IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 03; Issue no 03: March, 2022

Teleworking and Cyber security in the Higher Education Institutions, Dominican Republic Case

Rosilda Miranda Cruz[1]

[1] *Faculty of APEC University, Santo Domingo, Dominican Republic, USA*

Abstract

The rise of remote work has produced an exponential growth in cyber attacks, during the first half of 2021, there was an increase in the number of cyber attack attempts, reaching more than 196 million cyber attack attempts from January to June 2021. The increase in cyber attacks leads institutions to strengthen their computer models, applying work strategies that provide security in the cyber work they do; as well as a solid construction of cyber security culture involving all members of the institution, where each person understands that their daily activities are at risk. The objective of investigating this topic is to identify the factors that affect cyber security in remote work, as explained by Abad, 2018, (cited by James Navarro & Gainza Reyes, 2021). To ensure an acceptable level of security it is necessary to achieve security controls effectively, directly, and professionally to communicate to end-users. Cyber security experts consider it essential that institutions develop programs to prevent and avoid risks derived from the incorrect use of the organization's computer equipment, as they express (James Navarro & Gainza Reyes, 2021; Leornardo, C., 2022; Fortinet, 2021; Garcia, A. A., 2019). Since a user can represent vulnerability for any entity, and a person can be a point used by cybercriminals, it can be sufficient reason to consider the awareness and training of collaborators as a priority of computer security. The main risks and weaknesses that have been identified, which have a key impact in the violation of systems and networks in private institutions in the last two years, the interviewees agreed that many organizations went virtual without being prepared, opening up to considerable gaps for emerging threats..

Keywords: Telework, Cyber security, Cyber-attacks in higher education

Introduction

Since the confinement of March 2020 caused by the COVID-19 pandemic, educational organizations have relied on electronic devices, resources, applications, and technological programs thus classes can continue. Work performance is enhanced by remote schemes for employees to carry out their work, and teachers and students will continue the teaching-learning processes. This resulted in the increased use of IoT devices (Internet of Things devices), of vulnerable resources used in meetings and classes, such as cameras and microphones, offering more opportunities or weak points to cybercriminals, with the limitation of monitoring risks in the teleworker's environment (administrative and/or academic) for the implementation of controls.

The rise of remote work has produced an exponential growth in cyberattacks, as described in data reports from the company's FortiGuard Labs threat intelligence and analysis lab, (2021), Fortinet Inc. (2021), reported that during July 2020 and June 2021 there was a nearly eleven-fold increase in ransom ware, and during 2020 in the Dominican Republic there were more than 158 million cyber attacks, out of a total of 41 billion in Latin America and the Caribbean. During the first half of 2021, there was an increase in the number of cyber attack attempts, reaching more than 196 million cyber attack attempts from January to June 2021.

Referring to remote work or teleworking, (Pérez Pérez, Martínez Sánchez, Carnicer, & Vela Jiménez, 2005) as the form of work organization that uses information and communication technologies (ICT) to enable remote work, either in the employees' own home, in their work displacements or special centers designed for this purpose.
The increase in cyber attacks leads institutions to strengthen their computer models, applying work strategies that provide security in the cyber work they do; as well as a solid construction of cyber security culture involving all members of the institution, where each person understands that their daily activities are at risk. As expressed by James Navarro & Gainza Reyes, (2021) information and the systems that process it are part of the assets for any organization, people are responsible for using and managing it, which is why the management of human resources should be considered among the elementary aspects for the implementation and maintenance of a computer security system. Schneier, B. (2015) (p.22) states that the Internet is the perfect medium for successful propaganda of

Cyber attack tools, wherefrom an innocent initial post you can enter a file on your computer that allows you to have remote control of your computer.

