CZU: 341.4 DOI: 10.5281/zenodo.6400687

CYBER SECURITY'S NEW CHALLENGES UNDER COVID-19 PANDEMIC: BETWEEN TECHNIQUE AND LAW

Corina DODI, PhD in Law, Associated Professor (ORCID: 0000-0003-3906-1372)

COVID-19 has changed the way cyber security is viewed by corporations in the global community. "Data is the new oil" — the value of information has become comparable to the value of raw materials. Information becomes especially important in the context of its processing using machine learning and other modern technologies. The more valuable information is for a business and civil society, the greater the need to protect it. Cybersecurity refers to one of the branches of information security and covers the protection of data in the networks of companies and organizations, as well as the protection of private information of individuals. Cybersecurity has a huge importance to business, civil society, governments, national and international critical infrastructure and includes protecting information systems and data from cyber threats such as computer fraud, espionage, sabotage or vandalism.

Keywords: *cybersecurity, COVID-19, healthcare system, cybersecurity legislation, cyber-attacks, cybercrimes*

Noile provocări ale securității cibernice în prioada pandemica COVID-19: între tehnică și lege

„Datele sunt noul petrol" — valoarea informațiilor a devenit comparabilă cu valoarea materiilor prime. Informația devine deosebit de importantă în contextul prelucrării ei folosind învățarea automată și alte tehnologii moderne. Cu cât informațiile sunt mai valoroase pentru o afacere și societatea civilă, cu atât mai mare este nevoia de a le proteja. Securitatea cibernetică se referă la una dintre ramurile securității informațiilor și acoperă protecția datelor în rețelele companiilor și organizațiilor, precum și protecția informațiilor private ale persoanelor fizice. Securitatea cibernetică are o importanță imensă pentru afaceri, societatea civilă, guverne, infrastructura critică națională și internațională și include protejarea sistemelor informaționale și a datelor împotriva amenințărilor cibernetice, cum ar fi frauda informatică, spionajul, sabotajul sau vandalismul.

Cuvinte-cheie: *securitate cibernetică, COVID-19, sistem de sănătate, legislație privind securitatea cibernetică, atacuri cibernetice, infracțiuni cibernetice*

The restrictions imposed by governments in response to the coronavirus pandemic have encouraged employees to work from home, and even 'stay at home'. As a consequence, technology has become even more important in both our working and personal lives. Despite this rise of technology need, it is noticable that many organisations still do not provide a 'cyber-safe' remote-working environment. Where business meetings have traditionally been held in-person, most now take place virtually.

In June 2020 Swissinfo.ch reported figures from the NCSC (National Cyber Security Center) showing that there were 350 reported cases of cyberattacks (phishing, fraudulent web sites, direct attacks on companies etc.) in Switzerland in April, compared to the norm of 100-150. The coronavirus pandemic and increase in working from home were seen as a major cause of this increase, since individuals working at home do not enjoy the same level of inherent protection/deterrent measures from a working environment (e.g. internet security).

An example of criminals exploiting the cybersecurity weaknesses in remote working has been the series of cyberattacks on video conferencing services. Between February 2020 and May 2020 more than half a million people were affected by breaches in which the personal data of video conferencing services users (e.g., name, passwords, email addresses) was stolen and sold on the dark web. To execute this attack, some hackers used a tool called "Open Bullet".

Hackers also use credential stuffing techniques to gain access to employees' credentials and the stolen data is then sold to other cybersecurity criminals. One of the consequences is a serious disruption to businesses that rely heavily on videoconferencing platforms. Credential stuffing is a form of cyberattack whereby hackers use previously-stolen combinations of username and password to gain access to other accounts. This is possible because it is very common for individuals to use the same username/password combination across multiple accounts[1].

The disruption due to COVID-19 has disclosed the weaknesses of existing institutions in protecting human health and well-being. A lack of timely and accurate data and widespread misinformation have caused ever-increasing harms and growing tension between public health concerns and data privacy. In the absence of accurate data and reliable information, the suffering due to COVID-19 has been worse. The COVID-19 crisis is an information crisis as well as a trust crisis. It has underlined failures of existing systems in trust and data sharing. During the crisis, main supply chain failures have been noticed, especially for personal protective equipment (PPE) and lifesaving ventilators in clinics and hospitals.

