Original: **Spanish**

www.cepal.org/transporte

number 6 / 2020 / ISSN: 1564-4227

FAL

BULLETIN 382

FACILITATION OF TRANSPORT AND TRADE IN LATIN AMERICA AND THE CARIBBEAN

Cybersecurity in the time of COVID-19 and the transition to cyberimmunity

Background

Security is a regional public good, as it is in the interest of the whole of society in its different spheres (local, national, regional and international). In the logistics field, a sensible application of measures duly coordinated with facilitation processes not only reduces the levels of risk and vulnerability for logistics chains, →

This *FAL Bulletin* forms part of the Reflections on Disruptive Technologies in Transport that often appear in Economic Commission for Latin America and the Caribbean (ECLAC) publications. On this occasion, it examines the importance of cybersecurity from a logistical standpoint, especially in the current context of a pandemic.

This issue was writtent by Rodrigo Mariano Díaz, ECLAC consultant. For further information on this subject, please contact logisticsand infrastructure@cepal.org

UNITED NATIONS

ECLAC

COVID-19 RESPONSE

but also helps to raise awareness of the problem of security, brings order to the operation of cargo terminals, promotes better operating conditions and increases the efficiency of the authorities' controls. Taking account of all the above elements will have positive effects on the competitiveness and productivity of the economy (Pérez-Salas, 2013).

Both the public and private sectors have developed measures to strengthen the security of logistics chains, such as the Customs Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), the Free and Secure Trade (FAST) program and the Business Alliance for Secure Commerce (BASC) initiative. Quality and security certifications should also be highlighted, such as ISO 28.000, which is a cross-cutting standard that promotes best practices in risk auditing and security event management in the supply chain, as well as the adoption of Safety of Life at Sea (SOLAS) Convention and International Ship and Port Facility Security (ISPS) Code certifications in the area of maritime transport and ports.

ECLAC has also highlighted the need for a "National Logistics Policy" to govern the activity, coordinating and bringing together various international, regional, national and local initiatives, both public and private, to develop comprehensive and efficient solutions. Such a policy should be the result of the participation of private actors and consider at least three interrelated core issues —namely, Trade Facilitation, Logistics and Infrastructure— in order to encourage the opening of new markets for cargo, reduce the infrastructure gap, promote a systematic reduction in logistics costs, and encourage innovation and the incorporation of technology to generate value, in line with the paradigm of integrated policies developed and promoted by ECLAC (Jaimurzina, Pérez-Salas and Sánchez, 2015).

Recently, the attention of the authorities and of the private sector within the logistics sector has also been drawn to the changes brought about by the fourth industrial revolution, composed of technologies such as automation and robotics, blockchain, internet of things, big data and artificial intelligence, among others. The logistics system of the future, therefore, aims at the interconnectivity of information and the optimization of time and resources, along with strong investment and development in the area of innovation to maintain its competitiveness. With increasing technology, cyberattacks are also becoming more sophisticated, as cybercriminals use different tactics and technology to exploit vulnerabilities. As a result, the logistics sector will have to learn to deal with this issue and make it part of their risk matrix, just as it did with other threats in the past, such as drug trafficking and terrorism. Technological progress demands a new look at the business model that currently exists. The space-time paradigm is different from anything known a few years ago and will be much more so soon. The extent of the changes requires a profound cultural change in logistics governance, especially with regard to public-private cooperation, cybersecurity and the incorporation of resilience objectives in all logistics chain processes (Barleta, Pérez-Salas and Sánchez, 2019).

Within the growing framework of digital and virtual representations of physical objects (or in some cases their replacement) that the digital transformation of logistical processes entails, an increase in the possibility of being affected by digital wrongdoing is to be expected. In the current context of digital transformation, accelerated in March 2020 by the COVID-19 pandemic, cybersecurity must be considered inseparably as an integral and updated part of physical and property security. The World Economic Forum's Global Risks Report 2020 confirms this perception, with cybersecurity risks occupying second place behind natural disasters in terms of probability of occurrence and impact. See WEF, 2020.