The objective of investigating this topic is to identify the factors that affect cyber security in remote work, as explained by Abad, 2018, (cited by James Navarro & Gainza Reyes, 2021). To ensure an acceptable level of security it is necessary to achieve security controls effectively, directly, and professionally to communicate to end-users. As well as mitigate the risks of the human factor that could materialize in a cyber attack, and leakage of information through teleworkers. It is important to analyze these factors, as they affect the effectiveness of the digital transformation of heI services at the administrative level – impacting support services for students, staff, and teachers, and academic services in the teaching-learning process (students and teachers). This qualitative research seeks to identify the following: to what extent employees who are in working from home can be victims or sensitive to open a weak point in the security of organizations? And how is it possible to implement a control system and a culture of cyber security in the academic community for the prevention of information leakage and system breaches caused by teleworkers?

This study analyzes the review of the literature that deals with cyber security, and the relationship between teleworking and the use of information and communication technologies (ICT). Then, it continues with the presentation of the outcomes of the interviews conducted with two computers and cyber security managers of government organizations of the Dominican Republic and a general director of ICT of a university in the city of Santo Domingo. Finally, it will end with a reflection of the results obtained in the interviews, and the conclusions reached.

Definitions

Throughout the work, terms that are pertinent to define are used, such as Telework[1]. This refers to the work that is done outside the place of work using telecommunication networks to meet the assigned workloads. In the same way, we use the concept of cyberspace[2], metaphorically referring to the place that the Internet imaginatively presents us as a place or space to share and interact for the work or personal environment.

The threat is mentioned[3], which refers to any harmful situation that can happen and when it happens, it has negative consequences on information assets affecting their operation. They can be carried out by Hackers[4], bone the person who can enter the systems of an organization by linking to them and successfully posing as legitimate users with the rights and privileges of any other user. In some cases, hackers go further, tricking a network into thinking they have the privileges of a system administrator (sysadmin). The term cyberattacks[4] is mentioned, an operation that uses digital information (strings of zeros and ones) to interfere with the operations of an information system and, therefore, produce bad information and, in some cases, bad decisions. They can also be called Security Incident, as the event that affects the pillars of cyber security that are confidentiality, integrity, and availability of information assets.

Cybercrime[1], referring to the criminal activity that takes place through the Internet. Ransomware[2] is when the cybercriminal takes control of the infected computer and "hijacks" the user's information by encrypting it, in such a way that it remains unreadable if the decryption password is not available. In this way it extorts the user by asking for an economic ransom in exchange for this password so that, supposedly, he can recover his data.

The conceptual framework

This qualitative research seeks to identify to what extent employees who are in telework format can be victims or sensitive to open a weak point in the security of organizations? and how it is possible to implement a control system and a culture of cyber security in the academic community, for the prevention of information leakage and violations to systems caused through teleworkers.

It is impossible to notice how the health crisis that began in March 2020, led large and small cities to use information and communications technologies (ICT) to function during the confinement, Cifuentes-Leiton & Londoño-Cardozo, (2020) cited by Vilcacundo-Reinoso, G. I., & Gómez (2021)," presents how they have been modified traditional social relations, and how teleworking was the means that guaranteed and allowed entities to obtain the desired results of their collaborators, breaking the paradigms of face-to-face or compliance with rigid schedules; although teleworking is not new, the COVID-19 pandemic redefined it.

Experts say that cybercrime has doubled since the beginning of the pandemic as a result of the intensive use of technological resources, and may double as teleworking increases, said Vilcacundo-Reinoso, G. I., & Gómez (2021)

[1] Royal Academy of the Spanish Language www.rae.es

[2] Lemley, Mark A. 2003, Place and cyberspace, REVIEW OF CALIFORNIA THE W, Vol. 91:521-542

[3] Cyber Incident Identification & Reporting Guide, Edition: 01, National Cybersecurity Center (CNCS), National Cyber Incident Response Center of the Dominican Republic (CSIRT-RD) June 01, 2020

[4] Martin C. Libicki (2016) (p.21)

quoting Lema, L. L, (2020). They exposed how ransom ware attacks increased due to insecure remote access to corporate networks, and how the lack of knowledge of teleworkers who expose their computer login information. As well as, the use of computer equipment shared with the family, a weakness that can be exploited by cybercriminals compromising the files and information of the institution to which it provides its services, so it recommends a vulnerability analysis.

