Impacts of Cybersecurity on the Global Economy

Cybersecurity Impacts on the Global Economy

Wanderley Martins Junior[1]

Submitted on: 01/31/2023
Approved on: 02/01/2023
Published on: 02/06/2023 DOI
10.51473/ed.al.v3i1.478

Summary

This article aims to portray the position of various government and private entities when dealing with topics relating to cybersecurity. It is common to see in social and digital media that the world is experiencing several challenges when it comes to cyber attacks, invasions in corporate environments, information theft, data leaks, extortion and even problems related to privacy. With the expansion and elasticity of the internet, several new technologies have emerged allowing more and more forms of interaction and possibilities. It is in this interactivity that we must coldly worry about security from a globalized point of view. So, the idea here is to present and understand how all these items can, together or separately, directly affect the global economy. Many companies feel threatened by the most dangerous resources that can put them at risk, but as a result they are not prepared to protect themselves from attacks such as*Ransomware*, in which attackers hijack data for ransom. In this work we will mention some damages that can be caused by corporate default, or simply by groups of invaders targeting government bodies with the aim of mass destruction. Finally, we will identify some resources that may be favorable for mitigating these intrusions and attacks, as well as outline ways to keep risks at an acceptable level.

Key words: 1. Global Economy 2. Cyber Security 3.*Ransomware*4. Risks

Abstract

This article aims to portray the position of the various governmental and private entities when dealing with issues related to cybersecurity. It is common to see in social and digital media that the world has been experiencing several challenges when it comes to cyber-attacks, invasions in corporate environments, information theft, data leakage, extortion, and even problems related to privacy. With the expansion and elasticity of the internet, several new technologies have emerged allowing more and more forms of interaction and possibilities. It is in this interactivity that we must coldly worry about security from a globalized point of view. So, the idea here is to present and understand how all these items can, together or separately, directly affect the global economy. Many companies feel threatened by the most dangerous resources that can put them at risk, but as a result, they are not prepared to protect themselves from attacks like Ransomware, where attackers hijack data for ransom. We will cite in this work some damage that can be caused by corporate default, or simply by groups of invaders targeting government agencies with the aim of mass destruction. Finally, we will identify some resources that can be favorable for mitigating these intrusions and attacks, as well as outline ways to keep the risks at an acceptable level.

Keywords:1. Global Economy 2. Cyber Security 3. Ransomware 4. Risks

1Master's student in Business Administration at Must University. Specialist in Information Security Management (UNICIV). Technologist in Information Security Management and Cyber Defense (UNINTER). CV lattes:http://lattes.cnpq.br/9768260128060816 / email:wanderleymjr@protonmail.com

1. Introduction

Cybersecurity has been a hot topic since the start of the Covid-19 pandemic. The possibility of teleworking, the mandatory lockdown demanded by governments around the world and companies being forced to change their paradigms to continue to survive, were immediately problems and/or palliative solutions imposed by this pandemic. When we refer to paradigm shifts, these were new *modus-operandi* necessarily created to meet the demands of companies, such as adapting their environments, employees, suppliers and all those *stakeholders* directly impacted. This brings us to the reality that many of these organizations have had to reevaluate their computing assets, introducing new technologies and new adaptation processes.

We must consider, according to (Bandyopadhyay,2023, p. 1) that "new technologies or services introduce new cyber risks that need to be assessed, prioritized through impact analysis and mitigated through a process, technology, skills and governance perspective."

WEF (2023) explains that:

> Geopolitical instability, emerging and rapidly maturing technologies, lack of available talent, growing shareholder participation, and regulatory expectations represent some of the significant challenges that concern cyber and business leaders (...) technologies are now shared across multiple organizations . These organizations consequently have common dependencies or weaknesses.

And with all these problems seriously drawn, some organizations were suddenly limited, exposed and unprotected, which gave rise to something we can call "***cyberterrorism*** in large scale".

(Pinto, 2011, p. 9) defines cyberterrorism as:

> Acts based on political, ideological or social motivations and hacking operations with the aim of causing severe damage (loss of human life, economic losses, attacks or threats against computer systems, networks and the information stored therein) in order to intimidate or coerce a government. It can be a physical attack with the aim of destroying computerized networks of critical infrastructures (Internet, telecommunications) or the electrical grid of a country or city.