Digital methods have played a significant role during the COVID-19 pandemic. However, there are telemedicine challenges and other digital approaches in privacy and security for protected information. Since the beginning of the COVID-19 pandemic, there has been remarkable increase in the number of cyber-attacks. During the pandemic, major cyber risks are caused by people`s actions as well as failures of systems and technology. The source of operational risk includes people`s actions, for example, deliberate (e.g., theft, sabotage, fraud, and vandalism), inadvertent (i.e., omissions, errors, and mistakes), and inaction (e.g., availability, knowledge, skills, and

[1] Impact of COVID-19 on Cybersecurity URL: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

guidance). Failures of systems and technology lie in software (i.e., coding practices, testing, security settings, change control, configuration management, and compatibility), hardware (i.e., capacity, performance, maintenance, and obsolescence), and system (i.e., specifications, design, integration, and complexity)[2].

Clinic and hospital cyber security are an integral part of running a health care business. And when a crisis like the COVID-19 pandemic occurs, health care cyber security is crucial to maintain patient data, remote communications technology and smooth facility operations, especially where high numbers of confirmed cases are present[3].

A major hospital in Brno, the Czech Republic's second-biggest city, was hit by a cyber-attack on March 13, 2020. According to the hospital's management, the attack forced the staff to postpone urgent surgical interventions, reroute new acute patients, and reduce some of their other activities. The hospital is in charge of administering coronavirus tests in the city and the disruption delayed the processing of the tests by several days. Since then, cyber incidents targeting the health-care sector have been reported in a number of countries, including France, Spain, Thailand and the United States.

In a situation where most, if not all of us are potential patients, few government-provided services are more important than the efficient delivery of health care. The strain on hospitals around the world is rapidly growing, to which States have responded by mobilizing military medical units, nationalizing private medical facilities, and building emergency hospitals. It is essential that all of these facilities can function without interruption and that they have sufficient resources as they scale up their operations due to the unfolding crisis. However, as noted in a 2019 International Committee of the Red Cross (ICRC) report on the potential human cost of cyber operations, even in ordinary times the health-care sector is particularly vulnerable to cyber attacks due to its increasing digital dependency and "attack surface"[4].

In today's highly connected, interdependent world, several critical infrastructure (CI) sectors, such as health care (especially in our COVID-19 pandemic days), telecommunications, finance, energy, among others, increasingly rely on information technology (IT) and operational technology (OT) systems. Not only are these critical information infrastructures (CII) in their own right, for example, cloud-based technology services, but they also underpin many other critical services, for example, water supply, power grids, and fuel pipeline supply. The malfunctioning or disruption of these critical services could cause significant social and economic harm and

[2] Lidong Wang, Cheryl Ann Alexander Cyber security during the COVID-19 pandemic // AIMS Electronics and Electrical Engineering, 5(2): 146-157

[3] Health Care Cyber Security During Epidemics URL: https://onlinedegrees.und.edu/blog/health-care-cyber-security-during-epidemics/

[4] Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections? URL: https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/

even loss of life. For this reason, key stakeholders from the CI/CII ecosystem should adopt a strong cybersecurity posture to ensure the protection and cyber-resilience of CI/CII sectors and services.

To achieve this goal, CII operators should allocate sufficient resources to adopt and implement cyber-tools and internationally recognized security standards (at least as good practice) and also comply with domestic CIIP policy and legal frameworks (if any) to protect their information and communications technology (ICT) infrastructures and data from increasing cyber-risks and attack vectors.

On the other hand, governments, through coordinating authorities, should also allocate sufficient resources to implement and monitor critical information infrastructure protection (CIIP) policy and regulatory frameworks with clear legal mandates, roles and responsibilities, security requirements, and legal obligations to ensure that the CII's sectors and services are adequately protected[5].

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.

Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks.

As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of people depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission[6].