Another of the vulnerabilities are found in emails, (Fortinet, Inc., 2021) explains how hackers use them to compromise mail servers by executing man-in-the-middle attacks, which allow them to generate new emails by imitating the response and writing styles of the person and commenting on previous conversations. Even now, there are online software tools designed to clone someone's voice, and they can create a vocal fingerprint of someone by using only a few seconds of audio and then generate a provocative, illegal, absurd, or irrational speech in real-time.

Cybercrimes continue to increase, and they go from attacks on intellectual property to cyber bullying among others. Arroyo (2020) highlights how people are vulnerable to cybercrimes since others are able to access credentials or login data. They allow them to have access to privileged information of different types of entities since they have already managed to access credentials or login data, and either for the benefit of the cyber attacker or to be able to obtain benefits with third parties.

Cyber security experts consider it essential that institutions develop programs to prevent and avoid risks derived from the incorrect use of the organization's computer equipment, as they express (James Navarro & Gainza Reyes, 2021; Leornardo, C., 2022; Fortinet, 2021; Garcia, A. A., 2019). Since a user can represent a vulnerability for any entity, and a person can be a point used by cybercriminals, it can be sufficient reason to consider the awareness and training of collaborators as a priority of computer security.

These approaches are like García, A. A. (2019) states when he says that the human factor needs special attention, due that criminal groups and competing institutions that are looking for the opportunity to identify vulnerability in our information management, and comprehensive security system. Recalling the specific value of information with the words of Menguzzato and Renau (1992), when they expressed "that the costs of all information can be estimated based on the content of the information required, the speed with which the information is required, the amount of information needed and the accessibility of that information.”

Experts such as García, A. A. (2019) make recommendations to higher education institutions on the need to redesign their cyber security strategies and implement policy and good practices that allow them to effectively safeguard the valuable assets that the institution. In the same manner, James Navarro & Gainza Reyes, (2021) affirm that the controls can be tailored to the specific needs of each organization for their implementation, providing a protective barrier for information, and considering people as the weakest link in the chain. Under this premise, we can say that it is necessary to create or implement institutional regulations in the field of cyber security, with the idea of realizing or hiring personnel in the modality of telework to prevent, and mitigate cyber security risks through the correct management of information by teleworkers.

Methodology

The paper was completed using the qualitative method, along with the analysis of the literature regarding cyber security in organizations that have implemented teleworking, as well as the main weaknesses it faces.

Six (6) cyber security executives were chosen to provide insights in relation to the topic, three were from universities, and three were government institutions in Dominican Republic. The last three executives are responsible of protecting and establishing cyber security action protocols in the country; however, I was only able to achieve a total of three structured online interviews, one from a university executive and two from government officials.

The instrument had eight variables, first, focused on identifying the opinion of the interviewees about the role of the users of the computer; and second, identify the main weaknesses. Then, the importance and need to train these for the prevention of cyber security of organizations. To achieve the interviews, the instrument was sent via email, and a subsequent meeting through Teams to discuss the variables was sent. The interviewees were:

1. Carlos Leonardo, Director of the National Cyber Incident Response Team, National Cyber security Center of the Dominican Republic, Email: carlos@cncs.gob.do
2. César Moliné Rodríguez, Director of Cyber security, Electronic Commerce and Digital Signatures, Dominican Institute of Telecommunications, INDOTEL, Office: 809-732-5555 Ext.:6187, Email: cmoline@indotel.gob.do
3. Ricardo Augusto Pérez Álvarez, Director General of Information Technology, Universidad APEC, UNAPEC, Email: raperez@adm.unapec.edu.do

Results and Discussion

The main risks and weaknesses that have been identified, which have a key impact in the violation of systems and networks in private institutions in the last two years, the interviewees agreed that many organizations went virtual without being prepared, opening up to considerable gaps for emerging threats. The main threats that affect Dominican cyberspace have been the theft of information, intrusion into systems, fraud, attacks on the availability of systems, abusive content, compromise of information, and malicious codes; this last includes events such as phishing, malware, modification or deletion of information, exploitation of vulnerabilities, ransom ware, among others.

