world. Every new gadget and software sooner or later become a target for cybercriminals, which is why their manufacturers do everything they can to stay one step ahead of them.

The Internet was created primarily for military purposes as a global network. Unsurprisingly, the importance of security has been high from the start. Later, when the internet became accessible to the majority, criminals started using it for their own purposes. Cyber security specialists and cyber criminals have started a rivalry that is comparable to the development of crime.

Research Questions

1. What is the influence of data (Cyber) security in the Egyptian Telecommunication sector?
2. What are the benefits of data (Cyber) security in the Egyptian Telecommunication sector?
3. What is the relationship between the data (Cyber) security and customer Business Continuity in the Egyptian Telecommunication sector?

Research Objectives

There in one main objective this research is targeting which is "can the data (Cyber) security variables effect on Business Continuity in the Egyptian Telecommunication Sector?" and to reach this objective, there are some other sub-objectives must be clarified such as:

1. Explore the relationship between the data (Cyber) security & Business Continuity.
2. Finding the variables that have the most impact on Business Continuity.
3. Studying the impact of data (Cyber) security on Business Continuity.

The purpose of the business continuity plan is to minimize the negative impact of possible disruptions in the organization's operations and ensure a speedy return to normal operations.

Research Hypothesis

In order to conduct a controlled experiment and empirically verify the facts, a single null hypothesis was developed:

Main Hypothesis:

H1: There is a Significant Impact of data (Cyber) Security on business continuity in the Telecom Egypt sector.

Sub Hypotheses:

H 1.1: There is a significant impact of data (Cyber) Security on Understand the nature of the organization's business.

H 1.2: There is a significant impact of data (Cyber) Security on Formulating a business continuity strategy.

H 1.3: There is a significant impact of data (Cyber) Security on Continuous improvement of business continuity.

H 1.4: There is a significant impact of data (Cyber) Security on Evaluate and update business continuity plans.

Previous studies

The previous studies are divided into two parts: the first part will address some updated articles related to Data (Cyber) security, elements, and results of their application. The second part will focus on the Business Continuity, its dimensions, and its importance for companies.

Data (Cyber) security Previous studies:

(Arturo S. Bretasa, 2019)

This article introduces another contribution to smart grid cybersecurity in the form of a malicious data attack. The stakes are double. First, a formal proof of how the parameter errors is distributed over the measure function. with a parameter with error. The largest composite measurement error property in its normalized form is .then proved for this error case.

The proposed solution works well against malicious attacks on measurement and parameter data. However, the state estimator software does not require major changes. The validation takes place on the bus systems IEEE 14 and 57.

(David W Chadwick, 2020)

This article provides an answer to this problem by providing a flexible framework that allows CTIs to be shared confidentially for analysis among colleagues. We propose a five-layer trust model for the data exchange infrastructure at the cloud edge. The data owner can choose the appropriate level of trust and approach to sanitizing CTI data, ranging from plain text to anonymization/pseudonymization to homomorphic encryption, to manipulate the CTI data before making it available for analysis become.

Dependent on the organization's level of trust in them. We describe our trust model, cloud edge infrastructure, and delivery model designed to meet a wide variety of data protection needs.

(Sudhakar Sengan, 2020)

In our research paper, we examine the security issues of SC infrastructure development and examine the perspectives of both technology and business operations. We have also introduced the Hybrid Smart City Cyber Security Architecture (HSCCA) method. This method not only develops secure data, but also analyzes threats.

Finally, our research leads to the evaluation of some key cybersecurity solutions for smart cities proposed for HSCCA. This paper recommends configuring contextual security for traditional cyber-physical systems and outlines some potential areas to explore and their implications.

(Lewei Dong, 2021)

This article proposes the idea of a combined observer-based security remediation control for cyber-physical stochastic systems (CPS) exposed to deceptive data injection attacks (FDIA).

It has been shown that corrupted state signals can be corrected, and the desired safety performance can be guaranteed for stochastic CPS under FDIA with heterogeneous effects. Finally, two simulation tests including the longitudinal dynamics system controlled by the F-16 network.

Business Continuity Previous studies:

(Francisco Serrano, 2020)

The purpose of this document is to provide insights to aviation personnel during events related to the pandemic in order to set appropriate standards for the company and employees.

It also showed that staffing needs are unpredictable, but that flexibility is needed in times of crisis. In this context, good communication with employees about what the organization expects of employees is important. However, the well-being of employees must remain at the heart of the organization.

(Alessandro MARGHERITA, 2021)

In our study, we examine the actions taken by 50 of the world's largest companies in response to the outbreak of the pandemic.

The study continues the scholarly discussion on the impact of emergencies on business continuity and provides managers with a complete overview and some ideas for defining response strategies and measures in the current difficult scenario.

(Luca Galbusera, 2021)

In this paper we document the concept, implementation and results of a survey conducted by the European Commission's Joint Research Centre. The

Topics covered in this study include assessing business continuity and evaluating aspects of crisis management and disaster recovery from the perspective of different industries, types of organizations and personal opinions of respondents.

(Taarup-Esbensen, 2021)

This article explains how Business Continuity Management can be used in the Arctic using the example of mining companies in Greenland.

This article discusses how mining companies can manage the complexity of the Arctic environment and the interdependencies of risk events through the use of organizational skills and competencies.

Researcher's comment on previous studies

Customer retention insights come from all of the brand interactions consumers have had with your business throughout their journey. From phone calls to emails or social media conversations, this data also represents the largest non-monetary data set for most telecom companies. Brands need to listen to this feedback by creating listening posts that enable them to correctly and wrong as well as assessing the competitive landscape. (Lewei Dong, 2021)

“The customer will tell you exactly why they buy or leave, what they like or don’t, and if the service is valuable or empty.”