The international political community has recognized the salience of cyberspace and the potentials for cyberthreats that undermine the security of states and create instability in the overall modes of international relations. For example, in 2010, the Secretary General of the United Nations transmitted to the General Assembly the Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security.

[5] Enhancing the protection and cyber-resilience of critical information infrastructure URL: https://digitalregulation.org/enhancing-the-protection-and-cyber-resilience-of-critical-information-infrastructure/

[6] CYBERSECURITY. CISA leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life. URL: https://www.cisa.gov/cybersecurity

The Report states bluntly that "there is increased reporting that States are developing Information and Communication Technology (ICTs) as instruments of welfare and intelligence, and for political purpose." The Report proceeds with an explicit enumeration of the Experts' assessments and recommendations. Interestingly, the words "cybersecurity" and "cyberspace" — spelled in any form, with or without hyphens or spaces — do not appear anywhere in the text. The words that are conventionally used are "information and communications technology"[7].

A strong cybersecurity strategy has layers of protection to defend against cybercrime, including cyber-attacks that attempt to access, change, or destroy data; extort money from users or the organization; or aim to disrupt normal business operations. Countermeasures should address[8]: Critical infrastructure security, Network security, Application, Cloud security, Information, End-user education, Disaster recovery/ business continuity planning.

Countries do not even use the same terms, some apparently preferring to use the term "information security" over "cybersecurity". Yet, under international law, what governments perceive (legitimately or not) as cybersecurity threats bears special significance. On this point, for instance, following the distinction above between privacy and security, the USA concerns regarding China's regime of cross-border transfer of data would fall under the umbrella of privacy.

Concerns relating to China's restrictions on the use of virtual private networks (VPNs) and leased lines may fall under the umbrella of security. But if one accepts that cybersecurity covers social, cultural, and sociocultural concerns and threats, as further discussed later in this article, then the distinction between the two blurs and privacy-related concerns become so entrenched with cybersecurity ones that distinguishing them in practice may become impossible. As a case in hand, both the Chinese and Vietnamese cybersecurity laws cover several areas, including data security and control over domestic data flows. Along the same lines, as subject to criticism as it may be, the USA has had extremely broad views of what is cybersecurity[9].

It is a consensus that cybersecurity concerns have presented significant national security challenges. Cybersecurity concerns have become a major source of allegations and growing commercial disputes as different cybersecurity policies are implemented, like various barriers to international trade and investing. These policies will shape not only cyberspace for the countries themselves, but the broader globalized society.

Although we have witnessed many international trade restrictions due to cybersecurity concerns, such as Kaspersky's ban in the U.S., LinkedIn's restriction in

[7] Nazli Choucri, Gihan Daw Elbait, Stuart Madnick, 'What is Cybersecurity? Explorations in Automated Knowledge Generation', Massachusetts Institute of Technology Political Science Department Working Paper No. 2012-13 (2012), at 4, SSRN version, URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2178616

[8] What is cybersecurity? URL: https://www.ibm.com/topics/cybersecurity

[9] Gabriele Gagliani Cybersecurity, Technological Neutrality, and International Trade Law Journal of International Economic Law, 2020, 23, 723-745 — P.725-726

Russia, the restriction of data flow to India from the E.U., the restriction of VPN in China etc., there exists no systematic framework to understand how cybersecurity concerns evolve in the international trade context. Of particular concern, recently the international community has become trapped in a "tit for tat" circle, which may eventually result in a "cyber cold war". Without a clear understanding of larger impacts, governmental agencies are implementing policies that may result in cyber conflicts, while businesses struggle to adapt to evolving cybersecurity concerns and restrictions[10].

Cybersecurity measures may be inconsistent with a number of trade obligations, including nondiscrimination obligations, rules on market access for goods and services, or IP rights protection. As a case in hand, data-localization measures may heavily affect trade in services by increasing the costs incurred by service providers and reducing their competitiveness, ultimately being inconsistent with obligations under the General Agreement on Trade in Services (GATS).