According to Dijk (2019), two years before the pandemic, cyber attacks and the threats contained therein were already the fifth biggest concern for organizations around the world and were considered by the World Economic Forum (WEF) as a priority risk number one, mainly in North America, Europe and eastern Asia-Pacific.

This article aims to explore the socioeconomic problems that are directly affected by Cybercrime in the context of cyberterrorism.

For the context of this article, we will use amethodology in the nature of descriptive research focusing on bibliographical research and resources from reliable sources extracted from the internet.

2. Cyberterrorism combined with the global economy

Cyberterrorism is an emerging topic in many parts and sectors around the world. It involves all types of crimes that can be committed digitally, better known as cybercrimes. “Cyberterrorism is the disruptive use of information technology by terrorist groups to advance their ideological or political agenda. This takes the form of attacks on networks, computer systems and telecommunications infrastructures” (Ciaramello, 2019, p. 1).

Cybercrime has become a terror throughout the world. Thousands of companies suffer cyber attacks annually. And, today, it would be impossible to measure the impact this causes on public coffers and private initiatives.

> If measured as a country, cybercrime – which inflicted damage totaling $6 trillion globally in 2021 – would be the world's third-largest economy after the US and China. According to experts, the global costs of cybercrime are expected to grow 15% per year over the next 5 years, reaching 10.5 trillion dollars per year by 2025, up from 3 trillion dollars in 2015. (Brasiline, 2022, p. 1)

Pinto (2011) says that the*cyber terrorists*They are normally young males, academically grounded (Masters or Doctors), who are aware that they are violating the Law and order and causing disrespect to society, as well as disrupting social order systems.

According to James (2023), hackers are constantly changing their ways of bypassing security and carrying out more attacks on commercial assets. The world experiences around 2,200 cyber attacks daily. Data states that there is a hacker attack every 39 seconds, and around 300 thousand malware are created each year.

Still on the global economy related to cybersecurity, (Brasiline, 2022, p.1) explains that:

> The costs of cybercrime include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption in the normal course of business, forensic investigation, restoration and data deletion hacked data and systems and damage to reputation.

(Pinto, 2011, p. 9) states that “cybercrime is an act based on or targeting computer systems. It may involve theft of intellectual property, patent infringement, theft of trade secrets, violation of copyright laws, and identity theft.” He further explains that cyberterrorism is similar to cybercrime in an expanded version, but that it has worse consequences.

“Cybercrime is a low-risk crime that offers high returns. A smart cybercriminal can make hundreds of thousands, even millions of dollars, with almost no chance of being arrested or jailed.” (CSIS, 2018, p. 4)

There are many challenges caused by the damage caused by cyberterrorism. Therefore, companies need to anticipate and put together a strategy to contain this range of criminal actions. One of the options that companies went through to be contracted more frequently and is gaining more and more popularity in the market is cyber insurance. It can be compared to car insurance in the sense that it aims to protect the company in the event of damage to infrastructure or moral damages. (Vandiver; Murphy, 2023, p. 1) state that:

> Cybersecurity insurance protects businesses against financial losses caused by incidents such as data breaches and theft, system hacking, ransomware extortion payments, and more. If your small business stores sensitive information online or on a computer, you should have at least some cyber insurance coverage.

2.1.Hacktivism and Hacktivists

We will bring to our article two very relevant topics in the world of cyberterrorism. The first of these refers to the concept of "*hacktivism*".

> Hacktivism deals with the combination of two concepts: online activism (or cyberactivism) and the practice of hacking. In other words, it is a form of manifestation that uses the internet to disseminate information, in a set of methods known by hackers (individuals with great knowledge of computers), normally illegal, and may be destructive, so that the transmission of messages reaches a greater number of people. (Arimura, 2016, p.1)

The second portrays which authors act in manifestations of*hacktivism*, better known as *hacktivists*. Stouffer (2021) states that the*hacktivists*are online activists who seek out injustices committed by religious, social and political orders and try to draw public attention to a cause that is important to them, with the intention that these acts bring about changes and improvements.

You*hacktivists*fall under cybersecurity as cyberterrorists, considering that their actions have the same focus, direction and generally the same target audience.

Here we can cite some examples of the most common attacks carried out by*hacktivists*: defacement and redirection of websites, distributed denial of service attacks (DDoS), data leakage of public information, geographic bombing with the aim of revealing the location of political prisoners and human rights activists, among others.