Of course, before telcos engage with this incoming data, they need to determine which points are most valuable for strategic planning and business growth. Rebecca Sendel, senior director of product management at TM Forum, explains that telcos should first define the end goal to determine the relevant data points for collection and analysis. Brands need to consider what problems they are solving by collecting data and what they want to improve. This way of thinking must be at the heart of data collection because data by itself is useless. This data is also designed to help uncover opportunities for improvement, track success, and prioritize to ensure your most valuable customers receive the best possible service, regardless of the interaction channel in particular, external data can provide insight into what types of services customers desire, allowing the Company to better target or modify its marketing practices to decline and customize upselling offers based on customer behavior.

For example, large telecommunications company currently uses usage data to track overall daily usage of its products and services at the individual customer level. The brand can identify when individual daily usage doesn't match a given customer's overall usage patterns, as this can indicate issues with the service that need to be resolved quickly. By proactively investigating, the company can often find and fix problems before the customer knows about them. Then employees will inform the customer about the problem and its solution, draw attention to their actions and ask the customer to confirm the great service. Ultimately, this strategy changes the dynamic as the business takes responsibility for monitoring service rather than relying on the customer to identify and report problems. The brand can anticipate key issues that could impact long-term customer satisfaction and retention, and provide seamless, consistent service that differentiates the customer experience.

With more data to collect and analyze, it's often difficult for organizations to do everything at once. Therefore, telcos must set ultimate goals to collect and analyze data to derive real value from this wealth of information effectively and efficiently.

The relationship Between Data (Cyber) Security and Business Continuity (Järveläinen, 2015)

1. Business continuity focuses primarily on the information systems of each organization. Business continuity consists of two main components: business continuity management (BCM) and business continuity planning (BCP).
2. Business continuity planning is an important activity that requires the involvement of many business units.
3. Since computers are an important part of the organization, the APC must contain a detailed specification of the information systems. These specifications should include documentation of computer systems, preferably in graphical form. In addition, business functions should be linked to IT systems through Business Impact Analysis (BIA) or business modelling.
4. The challenge of having a near perfect and still valid BCP for computing stems from the fact that computer systems are inherently dynamic in terms of updates and reconfigurations.
5. “Preventive measures are more important than recovery measures.” Preplanned recovery procedures are an important part of IT disaster planning, especially for organizations with critical business functions that rely heavily on data communications. Good IT emergency planning is therefore essential in order to optimize processes and investments.

Pilot Study

At the start of the study, a pilot study was conducted to collect primary data on the research problem, hypotheses, and variables.

The researcher conducted interviews with 15 managers and employees in the IT departments, the quality control department, the sales and marketing department, and others at the headquarter of in Egyptian Communication Company.

The goal of the pilot study was:

1) Know the research problem.
2) Clarify any details that must be addressed before proceeding to
3) collecting master data.
4) Gain a thorough understanding of the factors affecting the study variables.
5) Explain the current situation of the IT sector regarding Data(cyber) Security .
6) Gather more information about the green supply chain and the
7) competitive practices of ceramic companies in Egypt.

Research Methodology

Research Approach

While primary data for the purpose of testing the hypotheses will be collected by distribution of survey forms to managers and employees of Telecom Egypt dealing with the Data (Cyber) Security concept their number are 384 by distributing two types of surveys:

- First: Survey to measure Data (Cyber) Security.
- Second: Survey to measure Business continuity.
- The terms of the survey were used through some previous studies and references, with the addition of some modifications by the researcher.
- Analyzing the Questionnaire results by using SPSS program.

Population

We conducted an applied study on some samples from Telecom Egypt employees and their number (35.000) person works across various sectors around Egypt and in different geographic areas and various functions sectors to find out whether they are aware in Data Security initiatives done by TE .

Research Limitations

The study will be conducted in Telecom Egypt Company, this study targets to investigate "The Impact of Data (Cyber) Security on Business Continuity in Egyptian Telecommunication sector" as the development of the telecommunications sector in Egypt is the result of close cooperation between many players.

The Theoretical Framework of The Research

While there are countless studies on cybersecurity issues in the Arab world, there is a lack of research that focuses on the cybersecurity awareness of managers and employees and the impact of their attitudes contributes to business continuity. All personnel can be equipped to act as a human firewall to ward off any attack. Al- Alawi et al. (2016).

Data (Cyber) Security

Cybercrime is any crime that takes place and influences computer systems and networks that brings about the need for cybersecurity, which represents an important issue facing the world today (Johnson, 2016 a).

Cybersecurity is a network system security protection for the organization's information against any cyber threats, which acts as a prevention against any damage to, or destruction of, vulnerable databases. Moreover, all businesses need to protect their network from threats which could arise from weakness of the network design, end-user carelessness, inheriting a weak technology or even from the misconfiguration of hardware and software (Spalević, 2014).

Cybersecurity may not be accomplished throughout technology alone (Herath & Rao, 2009). No matter how strong an organization's technical defenses are, the cybersecurity ultimately relies on user behaviors (Rhee et al., 2009). Incidents which might attributed to mistakes made by staffs will result in far more damage to businesses annually than outside attacks. Gaining the help and contribution of an institution's staff involves an effective awareness program that is supported by all layers of management (Olzak, 2006). Nevertheless, end users do not usually act when their organization is attacked by a security incident. Kaspersky (2018) reported that in 40% of industries around the world, workforces hide an incident when it occurs Moreover, 52% of industries acknowledge that workers are their main weakness in cybersecurity, with their irresponsible activities driving corporation cybersecurity strategy at total risk. The findings of the survey illustrated that industries definitely have valuable intentions to be concerned about workforces being involved cybersecurity risks. Employees may generate mistakes that place their business's data and systems at risk either due to their negligence and accidently slip up or due to not having the required training to educate them how to behave and act appropriately to support their business (Gelles, 2016).

Some individuals or organizations can benefit from compromised information about company assets. These may be former employees of the company or people with whom the company does business. The negligence of an employee who inadvertently compromises company data, or the negligence of other business competitors attempting to break into other profitable businesses for financial gain, poses a cybercrime risk to a company. This can disrupt business operations, particularly for those conducting their business online, resulting in financial losses due to information theft, which in turn entails data breach costs for the company. and other associated costs associated with such incidents such as B. Loss of business and customer reputation, as well as costs for cleaning and maintaining the affected system, damage costs incurred by other companies associated with the company concerned and other penal costs for any other loss of personal data.