Mr. Ricardo Pérez, shed light from an educational perspective, stating that there are vulnerable points through information systems. He highlights access to the internet. Such as the Student or Teacher Information System, and internal attacks on the institutional database.

In addressing the main causes of system violations in private institutions, Mr. Carlos Leonardo, agrees with the opinion of authors such as Vilcacundo-Reinoso, G. I., & Gómez (2021)," and the company Fortinet Inc., which establish that the lack of knowledge on the part of users weakens cyber security controls. While Mr. Moline and Mr. Pérez agree that threats and incidents increase due to the dependence of society and young people, and how criminals are increasingly organized to assess existing vulnerabilities in known institutions to exploit them and make themselves known.

Dominican state officials comment that actions have been established to mitigate cyber security risks, through mandatory controls for organizations, and how they have understood the importance of the user's role in cyber security. As well as institutions, assume the importance of preventing and mitigating threats. An express that being a global problem requires solutions that involve all actors from the public and private sector, civil society, academia, the international community, among others. Since the measures should not be limited to the technical or legal characteristics, but as Cesar Moline says, "it is necessary to assess psychological, sociological and educational factors that allow us to determine what will be the new threats that we will face in the near future."

As previously agreed, that the digital transformation came as a surprise and many institutions were not prepared for the adoption of teleworking for example, within the main controls they recommend to reduce the risks of being subject to cyber attacks, at the government level the National Cyber security Center has developed guides of action focused on the efficient management of teleworking and remote access security, as well as the use of mobile devices for professional use, which allow to establish controls that protect the devices of the collaborators, even if they are for personal use, the recommendation of double authentication and "Zero Trust" to access all remote services of the organization, and as vital establish to create awareness and knowledge of the risks and threats to all employees of the organization.

In the case of the university, the protection of your data is through third parties, centralized all the actions of the collaborators in cloud services, thus giving the ease of stopping access to your information and meetings from any smart device without losing the security aspects provided by this cloud solution. In the same way, the administration of the technological equipment has been centralized in the same tool, which can notify the administrators of security patches that the equipment has within the infrastructure.

Some of the questions addressed are linked to the considerations of some authors, who consider that collaborators are the weak point in the search for weaknesses of a cyber attacker, a point of total agreement on the part of the three interviewees, considering the end user, as the weakest link in the security chain, because it is in the first line of defense against cyber threats, and their ignorance puts at risk an entire network with the simple fact of clicking on a link within an email or visiting ill-intentioned websites. Establishing that, regardless of the technological solutions implemented in an organization, the entry point of threats are users.

Reason why they consider that it is essential that the user knows the cyber risks and how to come from them, with general aspects of social engineering to help people take measures to avoid being a victim of this type of attack. Reason why they confer on the end user a medium to high degree of responsibility, on a scale of 1 to 10, the responses received were between 6 and 10, considering that effective cyber security requires that each individual and each part of the organization be an active actor and work together as a team, with tools that provide the necessary infrastructure to protect the organization's assets, as well as the implementation of cyber security policies and standards. Considering that employees should not be the weakest link in the organization but the greatest resource if they are aware of the risks and threats, informed and motivated to collaborate.

Considering the cyber security training of end users with the highest level of importance, expressing as an essential requirement to have a secure cyberspace, considering that effective cyber security training is the key, to change the way in which employees perform their work. Valuing the appropriate knowledge of the user, helps to determine or discern that it could be an eventual cyber threat that not only exposes it as individual users, but to the organization, it can even serve to avoid incidents to the critical infrastructure of our country or even to other countries. So, they recommend a continuous training program that is updated periodically.