About groups*hackitivism*, Arimura (2016) explains that "Anonymous" is one of the most well-known and influential in the world. It includes people of different nationalities, who always use the concept of anonymity, and have as a symbol the mask worn by the protagonist of the film "V for Vendetta", released in 2005 by Alan Moore.

Other groups*hacktivists*of note are WikiLeaks, LulzSec and the Syrian Electronic Army.

3. Ransomware: the biggest cyber threat

O*Ransomware*is a type of malware or virus designed to steal confidential information from a wide range of operating systems, directories, and hardware and software assets in general. Once the attacker finds valuable data, he uses the encryption feature to make this data unavailable to the user responsible for it. This attack is considered one of the oldest, with data occurring since the 90s.

> This is the most famous because it was widely used during the Covid-19 pandemic. This is a type of malware that enters systems in order to hijack data and demand ransom payments. A huge number of companies have fallen victim to this type of attack in recent years, causing financial and reputational losses. (Mack, 2022, p.1)

Comparitech (2022, p. 1) explains that "some research has shown that losses for companies can reach $2,500 on average for each incident, with companies willing to shell out millions of dollars to decrypt their data in some cases." However, according to Armis (2023), whether nation-state actors or cybercriminals, the anatomy used by a ransomware attack is relatively the same. Attackers first look for a way to gain access to the environment through a compromised website, use of*Phishing*or a targeted attack. Once inside the environment, attackers move laterally through the network, escalating privileges to gain access as administrators and infiltrate the network.

Attacks of this type have been taking away the peace of many companies around the world and events such as Russia-Ukraine wars are often a gateway of weakness for cyber gangs to attack freely.

Constantin (2023) says that there have been changes in the ecosystem of *Ransomware* in the year 2022. The use of *Ransomware* as a service (RaaS) was reduced so that attackers could be more flexible and not draw so much attention from the law. He further states that groups of *Ransomware* they may have improved their alliances with criminal members and affiliates in Russia, Ukraine or other countries of the former USSR.

As for the types of *Ransomware*, we can see in the table below with data provided by ESET (2022):

Tipo de Ransomware	Objetivo
Diskcoder	Utiliza o serviço de criptografia em todo o disco da máquina e impede o acesso do usuário alvo ao sistema operacional.
Screen locker	Utilizado para realizar o bloqueio da tela do dispositivo, não permitindo que usuário acesse sem conseguir o código.
Crypto-ransomware	Criptografa arquivos que ficam armazenados dentro do disco da máquina do usuário alvo.
PIN locker	Ataque aos dispositivos Android que tenta bloquear o aparelho e impedir que o usuário alvo possa acessá-lo sem um código.

Table 1- Types of Ransomware

There are still many variants of the virus *Ransomware* and among the most famous we can mention PC Cyborg, Locky, WannaCry, Rokku and Petya. All of these have their particularities, but the final objective is generally the same, extortion. To do this, the attacker always looks for a "ransom" value so that those attacked receive the key to unlock access and get their data back. However, Miller (2017, p. 8) warns that:

> There is no honor among thieves. Although an attacker will usually provide the decryption key for your files if you pay the ransom, there is no guarantee that the attacker has not already installed other malware and exploit kits on your endpoint or other networked systems, or that they will not steal your data for other criminal purposes or to extort further payments in the future.

There are many strategies used by cyber scammers when they think about carrying out this type of attack. According to Inforchannel (2022), these scammers need to have a better understanding of the relevance of the information to be acquired, taking into account steps to carry out the attack. The first of these would be the study of the victim, especially whether they have the potential to pay the ransom in accordance with the amount that the attacker intends to receive. The second step would be how the criminal will gain access to the victim's corporate network.

4. Final Considerations

We live in the famous "information age" in which the increase in digital interaction possibilities has made the internet a niche for various malicious actors to commit cybercrimes around the world. This increase is increased by the devastation caused by the COVID-19 pandemic, a period in which public and Private companies are more vulnerable.

In this article, we saw a synthesis of the impacts caused by cyberterrorism on the global economy, with dis- cybersecurity threads when mitigating, containing and resolving the most diverse scams, extortion and other attacks that could compromise a company's activities. We briefly mentioned the concepts of cyberterrorism and cybersecurity, the use of cyber insurance, as well as what the *Hacktivism*, its actors and potential vectors.

Finally, we explore information about the*Ransomware*, considered one of the imminent and most widespread in the world in terms of protection, data leakage and criminal extortion.