The Main Objective of Cybercrime

The main purpose of cybercrime is to affect the computer equipment or computer services of governments or companies to make money or damage their reputation. It does this by hacking into the company's IT equipment to affect its valuable asset information, which mainly includes data related to customer databases and their financial records. Therefore, its customer lists, the company's pricing information and relationships with other companies, as well as the company's product design and manufacturing process are valuable information, which are mainly stored in the company's computer systems and can be compromised by cyber criminals. (Arlitsch & Edelman, 2014).

Furthermore, one of the causes of cybercrime in society is related to the concept that whenever the return on investment is high and the risk is low, many people in such a situation have an advantage, which means they access valuable content and want to use this Article information ensures a high yield efficiency. Therefore, it is difficult to stop and catch these criminals, which explains the increase in cybercrime in many societies. (Al-Alawi, 2014).

Cyber Security Policy Axes

This study is based on the instructions to adapt to cyber risks issued by the Central Bank for the year (2018), and these instructions required all licensed banks, financial institutions, credit reference agencies and microfinance companies subject to the supervision and control of the Central Bank to implement the legal requirements related to these instructions, and Article (9) stipulates , on fourteen axes that should be included in the cybersecurity policy, at a minimum. For the purposes of facilitating the study and the lack of justification for excluding any axis, the relevant policy axes that are related to each other were merged (Marina,2021).

The researchers believes that rapid development and change in network infrastructure, it has led to great problems and challenges facing businesses, organizations, and managers of information technology departments regarding security procedures and policies related to investing in the capabilities and developments of the Internet. This requires managers to balance the need for the security aspects of the Internet on the one hand, and access to it, and the investment of its enormous potential on the other.

This requires huge amounts to increase the security aspects because of the necessary need for the organization with the link other companies via the Internet for business purposes, and this leads to an increase in external attacks through professional crimes, and this requires security tools, methods, and defensive and preventive standards, and among these means are encryption, firewalls, and denial of service.

Data security is a set of measures and methods that protect information systems, data and processes from any action aimed at destroying, modifying, or impairing the systems and their functioning. Cyber security protects data, networks, computer programs, computer processing power and other elements of computerized information systems. Cyber security is a very broad field due to the many attack methods and many defense mechanisms. Attacks and countermeasures can target computers, individuals, organizations, countries, or networks. The aim of computer security is to prevent or at least limit attacks.

Business Continuity

The concept of business continuity has developed into an operation that determines the exposure of any organization to potential threats, whether internal or external, and how to provide effective prevention against them, and remedial if these threats occur. Effectiveness of these threats will be determined through the behavior of employees during the process of business recovery (Herbane, Elliott & Swartz, 2004).

Business Continuity Concept

Business organizations are exposed to disturbances of varying severity, which can escalate into a disaster or crisis if not managed properly, in addition to damaging the organization's reputation and other material damage, so organizations must be fully prepared to face these disturbances before they occur and reduce their effects if Occurrence (Heng, 2015)

The main objective of business continuity management is to make the organization's flexibility, and to ensure the delivery of basic products after the organization has been exposed to crises that have damaged the organization's assets and prevented access to the necessary resources, in order to reduce direct and indirect economic losses that may They result from these crises and the consequent disruption to the business, as the Business Continuity Department does this by reducing weaknesses, mitigating their effects, and returning the situation to normal as soon as possible after the crisis (International Labor Office, 2011).

Business Continuity Objectives

Business continuity makes it easier for the organizations that rely on it to predict future worst-case scenarios, how the organization might operate in the aftermath of a disaster or crisis, as well as the speed at which the organization can restore its normal operations. (Gibb & Buchanan, 2006).

Business continuity also achieves the financial benefit of the institution as it addresses the weakness within it, because failure has financial consequences and costs the institution even if that failure does not lead to disruption or interruption of the institution from work, and by addressing weaknesses, the institution becomes more flexible and more effective in terms of its ability to reduce the cost Loss resulting from exposure to crises and disasters, and business continuity management aims to increase confidence in the organization and build its capabilities at a high level of flexibility, and this would later improve the defense capacity of the organization against various organizational risks, disasters and crises in order to ensure the long-term survival of the institution. (Elliott *et al.* , 2010).

Stages of Business Continuity Development

The need for business continuity management arose in the early 1970s to protect information systems from the effects of disasters, as disaster planning focused on restoring an organization's critical facilities after a major failure such as loss of information or computer communications, etc. Loss of a building by fire or flood, and responsibility for these plans has been distributed across different functions within the company, usually related to information technology, hardware security, and real estate. In the mid-eighties, the concept of business continuity developed and became a new way to manage business risks on the basis that the responsibility of business continuity management rests with enterprise managers to ensure the continuity of business functions at all times and under any circumstances, and many researchers have discussed this development for business continuity management. (Gallagher, 2003; Pitt&Goyal, 2004 ;Herbane *et al.*, 2004; Kelly, 2007; Elliott *et al.* , 2010).

Many previous studies suggest that the focus of business continuity management in the 1970s and 1980s was information technology continuity because business continuity was considered a purely IT issue and that this function itself is the engine principle of business continuity management. (Gill ,2006 ; Botha & Sloms, 2004).

While this approach to business continuity management encourages standardization of practices, it remains a management business grounded in common sense and best practices. (Gallagher, 2005).

Research Procedures

To investigate the phenomenon quantitatively, the researchers used an analytical approach in this study. The study reveals the influence between different dimensions in order to reach at a last result that might later be helpful for future research.

Measurement instrument:

The researcher used a questionnaire form created from the survey conditions used in some previous studies and references, with some modifications made by the authors, to check "The Impact of Data (Cyber) Security on Business Continuity (An applied Study on Telecom Egypt)".

Research Sample:

- **Research Population**: The research community includes all employees of Telecom Egypt, which employs up to (35,000) people.
- **Sample size**: Due to the large population, the sample size drawn from a large statistical firm can be determined by the following Steven-Thompson equation:

N = **35000**

Sample = 380.00

0.05 1.96 3.8416

0.0025 0.5

The online sample size reached 380 respondents.