This document seeks to raise the alert about the importance of cybersecurity in the area of logistics and to promote cybersecurity actions within it, together with a security paradigm shift, transitioning from cybersecurity to cyberimmunity.

I. Cybersecurity paradigm shifts

This section presents the main concepts that make up the technology sphere of security. In the sections that follow, those concepts will allow a more precise interpretation of the statistics on the current state of cybercrime threats worldwide, particularly in Latin America and the Caribbean.

Those concepts will also enable a better interpretation of processed information from cybersecurity activities and facilitate discussion between cybersecurity professionals and people with related backgrounds, thus, raising awareness of cybersecurity.

A. The cybersecurity triad

Security professionals consider three fundamental principles when assessing information protection. They are **confidentiality**, **integrity** and **availability**, the constituent components of what is known as the CIA triad:

- **Confidentiality**: establishes that the information can only be accessed by users and processes with the appropriate clearance level to do so.
- **Integrity**: refers to ensuring that information remains unaltered by unauthorized processes or access, from its origin to its use, and throughout the data's life cycle.
- **Availability**: refers to the objective of ensuring that the information, the systems to process and access it, the distribution networks and the necessary equipment on the part of the end user, are within reach and functioning correctly in a timely manner.

In cybersecurity risk analyses, these three principles are assessed individually to determine the level of exposure to each one. Then, for each, different countermeasures are used to achieve a permissible level of residual risk. The information security triad can be weakened (or defeated) by different types of attacks described below.

B. Description of malware and its main variants

Malware: A contraction of the expression **mal**icious soft**ware**, this term refers to any type of computer language code that, when executed, performs harmful actions on a system intentionally and without the knowledge of the system's user or owner. Before the term was coined in 1990 by Yisrael Radai, this concept was commonly referred to as a *computer virus*. These days, a computer virus, as will be explained later, is a particular type of malware and, in general, its most common motivations are:

- To experiment while learning.
- To be a nuisance and satisfy the creator's ego.
- To damage to a computer system. The damage may be to the hardware (e.g. Stuxnet),[1]

[1] Stuxnet is malware that affects computers running with Microsoft Windows. It was the first one discovered for attacking industrial equipment, reprogramming PLCs and hiding those changes to avoid being detected. Stuxnet was detected in attacks on critical infrastructure such as nuclear power plants.

the software or data, or cause the unavailability of an entire system (e.g. Code Red).[2]

- Degrade the operation of the system.
- Obtain an economic benefit by means of:
  - Theft of confidential information (personal, business, defence, etc.) to be used in subsequent fraud or to be resold to third parties. Such malware is known as **spyware**.
  - A ransom demanded from the system owner, as in the case of **ransomware** (explained in detail below).
  - The appearance of unsolicited advertising, known as **adware**.
  - The system's involuntary participation in hidden networks, for criminal purposes, known as **botnets**.[3]

In technical terms, the structure of the malware may contain more than one component. The key portion is the **payload**, which is the malicious code itself, so it is always present. It may contain three additional portions intended to automatically distribute the infection, hide the true functionality of the malware (e.g., by making the user believe that it is a screen saver) and, finally, conceal the malicious activity (e.g. by deleting activity logs).

Malware can go by specific names, depending on the function for which it was created or the malicious activity it carries out, some of which are:

- **Virus**: the most common type of malware. It is an executable file, which when activated produces the damage for which it was created. Its properties enable it to spread within the computer system where it is hosted.
- **Worm**: capable of executing itself. It can spread through a data network and find vulnerabilities in other systems and install itself on them.
- **Trojan**: It owes its name to the Trojan Horse and, as in that case, is a program that seems harmless and/or useful but has a hidden malicious functionality. That functionality usually allows the affected system to be controlled remotely or enables backdoors[4] which allow unauthorized connections that try to go unnoticed. They usually do not reproduce.
- **Logic bomb**: activated when particular conditions are met; usually after a specific number of iterations or, more commonly, at a specific date and time.
- **Adware**: displays unsolicited advertising. When adware is intended to raise advertising money to finance free applications, it is called **shareware**.
- **Spyware**: its function is to capture private information from the affected computer and send it without the user's consent. This information may be about industrial processes, personal data, credit card information, email addresses (which are then used to send unsolicited email), or pages visited. Sometimes spyware is installed as a trojan, i.e. it is hidden inside another program.
- **Keylogger**: allows all the keys pressed by the user to be saved in a file, no matter in which application. As a result, the file contains sensitive information such as passwords, private chats, confidential content, etc.
- **Rogueware**: emulates a product designed for security protection, such as an antivirus or anti-malware, and urges the user to run it in response to a supposed infection of the computer being used.[5] It is usually activated on a website, and when you want attempt to uninstall it, it demands a payment for its supposed use.

---

[2] CodeRed was a malware discovered in July 2001. On July 19 of that year, it affected 359,000 web servers.

[3] Botnets are networks formed by computers that have fallen victim to software capable of combining the processing and memory resources of a computer systems to work together to process, in a distributed and anonymous way, chains related, usually, to computer crimes such as mass spamming, distribution of child pornography information and attacks on systems that become unresponsive following the receipt of a large number of simultaneous requests.

[4] A backdoor is a programming sequence that enables access to a system without being noticed by the user and avoids access authentication algorithms.

[5] This technique of intimidating the user to install an application that promises protection is known as **scareware**.

- **Decoy**: imitates the access control interface of an application in order to steal user and password information.
- **Dialler**: Almost extinct due to newer modes of internet access via WiFi or ADSL; diallers were very popular when the Internet was accessed using telephone modems. They are intended to dial an unsolicited premium rate number and leave the line open, with the result that the cost is charged to the infected user.
- **Wiper**: a type of malware whose function is to delete information from the computer where it has been installed.
- **Ransomware**: a type of malware whose name comes from the combination of the words **ransom** and soft**ware** and which, when executed, takes the affected system hostage by means of an encryption process and then demands payment of a ransom to restore the operability of that system. Needless to say, paying a ransom for the key to do that does not guarantee its reception, and payment should never be relied upon as a solution to a problem of this nature.

C. Social engineering attacks

Social engineering refers to efforts by governments,[6] media outlets or private groups, to influence certain social attitudes and behaviours on a large scale in order to achieve certain results in the population reached. In the context of cybersecurity, the concept refers to those actions that are designed to manipulate people into doing certain things on a computer system or disclosing confidential information for fraudulent purposes. Social engineering attacks commonly occur through email or phone calls, as well as some other techniques. They are classified as follows:

- **Vishing**: making phone calls to attempt to obtain valuable information covertly through purported surveys or trusted persons or institutions, so that the victim does not suspect that they are being deceived.
- **Baiting**: appealing to people's curiosity and the human principle that everyone wants to help, a device with information (thumb drive, DVD, etc.) infected with malware, is deliberately left in an easy to find place. When the victim uses this found device to verify its origin or content, the malware is installed in one of the different forms described for the various types of malware.

[6] To understand the results of social engineering, we can refer to studies conducted by Professor Robert Cialdini, as mentioned in his book "*Influence: The Psychology of Persuasion*", where he concludes that the influence used in social engineering is based on the six fundamental principles of reciprocity, commitment and consistency, social proof, authority, liking and scarcity.