Without a doubt, in the coming years many challenges will still come in terms of cybersecurity. And to this end, we hope there will be an evolution of some technologies that will allow the reduction or containment of cyber attacks.

References

Arimura, M. (2016).**Hacktivism: villains or good guys?**Portal for e-government, digital inclusion and knowledge society (E-Gov). [online]. Available in:https://egov.ufsc.br/portal/conteudo/hacktividade-vil%C3%B5es-ou-mocinhos Accessed on December 14, 2022

Armis. (2023).**The state of Cyberwarfare**:Armis state of Cyberwarfare and trends report 2022-2023. [online]. Available in: https://www.armis.com/cyberwarfare/ Accessed on January 10, 2023

Bandyopadhyay, S. (2023).**Cybercrime is now the world's third-largest economy**. [online]. Khaleej Times Journal. Available in:https://www.zawya.com/en/legal/crime-and-security/cybercrime-is-now-the-worlds-third-largest-economy-hwpvrkdl Accessed on January 20, 2023

Brasiline. (2022).**Cybercrime as an empire would be the third largest economy in the world**. Brasiline Technology. [online]. Available in:https://brasiline.com.br/blog/o-cibercrime-como-imperio-seria-a-terceira-maior-economia-do-world/ Accessed on January 20, 2023

Ciaramello, Marina. (2019).**Information hijacking and cyber espionage are the main cyber threats for companies**. [online]. Available in:https://www.segs.com.br/info-ti/190703-sequestros-de-informacoes-e-cyber-espionage-is-the-main-cyber-threats-to-companies Accessed on January 25, 2023

Comparitech. (2022).**2018-2022 Ransomware statistics and facts**. [online]. Available inhttps://www.comparitech.com/software-supply-chain-attacks/ Accessed January 10, 2023

Constantin, L. (2023).**Ransomware ecosystem diversifies before 2023**. [online]. Available in:https://www.comparitech.com/antivirus/ransomware-statistics/ Accessed on Jan 18, 2023

CSIS. (2018).**Economic impact of Cybercrime: No slowing down**. [online]. Available in:https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf Accessed on January 20, 2023

Dijk, Gina Van. (2019). "**Why cyberattacks are a global concern**". [online]. Available in:https://neofeed.com.br/dados-blindidos/por-que-os-ciberataques-sao-uma-concecao-global/ Accessed on January 10, 2023

ESET. (2022). What is ransomware? [online]. Available in:https://www.eset.com/br/ransomware/ Accessed on January 20, 2023

Inforchannel. (2022).**Kaspersky warns: ransomware groups use Red Teaming tools**. [online]. Dis-

available at:https://inforchannel.com.br/2022/06/27/kaspersky-alerta-grupos-de-ransomware-usam-ferramentas-de-- red-teaming/ Accessed on Jan 20, 2023

James, Nivedita. (2023).**160 Cybersecurity Statistics 2023**–The Ultimate List of Statistics and Trends. [online]. Available in:https://www.getastra.com/blog/security-audit/cyber-security-statistics/ #Top_Cybersecurity_Statistics_2023 Accessed on January 10, 2023

Mack, Cecilia L. (2022).**Cyber attacks expected to continue in 2023**. [online]. Available in:https://www.segs. com.br/ info-ti/366234-ataques-ciberneticos-devem-continuar-em-2023 Accessed on January 15, 2023

Miller, Lawrence. (2017).**Ransomware defense for dummies®**, Cisco Special Edition. New Jersey: John Wiley & Sons.

Pinto, Marco AG (2011).**Relativistic theory of cyberterrorism**. Dissertation to obtain the degree of Master in Information Warfare. Military Academy. Lisbon. Available in:

https://comum.rcaap.pt/bitstream/10400.26/6826/1/Ciberterrorismo_tese_VersFinal.pdf Accessed on January 15, 2023.

Stouffer, Clare. (2021).**Hacktivism: An overview plus high-profile groups and examples**. [online]. Available in https:// us.norton.com/blog/emerging-threats/hacktivism# Accessed on January 25, 2023

Vandiver, W., & Murphy, R. (2023).**Cybersecurity Insurance: What It Covers, Who Needs It**. [online]. Available in: https://www.nerdwallet.com/article/small-business/cybersecurity-insurance Accessed on January 20, 2023

WEF. (2023).**Global Cybersecurity Outlook 2023**. World Economic Forum. [online]. Available in:

https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

Accessed on January 25, 2023