The research develops and test the following hypotheses:

<u>Main Hypothesis:</u>

H1: There is a Significant Impact of data (Cyber) Security on business continuity in the Telecom Egypt sector.

Sub Hypotheses:

H 1.1: There is a significant impact of data (Cyber) Security on Understand the nature of the organization's business.

H 1.2: There is a significant impact of data (Cyber) Security on Formulating a business continuity strategy.

H 1.3: There is a significant impact of data (Cyber) Security on Continuous improvement of business continuity.

H 1.4: There is a significant impact of data (Cyber) Security on Evaluate and update business continuity plans.

Questionnaire design:

To find the study dimensions, the questionnaire consisted of (46) statements on study variables. A set of statements using a Likert model as follows: (5 - 4 - 3 – 2-1) It expresses the strength or weakness of the answer.

The questionnaire consists of two sections:

Section one: personal information includes (Gender – Age - Educational Level - Years of Experience - Position level)

Section Two: study variables: Independent Variables: Data (Cyber) Security (23) statements about study dimensions (Application Security & Network Security). Dependent variable: Business Continuity (25) statements about study dimensions (Understand the nature of the organization's business, formulating the strategy, Continuous improvement & evaluate, update business plans).

Statistical methods:

IBM SPSS V.25 software was used, to classify the data, to test the stability of the questionnaire:

1. Reliability test with Cronbach's alpha coefficients to check the stability of the questionnaire.
2. Checking the validity using the Pearson correlation coefficient between the dimensions and the entire questionnaire.
3. Descriptive statistics of the data by filling in the data in the form (numbers, percentages, mean, standard deviation, weight percentage) of variable resolution.
4. Correlation using the Pearson correlation coefficient to prove the validity of the research hypotheses.

Straight and multiple regression to examine the effect of the independent variable on the dependent variable to prove the validity of the research hypotheses.

Research Results

All procedures used to verify validity and reliability of questionnaire items will be addressed, and the most important findings and outcomes for each hypothesis will be discussed according to the research methodology that was collected and followed as mentioned in the previous chapter. Several analytical practices are used to investigate the data collected in the study. Statistics involves methods of describing and analyzing data to make inferences or conclusions about the phenomena represented by the data.

Reliability:

To test the stability of the questionnaire, the researcher used Cronbach's alpha equation (Cronbach alpha). The table below shows the reliability coefficients generated using this equation.

Table 1: The reliability of Data (Cyber) Security dimensions

Variables	**Cronbach's Alpha**	**N of Items**
Application Security	0.805	10
Network Security	0.921	13

The table above shows that the reliability coefficients of the data security (cyber) dimension had high values, while the values of the reliability coefficients were high (0.805, & 0.921) for (Application Security & Network Security) consequently which indicate the values of the reliability-importance ratios of Data (Cyber) Security dimensions' statements for the application and the reliability of the results and trust.

Table 2: The reliability of Business Continuity dimensions

Variables	**Cronbach's Alpha**	**N of Items**
Understand the nature of the organization's business	0.892	6
Formulating a strategy	0.914	7
Continuous improvement	0.932	7
Evaluate and update business continuity plans	0.926	5

The table above shows that the reliability coefficients of the data security (cyber) dimension had high values, while the values of the reliability coefficients were high (0.892, 0.914, 0.932 & 0.901) for (Understand the nature of the organization's business, formulating a strategy, Continuous improvement & evaluate and update business continuity plans) consequently which indicate the values of the reliability-importance ratios of Business Continuity dimensions' statements for the application and the reliability of the results and trust.

Table 3: The reliability of questionnaire dimension

Variables	**Cronbach's Alpha**	**N of Items**
Data (Cyber) Security	0.928	23
Business Continuity	0.972	25
Total questionnaire	0.973	48

The table above shows that the reliability coefficients of the data security (cyber) dimension had high values, while the values of the reliability coefficients were high (0.928, 0.972 & 0.973) for (Data (Cyber) Security, Business Continuity and Total questionnaire) which indicate the values of the reliability-importance ratios of the questionnaire statements for the application and the reliability of the results as well as the confidence.

The Validity

The researcher calculates the significance of the correlation coefficient for each questionnaire dimension to calculate overall equity as follows:

Table 4: Correlations to calculate the validity of the Data (Cyber) Security dimensions.

Variables	**r**	**P-value**
Application Security	0.939(**)	0.001
Network Security	0.941(**)	0.001

** p-value significant at (0.01)

From the table above, the validity of the questionnaire dimension, we conclude that the values of the correlation coefficient at the level (0.01) between the dimensions Data Security (Cyber) and Data Security (Cyber) are statistically significant overall, which confirms the validity of the questionnaire size and of the Pearson correlation coefficient values (0.772, 0.939 & 0.941) for (Application Security & Network Security) consequently.

Table (5): Correlations to calculate the validity of the Business Continuity dimensions.

Variables	**r**	**P-value**
Understand the nature of the organization's business	0.894(**)	0.001
Formulating a strategy	0.939(**)	0.001
Continuous improvement	0.948(**)	0.001
Evaluate and update business continuity plans	0.920(**)	0.001

** p-value significant at (0.01)

From the previous dimensional validity table of the questionnaire, it can be seen that the values of the correlation coefficients at the (0.01) level between are statistically significant Business Continuity dimensions and total Business Continuity, which confirms the validity of questionnaire dimension and Pearson correlation coefficient values were (0.894, 0.939, 0.948 & 0.920) for (Understand the nature of the organization's business, formulating a strategy, Continuous improvement & evaluate and update business continuity plans) consequently.

Table (6) Correlations to calculate the validity of the questionnaire dimension.