When asking cybersecurity experts about their recommendations or exhortations to the directors of computer security of the country's higher education institutions, they value the impact and influence of he is, as part of the cybersecurity ecosystem, for the reach it has through students, collaborators, graduates and peer organizations, as well as the degree of advocacy to disseminate updated and quality information in their formal and informal educational programs.

Making an assessment that organizations have the need to have accurate, relevant and timely information to optimize administrative and management tasks, its recommendations are aligned with the need to establish protocols that generate trust, encouraging people to talk about mistakes and rewarding proactive behavior, for which it is necessary to listen, learn and lead with empathy.

Considering that effective security comes from having tools and solutions that are easy to implement and follow, as well as from adequate security policies and mechanisms for your IT infrastructure, supported by technical, organizational, and procedural measures that allow you to minimize cybersecurity threats and incidents such as breaches or leaks of personal data and corporate information, making the recommendation to apply and promote technological security practices among members of the academic and administrative community to maintain adequate protection of the information that is processed in their systems.

Conclusions

This analysis is made from an empirical approach, which may lead to the beginning of more comprehensive research covering many institutions. Based on the analysis of the interviews made and the review of the literature, we can reach the conclusion that collaborators and users are part of the access points of cyber attackers, therefore, they are medium to high-level weak points of security of organizations.

The main reason that employees are a vulnerable access point in the cybersecurity organizations, is the lack of knowledge about the dangers and threats, and the lack of ability to identify them. Therefore, if the user does not have the knowledge, and tools to implement the measures provided by the institutions the security will continue to be subject to cybercrimes.

Finally, it is key to recognize the human factor and its consequence, as it is its lack of knowledge and preparedness that leads to the majority of cyberattacks. Therefore, it is essential to develop programs within the institutions that address the awareness for the prevention of information leakage and breach of systems caused by teleworkers, and any other user of the organization such as teachers and students.

Works Cited

FortiGuard Laboratories. (2021). *Global Threat Landscape Report.* Fortinet Inc. Fortinet Inc. Obtained from www.fortinet.com

Fortinet, Inc. (2021). *Cyber threat predictions for 2022.* FortiGuard Labs. doi:1346406-0-0-EN

James Navarro, M., & Gainza Reyes, D. (July 2021). Information security procedures related to human resources. *Scientific Series of the University of Computer Sciences, 14*(7), 108-122. doi:ISSN: 2306-2495 | RNPS: 2343

Pérez Pérez, M., Martínez Sánchez, A., Carnicer, P., & Vela Jiménez, M. J. (2005). The adoption of teleworking and information technologies: study of relationships and organizational effects. *When talking about computer security, it is often heard that the human factor is the weakest link*(52 and 53), 11-27.

Pons Gamon, V. (June 2017). Internet, the new era of crime:. *URVIO, Revista Latinoamericana de Estudios de Seguridad*(20), 80-93. doi:https://doi.org/10.17141/urvio.20.2017.2563

Puime Maroto, J. (2009). Cyberespionage and cybersecurity. In B. López Rodriguez, *La violencia del siglo XXI. New Dimensions of War,* (pp. 45-76). doi:ISBN 978-84-9781-501-7

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company.

Viancha Acero, L. I., & Sarmiento Gámez, N. F. (2021). Methodological strategy to minimize risks of leakage of business information in teleworking. *Uniersiad St.* Thomas.

Vilcacundo-Reinoso, G. I., & Gómez, O. S. (October 2021). Proposal of Cybersecurity policies for Teleworking. Case study of the Rector of ESPOCH. *Scientific Journal Domain of Science, 7*(6), 63-82. doi:http://dx.doi.org/10.23857/dc.v7i6.2315

Garcia, A. A. (2019). Cybersecurity: Why is it important for everyone? Siglo XXI Editores México. GARCÍA, Adolfo Arreola. Cybersecurity: Why is it important for everyone? Siglo XXI Editores México, 2019.