Furthermore, practices aiming at favoring the licensing of technology-related IP rights may result in a violation of obligations under the TRIPS Agreement. It goes without saying that the inconsistency of any cybersecurity measure with countries' international trade obligations should be thoroughly assessed on a case-by-case basis, depending on the specific obligations applicable[11].

The NATO and Council of Europe identified the five main perspectives of national cyber security as:

1) **Military Cyber**. Nowadays many governments are building skills to wage cyber war and developing military cyber capability. This military cyber capability can be used as an option for military activities, including "enabling protection of their own defense networks, enabling network centric warfare capabilities, battlefield or tactical cyber warfare and strategic cyber warfare". Military cyber involves both cyber offense and defense capability.
2) **Counter Cyber Crime**. Cybercrime activities include not only attacks that impact individual citizens and corporations, but also those that support military cyber activities and cyber terrorism.
3) **Intelligence and Counter-Intelligence**. Cyber espionage can be perpetrated by a state, a criminal group operating on behalf of a state or a criminal group operating on its own and stealing intellectual property or government secrets. A government requires the capabilities to detect, combat and respond to such activities.
4) **Critical Infrastructure Protection and National Crisis Management**. The majority of critical infrastructures are increasingly connected to cyberspace.

[10] Keman Huang, Stuart Madnick, Simon Johnson, 'Interactions Between Cybersecurity and International Trade: A Systematic Framework', Working Paper CISL# 2018-13, URL: http://web.mit.edu/smadnick/ www/wp/2018-13.pdf.

[11] Gabriele Gagliani Cybersecurity, Technological Neutrality, and International Trade Law Journal of International Economic Law, 2020, 23, 723-745 — P.727

Critical Infrastructure Protection (CIP) requires that infrastructure providers, in both the public and private sector, be a part of the national security framework. National crisis management "must be extended by an additional cyber component".

5) **Internet Governance**. Cyberspace has become an important space for people's daily life. How the state and non-state actors interact to manage cyberspace and maintain its stability is considered a main aspect of national security.

Cybersecurity concerns have already been expressed within the WTO. Trade-related cybersecurity concerns have ranged across all types of cybersecurity concerns. From a cyber-threat perspective, national cyber security threats are defined from four distinct perspectives:

1) **Military Security Threats**. The military's capability to protect from forceful coercion and to fight wars could be impacted by cyberspace operations.
2) **Political Security Threats**. Cyberspace can be used to launch attacks which can impact a government's political authority, governing capacity and the capability of being recognized.
3) **Economic Security Threats**. Economic security includes trade, production and finance. IP theft and other problems associated with economic espionage is one of the main concerns for the U.S.A. Much cybercrime, especially organized cybercrime, has been financially motivated.
4) **Societal, Socio-Cultural or Cultural Security Threats**. Societal, socio-cultural or cultural security involves the sustainability of collective identities and value[12].

Types of Cyber Security Threats

1. Malware

Malware is malicious software such as spyware, ransomware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software. Cisco reports that malware, once activated, can:

- Block access to key network components (ransomware)
- Install additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt individual parts, making the system inoperable[13].

The most common types of malware[14]:

Macro viruses — These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to

[12] Gabriele Gagliani Cybersecurity, Technological Neutrality, and International Trade Law Journal of International Economic Law, 2020, 23, 723-745 — P.728

[13] 7 Types of Cyber Security Threats URL: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

[14] What is a Trojan horse? URL: https://www.malwarebytes.com/trojan

the application. The virus replicates itself and attaches to other code in the computer system.

File infectors — File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.

System or boot-record infectors — A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.

Polymorphic viruses — These viruses conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are initially decrypted by a decryption program. The virus proceeds to infect an area of code. The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine. The encrypted package of mutation engine and virus is attached to new code, and the process repeats. Such viruses are difficult to detect but have a high level of entropy because of the many modifications of their source code. Anti-virus software or free tools like Process Hacker can use this feature to detect them.

Stealth viruses — Stealth viruses take over system functions to conceal themselves. They do this by compromising malware detection software so that the software will report an infected area as being uninfected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.