Variables	**r**	**P-value**
Data (Cyber) Security	0.907(**)	0.001
Business Continuity	0.949 (**)	0.001

** P - value significant at (0.01)

From the above table, the validity of the questionnaire size, we conclude that the correlation coefficient values at the (0.01) level between the questionnaire size and the entire questionnaire are statistically significant, confirming the validity of the questionnaire size and Pearson's correlation coefficient (0.907 & 0.949) for (Data (Cyber) Security, Business Continuity and Total questionnaire) consequently.

Research Hypothesis testing:

head hypothesis: There is a Significant Impact of data (Cyber) Security on business continuity in the Telecom Egypt sector.

Table (7): Correlation matrix between Data (Cyber) Security dimensions and the Business Continuity

Variables		**Application Security**	**Network Security**	**Data (Cyber) Security**
Understand the nature of the organization's business	**r**	0.624^{**}	0.689^{**}	0.698^{**}
	P-value	0.000	0.000	0.000
Formulating a strategy	**r**	0.610^{**}	0.691^{**}	0.692^{**}
	P-value	0.000	0.000	0.000
Continuous improvement	**r**	0.564^{**}	0.655^{**}	0.649^{**}
	P-value	0.000	0.000	0.000
Evaluate and update business continuity plans	**r**	0.577^{**}	0.666^{**}	0.661^{**}
	P-value	0.000	0.000	0.000
Business Continuity	**r**	0.641^{**}	0.729^{**}	0.729^{**}
	P-value	0.000	0.000	0.000

** p-value significant at (0.01)

Table 7. illustrate there are a significant correlation between Data (Cyber) Security dimensions and the Business Continuity, where Pearson correlation values significant at P-value (0.01).

Table 8: A simple linear regression test to analyze of data (Cyber) Security on business continuity.

Model	**R**	**R^2**	**B**	**F**	**t**	**p-values**
Impact of data (Cyber) Security on business continuity	0.729	0.531	0.974	427.829	20.684	0.001

To investigate the impact of data security (cyber) on business continuity, a simple linear regression test was performed. The results are as follows:

- The value of the correlation coefficient (R) on the ratio between data security (cyber) and business continuity was (0.729).
- From the results of the coefficient of determination (R2) of linear regression in the previous table, it is concluded that there is an impact of data (cyber) on business continuity (53.1%).
- Significant regression test of the model based on the value (F) which was (427).829), which at < (0.05), which is confirmed by the significant regression model.
- A model test of a significant regression coefficient (B) explaining the presence of the impact of (cyber)security data on business continuity was performed and based on the value (T) which was (20.684), i.e. H. significant at < (0.05).

Table 9: Multiple regression test to study the impact of the dimensions of the data (Cyber) Security on business continuity.

Model	**B**	**t**	**p-values**	**R**	**R^2**	**F**	**p-values**
(Constant)	-0.253	-1.278	0.2	0.740	0.547	227.793	0.001
Application Security	0.249	3.625	0.000				
Network Security	0.721	10.662	0.000				

To investigate the impact of (cyber)security data dimensions on business continuity, a multiple regression test was performed, and the following results were obtained:

- Correlation coefficient (R) values on the relationship between (cyber)security The data size for business continuity was (0.740).
- From the results of the coefficient of determination (R2) of the multiple regression in the above table, we find that the influence of the data dimensions (cyber)security on the business continuity was (54.7%).
- Significant regression test of the model based on the value (F) which was (227).793) for organizational performance which were significant at level < (0.05), which confirms the significant regression model.
- The values of (T), which amounted to (3.625 & 10.662) for (Application Security & Network Security) consequently, which were significant at level <(0.05), while the values (T) indicated a greater influence of the dimension (network security) on business continuity than the influence of the dimension (application security) on business continuity.

From the previous results head hypothesis accepted “There is a Significant Impact of data (Cyber) Security on business continuity in the Egyptian telecommunication sector”.

H$_1$: There is a significant impact of data (Cyber) Security on Understand the nature of the organization's business.

Table 10 Simple linear regression test to study the impact of data (Cyber) Security on understanding.

Model	**R**	**R^2**	**B**	**F**	**t**	**p-values**
Impact of data (Cyber) Security on understanding	0.698	0.487	0.940	359.473	18.960	0.001

To study the impact of data (Cyber) Security on Understand the nature of the organization's business was tested by simple linear regression and the results are as follows:

- The value of the correlation coefficient (R) for the relationship between data security (cyber) and full understanding of the nature of the organization's work was (0.698).
- Based on the results of the coefficient of determination (R2) of the linear regression in the table above, we conclude that there is an impact of data (cyber) security on the full understanding of the nature of the organization's work (48, 7%).).

- Significant regression test of the model based on the value (F) which was (359).473), which at < (0.05), which is confirmed by the significant regression model.
- A model test of the significant regression factor (B) explaining the presence of the impact of data security (cyber) on the full understanding of the nature of the organization's work and on the confidence in the value (T) , which (18.960) was what at (0.05).

Table 11 Multiple regression test to study the impact of the dimensions of data (Cyber) Security on Full understanding.

Model	**B**	**t**	**p-values**	**R**	**R^2**	**F**	**p-values**
(Constant)	-0.059	-.282	0.8	0.704	0.496	185.607	0.001
Application Security	0.295	4.040	0.000				
Network Security	0.642	8.939	0.000				

To study the impact of the dimensions of the data (Cyber) Security on Understand the nature of the organization's business was test by multi regression and the results were as follows:

- The value of the correlation coefficient (R) to the ratio of data dimensions (cyber)security for Understand the nature of the organization's business was (0.704).
- According to the results of the coefficient of determination (R2) of multiple regression in the table above, the influence of the data dimensions (cyber)security on the Understand the nature of the organization's business was (49.6%).).
- Significant regression test of the model based on the value (F) which was (185).607) for significant organizational achievements at < (0.05), which is confirmed by the significant regression model.
- The (T) values of (4.040 and 8.939) for (application security and network security) were therefore significant at <(0.05), while the values (T) indicated a greater impact of size (network security) on the organization's understanding of the nature of its business than did size (application security) influence on the organization's understanding of its business.

From the previous results H_1 accepted "There a significant impact of data (Cyber) Security on Full understanding of the Nature of the Organization's work".

H_2: There is a significant impact of data (Cyber) Security on Formulating a business continuity strategy.

Table 12: Simple linear regression test to study the impact of data (Cyber) Security on Formulating a business continuity strategy.

Model	**R**	**R^2**	**B**	**F**	**t**	**p-values**
Impact of data (Cyber) Security on Formulating a business continuity strategy	0.692	0.479	0.654	347.778	18.649	0.001

To study the impact of data (Cyber) Security on Formulating a business continuity strategy was test by linear simple regression and the results were as follows:

- The value of the correlation coefficient (R) for the relationship between data security (cybersecurity) and business continuity strategy formulation was (0.692).
- Based on the results of the coefficient of determination (R2) of the simple linear regression of the above table, there is an influence of data security (cyber) on the formulation of the business continuity strategy (47.9%).
- Significant regression test of the model based on the value (F) which was (347).778), which at < (0.05), which is confirmed by the significant regression model.
- A model test of the significant regression coefficient (B) was performed, which explains the presence of the influence of (cyber)data security on the formulation of the business continuity strategy and the use of the value (T) which (18.649), which when (0.05).

Table 13 :Multiple regression test to study the impact of the dimensions of the data (Cyber) Security on Formulating a business continuity strategy.

Model	**B**	**t**	**p-values**	**R**	**R^2**	**F**	**p-values**
(Constant)	-0.331	-1.470	0.1	**0.702**	**0.493**	**183.083**	**0.001**
Application Security	0.264	3.379	0.000				
Network Security	0.728	9.445	0.000				

To study the impact of the dimensions of the data (Cyber) Security on Formulating a business continuity strategy was test by multi regression and the results were as follows:

- The values of the correlation coefficient (R) to the relation between the dimensions of the data (Cyber) Security on Formulating a business continuity strategy was (0.702).
- According to the results of the multiple regression coefficient of determination (R2) in the table above, the influence of the (cyber)security data dimensions on the formulation of the business continuity strategy was (49.3%).
- Test the significant regression of the model based on the value (F) which was (183.083) for organizational outcomes found at < (0.05), which is confirmed by the significant regression model.
- The values of (T), which amounted to (3.379 & 9.445) for (Application Security & Network Security) consequently, which were significant at level <(0.05), while the values of (T) indicated to the impact of the dimension (Network Security) on Formulating a business continuity strategy bigger than the impact of the dimension (Application Security) on Formulating a business continuity strategy.

From the previous results H_2 accepted “a significant impact of data (Cyber) Security on Formulating a business continuity strategy”.

H_3: There is a significant impact of data (Cyber) Security on Continuous improvement of business continuity.

Table 14: Simple linear regression test to study the impact of data (Cyber) Security on Continuous improvement of business continuity.

Model	R	R^2	B	F	t	p-values
Impact of data (Cyber) Security on Continuous improvement of business continuity	**0.649**	**0.421**	**0.927**	**274.70**	**16.574**	**0.001**

To study the impact of Promotion dimension as one of data (Cyber) Security on Continuous improvement of business continuity was test by linear simple regression and the results were as follows:

- ➢ The value of the correlation coefficient (R) on the connection between (IT) data security and continuous improvement of business continuity was (0.649).
- ➢ Based on the results of the coefficient of determination (R2) of the linear regression in the table above, we conclude that the impact of data security (cyber) on continuous improvement of business continuity was (42.1%).
- ➢ Significant regression test of the model based on the value (F) which was (274).7), significant at (0.05), which is confirmed by the significant regression model.
- ➢ A test was performed with a model of a significant regression coefficient (B) that explains the presence of the impact of (cyber) data security on continuous improvement of business continuity and on the use of the value (T). , which was (16.574), which at (0.05).

Table 15: Multiple regression test to study the impact of the dimensions of the data (Cyber) Security on Continuous improvement of business continuity.

Model	**B**	**t**	**p-values**	**R**	**R^2**	**F**	**p-values**
(Constant)	-0.066	-0.281	0.8	0.662	0.438	147.154	0.001
Application Security	0.199	2.438	0.02				
Network Security	0.723	8.983	0.000				

To study the impact of the dimensions of the data (Cyber) Security on Continuous improvement of business continuity was test by multi regression and the results were as follows:

- ➢ The value of the correlation coefficient (R) to the ratio of data security dimensions (cyber) to continuous improvement of business continuity was (0.662).
- ➢ According to the results of the multiple regression coefficient of determination (R2) in the table above, the influence of the (cyber)security data dimensions on the continuous improvement of business continuity was (43.8%).

- Significant regression test of the model based on the value (F) which was (147).154) for significant organizational achievements at < (0.05), which is confirmed by the significant regression model.
- The values of (T), which amounted to (2.438 & 8.983) for (Application Security & Network Security) consequently, which were significant at level <(0.05), while the values of (T) indicated to the impact of the dimension (Network Security) on Continuous improvement of business continuity bigger than the impact of the dimension (Application Security) on Continuous improvement of business continuity.

From the previous results H_3 accepted "There is a significant impact of data (Cyber) Security on Continuous improvement of business continuity".

H_4: There is a significant impact of data (Cyber) Security on Evaluate and update business continuity plans.

Table 16: Simple linear regression test to study the impact of data (Cyber) Security on Evaluate and update business continuity plans.

Model	R	R^2	B	F	t	p-values
Impact of data (Cyber) Security on Evaluate and update business continuity plans	0.661	0.437	1.032	293.460	17.131	0.001

To study the impact of Promotion dimension as one of data (Cyber) Security on Evaluate and update business continuity plans was test by linear simple regression and the results were as follows:

- The value of the correlation coefficient (R) to the relation between the data (Cyber) Security and Evaluate and update business continuity plans was (0.661).
- From the results of the coefficient of determination (R^2) of regression simple linear in the previous table, we find that there is the impact of the data (Cyber) Security on Evaluate and update business continuity plans were (43.7%).
- The test significant model regression based on the value of (F), which amounted to (293.46) which was significant at level < (0.05), which confirms the significant regression model.
- It has been through model significant regression coefficient test (B), which explains the presence of the impact of the data (Cyber) Security on Evaluate and update business continuity plans and rely on the value of (T), which amounted to (17.131) which was significant at level < (0.05).