Trojans — A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers. For example, a Trojan can be programmed to open a high-numbered port so the hacker can use it to listen and then perform an attack.

A Trojan is a delivery strategy that hackers use to deliver any number of threats, from ransomware that immediately demands money, to spyware that conceals itself while it steals valuable information like personal and financial data[15].

Logic bombs — A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.

Worms — Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to

[15] What is a Trojan horse? URL: https://www.malwarebytes.com/trojan

conducting malicious activities, a worm spreading across the internet and overloading email servers can result in denial-of-service attacks against nodes on the network.

Droppers — A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.

Ransomware — Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.

2. Emotet

The Cybersecurity and Infrastructure Security Agency (CISA) describes Emotet as "an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware."

The EMOTET group managed to take email as an attack vector to a next level. Through a fully automated process, EMOTET malware was delivered to the victims' computers via infected e-mail attachments. A variety of different lures were used to trick unsuspecting users into opening these malicious attachments. In the past, EMOTET email campaigns have also been presented as invoices, shipping notices and information about COVID-19.

All these emails contained malicious Word documents, either attached to the email itself or downloadable by clicking on a link within the email itself. Once a user opened one of these documents, they could be prompted to "enable macros" so that the malicious code hidden in the Word file could run and install EMOTET malware on a victim's computer[16].

EMOTET has been one of the most professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years. The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this unauthorised access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware.

Law enforcement and judicial authorities worldwide have disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania,

[16] Top 10 Most Common Types of Cyber Attacks URL: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Malware%20attack

Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats. As part of the criminal investigation conducted by the Dutch National Police into EMOTET, a database containing e-mail addresses, usernames and passwords stolen by EMOTET was discovered[17].

3. Denial of Service

A denial of service (DoS) is a type of cyber-attack that floods a computer or network so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS. Several other techniques may be used, and some cyber attackers use the time that a network is disabled to launch other attacks.

A botnet is a type of DDoS in which millions of systems can be infected with malware and controlled by a hacker, according to Jeff Melnick of Netwrix, an information technology security software company. Botnets, sometimes called zombie systems, target and overwhelm a target's processing capabilities. Botnets are in different geographic locations and hard to trace.

The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

In a Smurf Attack, the attacker sends Internet Control Message Protocol broadcast packets to a number of hosts with a spoofed source Internet Protocol (IP) address that belongs to the target machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses.

A SYN flood occurs when an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect[18].

4. Man in the Middle

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unse-

[17] WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION URL: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[18] Understanding Denial-of-Service Attacks URL: https://us-cert.cisa.gov/ncas/tips/ST04-015

cured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

5. Phishing

Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. "The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine," Cisco reports.

6. SQL Injection

A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website search box.

7. Password Attacks

With the right password, a cyber attacker has access to a wealth of information. Social engineering is a type of password attack that Data Insider defines as "a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices." Other types of password attacks include accessing a password database or outright guessing[19].

Biggest Cyber Threats in 2021[20]

Covid-Themed Phishing Attacks

During a phishing attack, victims are presented with seemingly innocuous emails or websites that are infected with malicious links. Interacting with these links initiates a credential theft process. These attacks have the highest success rates when fear is used as a motivator for interaction. Since the coronavirus pandemic, Covid-themed phishing attacks have spiked, preying upon the virus-related anxieties of the public.

The following chart demonstrates the colossal spike in coronavirus-themed website domain registrations since the pandemic was announced. This is very unusual activity that raises glaring red flags.

Insider Threats

According to a Verizon report from 2019, 57% of all database breaches involved insider threats. Unlike phishing attacks, this type of security-bypassing cyber threat cannot be mitigated with a control strategy.

To best defend against insider threats, access to sensitive resources should be restricted to those that absolutely require it.

Ransomware Attacks

Ransomware attacks are one of the most frightening cyber threats. During these attacks, a victim's sensitive data is encrypted and only decrypted if a ransom price

[19] 7 Types of Cyber Security Threats URL: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

[20] Abi Tyas Tunggal What is a Cyber Threat? URL: https://www.upguard.com/blog/cyber-threat

is paid. Victims only become aware that they've been compromised when they're presented with a formidable message announcing the successful attack.