Table (17) Multiple regression test to study the impact of the data (Cyber) Security on Evaluate and update business continuity plans.

Model	**B**	**t**	**p-values**	**R**	**R^2**	**F**	**p-values**
(Constant)	-0.555	-2.186	0.03	0.673	0.453	156.375	0.001
Application Security	0.237	2.692	0.007				
Network Security	0.790	9.106	0.000				

To study the impact of the dimensions of the data (Cyber) Security on Evaluate and update business continuity plans was test by multi regression and the results were as follows:

- The values of the correlation coefficient (R) to the relation between the dimensions of the data (Cyber) Security on Evaluate and update business continuity plans was (0.673).
- From the results of the coefficient of determination (R^2) of multiple regression in the previous table, we find that there is impact of the dimensions of the data (Cyber) Security on Evaluate and update business continuity plans was (45.3%).
- The test significant model regression based on the value of (F), which amounted to (156.375) for organizational performance which were significant at level < (0.05), which confirms the significant regression model.
- The values of (T), which amounted to (2.692 & 9.106) for (Application Security & Network Security) consequently, which were significant at level <(0.05), while the values of (T) indicated to the impact of the dimension (Network Security) on Evaluate and update business continuity plans bigger than the impact of the dimension (Application Security) on Evaluate and update business continuity plans.

From the previous results H_4 accepted “There is a significant impact of data (Cyber) Security on Evaluate and update business continuity plans”.

Results

This research aimed to determine the impact of data cyber security on business continuity in Telecom Egypt, and based on the analysis of the study data and testing its hypotheses, the most important findings of the study can be summarized as follows:

The Results of the Applied Study

1. **Data (Cyber) Security variable:**

A. The greatest number for answering to The Application Security Statements with degree (Agree) and samples agree on all with dimension (83.4).

B. The greatest number for answering to The Network Security Statements with degree (Agree) and samples agree on all with dimension (86.0).

C. The weight percentile of the entire research sample of study participants for the size of the entire sentence (data security (cyber)) was (84.8%), indicating the level (agreement) in the response.

2. **Business Continuity variable:**

A. The greatest number for answering to understanding of the nature of the organization's business. Statements with degree (Agree) and samples agree on all with dimension (78.7).

B. The greatest number for answering to Formulating a strategy Statements with degree (Agree) and samples agree on all with dimension (78.0).

C. The greatest number for answering to Continuous improvement Statements with degree (Agree) and samples agree on all with dimension (77.5).

D. The greatest number for answering to Evaluate and update business continuity plans Statements with degree (Agree) and samples agree on all with dimension (76.7).

E. The weight percentile of the entire research sample of study participants for the entire sentence dimension (activity continuity) was (77.7%), indicating the degree (agreement) in the response.

3. **Hypothesis testing:**

A. The Main hypothesis accepted “There is a Significant Impact of data (Cyber) Security on business continuity in the Telecom Egypt sector”.

B. H_1 accepted “There a significant impact of data (Cyber) Security on understanding of the nature of the organization's business”.

C. H_2 accepted “There is a significant impact of data (Cyber) Security on Formulating a business continuity strategy”.

D. H_3 accepted “There is a significant impact of data (Cyber) Security on Continuous improvement of business continuity”.

E. H_4 accepted “There is a significant impact of data (Cyber) Security on Evaluate and update business continuity plans”.

<u>The Results of the theoretical Study</u>

A. The study showed that cyber security has a role in achieving business continuity.

B. The results of the study revealed that cyber security has a positive role to a large extent on the understanding of the nature of the organization's business in Telecom Egypt.

C. The results of the study showed the presence of positive indicators that support the role of cyber security in formulating a business continuity strategy in Telecom Egypt.

D. The results of the study revealed that business continuity is largely achieved in Telecom Egypt.

E. The study revealed that network security as one of the dimensions of cyber security contributes positively and substantially to Telecom Egypt in promoting business continuity.

Recommendations

Based on the results of this research, the researcher recommends the following:

1. The researcher recommends the necessity of increasing the updates of special applications in the field of cybersecurity and making a comprehensive plan with specific time periods to be circulated to all branches of Telecom Egypt.
2. The researcher recommends the necessity of giving a greater role in the field of cyber security training to all sectors and departments within the company to support the role of cyber security in formulating a business continuity strategy in Telecom Egypt.
3. The necessity of increasing attention to the privacy of customer data, due to its significant impact in the study on business continuity; In order to improve the level of performance in the related companies.
4. The need to increase attention to the issue of cyber risk management, given its impact on the quality of business continuity in the relevant companies.
5. The necessity of increasing attention to the issue of determining the owner, scope of application, powers, and work procedures, given that they have an impact on business continuity.
6. The necessity for the relevant companies to adhere to the cybersecurity policy in their annual reports because it has a significant impact on information security and its role in increasing customer confidence.
7. Encouraging researchers to conduct special studies on the issue of cyber security policy in companies working in the field of information.
8. Encouraging researchers to study other independent factors in the field of business continuity in telecommunications companies.

References

Alessandro MARGHERITA, M. H. (2021). Business Continuity in the COVID-19 Emergency: A Framework of Actions Undertaken by World-Leading Companies. *Business Horizons*, 1-32. doi:https://doi.org/10.1016/j.bushor.2021.02.020.*

Francisco Serrano, A. K. (2020). Business continuity during pandemics – lessons learned about airport personnel. *9th International Conference on Air Transport – INAIR 2020, CHALLENGES OF AVIATION* (pp. 56-66). Slovakia: Elsevier Procedia.*

Järveläinen, J. (2015). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*(5), 332 – 349. doi:https://www.researchgate.net/publication/263575725.*

Lewei Dong, H. X. (2021). Security correction control of stochastic cyber-physical systems subject to false data injection attacks with heterogeneous effects. *Journal Pre-proof*, 1-24. doi:https://doi.org/10.1016/j.isatra.2021.05.015.*

Luca Galbusera, M. C. (2021). The ERNCIP survey on COVID-19: Emergency & Business Continuity for fostering resilience in critical infrastructures. *Safety Science, 139*, 1-20. doi:https://doi.org/10.1016/j.ssci.2021.105161.*

Sudhakar Sengan, S. V. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future Generation Computer Systems*, 724-737. doi:https://doi.org/10.1016/j.future.2020.06.028.*

Taarup-Esbensen, J. (2021). Business continuity management in the Arctic mining industry. *Safety Science, 137*, 1-10. doi:https://doi.org/10.1016/j.ssci.2021.105188.*

Johnson, A. L. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. **NC Banking Inst**., 20, 277.

Spalević, Ž. (2014). Cyber security as a global challenge today. Singidunum Journal of Applied Sciences, 687-692.

Herath, T. and Rao, R. (2009) Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations. European Journal of Information Systems, 18, 106-125.

Olzak, S. (2006). The global dynamics of racial and ethnic mobilization. **Stanford University Press**.

Kaspersky (2018), The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Retrieved February 26, 2018. ***https://www.kaspersky.com/blog/the-human-factor-in-it-security/***

Gelles, M. G. (2016). Insider threat: Prevention, detection, mitigation, and deterrence. **Butterworth-Heinemann**.

Al-Alawi, A. I. (2014). Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status**. Research Journal of Business Management**, 8(3), 139-156.

Marina Evangelou, N. M. (2020). An anomaly detection framework for cyber-security data. **Computers & Security**, 1-10. doi:https://doi.org/10.1016/j.cose.2020.101941

Herbane. Brahim, Elliott. Dominic, & Swartz. Ethne` M. (2004). “Business continuity management: time for a strategic role?”. **Long Range Planning**, 37(5): 435- 457, ***https://doi.org/10.1016/j.lrp.2004.07.010***.

Heng. Goh Moh. (2015). “Business continuity management planning methodology”. **International Journal of Disaster Recovery and Business Continuity**. 6: 9-16, doi.org/10.14257/ijdrbc.2015.6.02.

International Labor Office. (2011). “**Multi-hazard business continuity management guide for small and medium enterprises**” , Geneva ILO.

Gibb, F. and Buchanan, S. (2006). A Framework for Business Continuity Management. International **Journal of Information Management**, 26(2), 128-141 .

Elliott,D.,Swartz, E. and Herbane, B. (2010), Business continuity management: a crisis management approach, **Routledge**, London.

Gallagher, M. (2003). Business Continuity Management: How to Protect your Company from Danger. 1st Edition. **Prentice Hall** .

Pitt, M. and Goyal, S. (2004). Business Continuity Planning as a Facilities Management Tool. **Facilities**, 22(3/ 4), 87-99.

Kamel, A. R., & Abonazel, M. R. (2023). A Simple Introduction to Regression Modeling using R. **Computational Journal of Mathematical and Statistical Sciences**, 2(1), 52-79.

Kelly,W.(2007).Continuity Belongs in Business Planning Process. **Business Insurance**, 41(9), 30.

Botha, J. and Solms, R. (2004). A Cyclic Approach to Business Continuity Planning. **Information Management and Computer Security**, 12(4),328-337. campaignkit1.pdf .

تأثير أمن البيانات (السيبراني) على استمرارية الأعمال "دراسة حالة تطبيقية على المصرية للاتصالات"

عمرو حسن [1]، وليد طه [2]

[1] مدرس مساعد معهد سيناء العالي للدراسات النوعية، مصر amr.hassan.std@iesr.asu.edu.eg
[2] المصرية للاتصالات، mero11111@yahoo.com

الملخص:

الهدف: تسعى المصرية للاتصالات إلى تحسين أداء أمن البيانات (السيبراني) الإلكترونية، لذلك هدفت الدراسة إلى إظهار تأثير أمن البيانات (السيبراني) الإلكترونية على استمرارية الأعمال، تم تنفيذ قائمة استقصاء موجهة لعدد من المفردات والتي بلغت 384 مفردة، وتم استخدام التحليل الإحصائي باستخدام برنامج spss للتحقق من صحة فرضيات الدراسة.

النتائج: قبول الفرضية الرئيسية "هناك تأثير كبير لأمن البيانات (السيبراني) على استمرارية الأعمال في قطاع الاتصالات المصري"، وأظهرت الدراسة أن للأمن السيبراني دور في تحقيق استمرارية الأعمال، وأظهرت نتائج الدراسة أن للأمن السيبراني دور إيجابي إلى حد كبير في الفهم الكامل لطبيعة عمل المؤسسة في الشركة المصرية للاتصالات، كذلك أظهرت نتائج الدراسة وجود مؤشرات إيجابية تدعم دور الأمن السيبراني في صياغة استراتيجية استمرارية الأعمال في الشركة المصرية للاتصالات.

التوصيات: يوصي الباحث بضرورة زيادة تحديثات التطبيقات الخاصة في مجال الامن السيبراني وعمل خطة شاملة بفترات زمنية محددة تعمم على جميع فروع الشركة المصرية للاتصالات، أيضاً يوصي الباحث بضرورة إعطاء دور أكبر في مجال التدريب على مجال الامن السيبراني لكافة القطاعات والإدارات داخل الشركة لدعم دور الأمن السيبراني في صياغة استراتيجية استمرارية الأعمال في الشركة المصرية للاتصالات، ضرورة زيادة الاهتمام بخصوصية بيانات العملاء لما لها من أثر كبير في الدراسة على استمرارية العمل. من أجل تحسين مستوى الأداء في الشركات ذات العلاقة، ضرورة زيادة الاهتمام بمسألة إدارة المخاطر السيبرانية، لما لها من تأثير على جودة استمرارية الأعمال في الشركات ذات الصلة.

الكلمات الدالة: امن البيانات السيبراني – استمرارية الاعمال- المصرية للاتصالات.