Ransomware represents the primary threat to health care cyber security, especially during a crisis. Clinics and hospitals caught unprepared by a ransomware attack are more likely to pay the ransom ASAP due to an increased level of urgency and higher demand on critical services — and hackers know this.

Blockchain technology offers immutable and distributed ledgers with auditable records, which

is ideal for tracking every asset in supply chain management. It depends on a distributed, privacy-preserving, secure, and immutable record-keeping framework. Governments and hospitals can identify COVID-19 suspected cases, locations related to reported cases, and infected areas with high risks using blockchain. Blockchain has also been utilized to guarantee healthcare data security. During the COVID-19 pandemic, it is significant to track patients and analyze their symptoms or reactions to the disease. Blockchain is a helpful platform in many countries affected by COVID-19, particularly in healthcare.

Insufficient data for risk assessment for catching or transmitting COVID-19 caused the quick spread of COVID-19 in general. Many patients were asymptomatic and the transmission mechanism for COVID-19 was not well understood until around May 2020.

When cyber-attacks lead to information block, a permissioned blockchain offers two advantages: 1) anybody in the medical consortium can check when and how transactions and information occur; 2) blocking the information will change the hash. Therefore, patients can transmit personal records without any tampering risks. For SARSCoV-2 (causes COVID-19) sequences, a closed hub was created that controls access and prohibits redistribution. Commercial aspirations can delay data sharing because patent incentives hinder open dissemination. Blockchain enables proof of the existence of specific data objects and their content[21].

It must be stressed that health care businesses must remain vigilant in preparing for ransomware attacks by[22]:

Helping the IT department to do its job: The IT department's work will flow more smoothly if all employees check inbound emails for threats; maintain the latest firmware and patches; confirm that security systems and firewalls are operating properly; use secure VPNs when working remotely; and ensure that sensitive information is properly encrypted.

Training: IT professionals should train health care workers on how to spot suspicious emails and phishing attempts. Training must also emphasize that no one should give out login credentials over the phone, by email or in messages. The facility also should have a contingency plan should a security breach occur.

[21] Lidong Wang, Cheryl Ann Alexander Cyber security during the COVID-19 pandemic // AIMS Electronics and Electrical Engineering, 5(2): 146-157

[22] Health Care Cyber Security During Epidemics URL: https://onlinedegrees.und.edu/blog/health-care-cyber-security-during-epidemics/

Backing up data: Health care facilities should keep all sensitive and critical data backed up with multiple recovery points and at different facilities. Whitney suggests the "3-2-1 Rule": Keep three different backups, two on different media and one offsite.

Using the cloud: Because many health care companies are too small to maintain an offsite server farm and backup location, they can instead use secure cloud services for storing sensitive data. Amazon Web Services (AWS) is one example. "Immutable buckets" services, which prohibit data from being deleted or altered, are also available to health care businesses.

As a recent example of a cyber-attack on health care system is the New Hampshire-based Coos County Family Health Services (CCFHS) is back in operation after a ransomware attack that forced it to shut down phone services and EHRs, according to The Berlin Sun. Coos County Family Health CEO Ken Gordon said that the organization discovered the attack on September 20 after noticing abnormalities in the network.

The network of clinics, which serves over 15,000 New Hampshire residents annually, was forced to shut down the entire system, including EHRs, email, and phone services, to prevent further damage. CCFHS offered limited services during the outage, including prescription refills and lab tests.

Another one the Horizon House fell victim to a healthcare ransomware attack that may have exposed the protected health information (PHI) of 27,823 individuals. The Philadelphia-based healthcare center, which provides behavioral health and housing services, discovered that its systems had been encrypted by a ransomware actor on March 5, 2021. Horizon House said it worked quickly to restore access to the information and conduct a thorough investigation into the incident.

On September 3, Horizon House determined that personal information was included in the breach, including Social Security numbers, financial account information, medical claim information, driver's license numbers, names, addresses, medical diagnoses, health insurance information, and medical record numbers[23].

Existing Rules Protecting the Health-Care Sector against Cyber Attacks

Individual criminal responsibility

At the individual level, relevant laws protect hospitals — or the health-care sector more generally — from cyber-attacks by criminalizing the relevant conduct. This is done primarily within domestic criminal law regimes, which often criminalize conduct that endangers public health and safety, irrespective of the means used. But international law may also play a role[24].

[23] Bad Actors Target Small Clinics With Healthcare Ransomware Attacks. Cybercriminals continue to target small healthcare facilities with ransomware attacks, causing EHR downtime and care disruptions. URL: https://healthitsecurity.com/news/bad-actors-target-small-clinics-with-healthcare-ransomware-attacks

[24] Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections? URL: https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/

Under the Budapest Convention on Cybercrime[25] States Parties are obliged to criminalized some cyber activities, such as:

- **illegal access** — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system,
- **data interference** — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- **system interference —** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

As well as State parties are also obliged to cooperate with each other in investigating and prosecuting acts criminalized by the Convention, these are stipulated in articles 23-35.

Conclusion

To sum up, the big question of the intersection between cybersecurity and free trade is two-fold.

First, it concerns how to allow countries to address legitimate cybersecurity concerns without affecting free trade. Given the previously noted pervasiveness of technologies and the existence of cybersecurity threats and concerns in time of peace, striking a balance is extremely difficult.

Second, cybersecurity concerns should not be exploited and abused when no legitimate threat or concern exist to roll back to protectionism. However, it is argued here, this second question is intimately connected to the first one, for the abovementioned pervasiveness of technologies and technology-related concerns make it difficult to precisely assess which concerns are real and which are not. Cybersecurity concerns may rapidly substantiate into actual cybersecurity threats depending on the circumstances[26].

Cyber security is one of the best examples of where the megacommunity approach could help each participant to increase its protection. For example, there

[25] Convention on Cybercrime, Budapest, 23.XI.2001, URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

[26] Gabriele Gagliani Cybersecurity, Technological Neutrality, and International Trade Law Journal of International Economic Law, 2020, 23, 723-745 — P.730

are various areas in the Cyber Security Strategy that require a megacommunity approach[27]:

- **Development of an Industrial Cyber Strategy**: governments and industry from states and abroad need to co-ordinate research and development of new solutions, leveraging national and EU/US funds to develop national and global solutions
- **Cyber Security Skills Strategy**: government and private sector organisations should work closely with academia and research institutions to plug skill gaps and train a new class of managers and officials
- **Providing better advice to business and citizens about the nature of the risks**: information-exchange and co-operation between governments and private sector organisations is essential for having a deep understanding of the new threats
- **Developing international law**: all parties involved should support the development of international law to fight electronic crime and all related phenomena (for example, cyber espionage and cyber terrorism)
- **Tackling the use of cyberspace by criminals and terrorists**: law enforcement should establish new methodologies of international co-operation, information exchange, and mutual support in order to fight electronic crime.

To avoid the many consequences of increasingly common and sophisticated attacks, the focus should be on cybersecurity. The specialists are recommending to have "a well-funded and widely supported security program that matches their specific organizational culture and operational needs and ultimately is aimed at mitigating risk down to an acceptable level". With the volume of threats to organizations steadily growing, mitigating risk to an acceptable level will be a massive undertaking. Compliance and security teams cannot rise to the challenge with manual labor alone; they need the right technology in place — in addition to a tactical strategy — and that means analytics powered by automation and artificial intelligence.

Organizations must still ensure they have a solid framework behind the technology. In order to ensure a strong program, organizations should leverage industry best practices for creating policies and procedures to ensure data security. Ongoing employee education through training materials and email programs is critical to creating a culture of compliance while staying up to date on the latest threats and will help you know where to focus resources in order to proactively reduce risk[28].

[27] Critical Information Infrastructure Protection: The Megacommunity Approach URL: https://rusi.org/publication/critical-information-infrastructure-protection-megacommunity-approach

[28] Nick Culbertson Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity URL: https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyber-attacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=32d513ae5650