- **Pretexting**: the creation of a fictitious scenario that encourages the victim to acts unusually or differently than he would under normal circumstances, thus revealing valuable information or leading to actions by the attacker. For example, through this technique, a social engineer could set himself up in a job by pretending to be a replacement for a person or by impersonating a legitimate person.
- **Social networks**: Although social networks came about for the purpose of interaction within circles of trust, careless use or incorrect privacy settings have become the most dangerous avenues of attack. People who do not pay attention to security or privacy settings on social networks can expose sensitive personal data and relationships, which can be used to perpetrate a targeted attack.
- **Phishing**: a very simple type of attack carried out by email that, despite its age, is so effective that it remains one of the most commonly used attack vectors in social engineering. It consists of sending an email that invites impulsive action as a result of the sense of urgency or opportunity that the sender manages to evoke. In the email, you are urged to access a link to a purportedly legal website using a username and password. In this way, the victim inputs their actual access credentials, which are then known to the attacker, who can use them at the genuine website. Generally, the pages that the attacker tries to emulate correspond to electronic payment sites, financial institutions or e-commerce sites due to their great potential for immediate monetization. However, they are not the only cases. Identity or tax information may also be targeted in phishing attacks. The effectiveness of this method is so high that in recent times it has become one of the three main attack vectors for ransomware to infiltrate systems. Anyone who unwittingly executes the installation of the malware, in the belief that they are accessing something in their interest or that they need, becomes a victim once the ransomware encrypts their system.
- **Quid pro quo**: which means "something in exchange for something", is the method used in telephone calls to employees of an institution, where the caller passes themselves of as a member of technical support, informs the user of the existence of an actual problem and then offers to help solve it. Once the user allows this help, the attacker installs the malware on the target system or performs the actual actions that prompted their call.

As tables 1 and 2 show, it is organizations with fewer employees that have a higher rate of receipt of fraudulent emails, as opposed to the existing cultural trend that attacks mainly affect large companies.

Table 1
Annual rate of malicious emails by organization size

Size of organization	Malicious email rate (1 in)
1–250	323
251–500	356
501–1 000	391
1 001–1 500	823
1 501–2 500	440
2 501+	556

Source: Symantec, ISTR - Internet Security Threat Report, vol. 24, Mountain View, February, 2019 [online] https://docs.broadcom.com/doc/istr-24-2019-en.

Table 2
Number of malicious emails by organization size

Size of organization	Affected users (1 in)
1–250	6
251–500	6
501–1 000	4
1 001–1 500	7
1 501–2 500	4
2 501+	11

Source: Symantec, ISTR - Internet Security Threat Report, vol. 24, Mountain View, February, 2019 [online] https://docs.broadcom.com/doc/istr-24-2019-en.

D. Different types of attack

The preceding sections cover the main methods for exploiting weaknesses arising from technology use. Based on these modalities, as well as some more specific ones that are inherent to certain technologies and therefore exceed the scope of this document, the industry led by cybercriminals has developed a range of techniques for different attack methods over the years; indeed, in recent times that development has been spurred by technology itself and the advances it has made. The use of artificial intelligence, for example, has refined the main methods of attack that can be carried out in a targeted, massive or mixed manner.

While there have been many recent victims of mass-distributed ransomware attacks that use phishing techniques, the cybercrime industry has improved its results by using a mixed approach that consists of a first step that involves mass discovery techniques to detect potential vulnerabilities, which are then exploited in a targeted manner using traditional procedures and tools. There has also been a considerable increase in the personalization of content used in social engineering techniques with the aim of exploiting information disclosed in data leaks. In 2019, leaked user information and passwords from breached sites began to be used in the content of extortive emails. In such emails, the attacker claims to possess illicit content from the recipient and to know the username and password sent to the email. Since in many cases people use the same password for multiple sites, the password sent may be familiar to the victim, and therefore he or she may be puzzled by the possible existence of such content. Of course, the attacker only has the username and password and is building a false story based on this weakness of using identical passwords for many sites. The figure revealed by IBM is alarming: 8.5 billion personal data records stolen in 2019, which are then traded or exchanged in cybercrime networks to be instantly monetized or used as information to develop social engineering attacks. This data is offered and traded on the same network and with the same connections as our normal Internet exchanges. The only difference is that they lie beneath different forms of access and are hidden from regular users and common methods of use and discovery. Although they share the medium, they do not have the same end, giving rise to different levels of complexity in accessing their contents.

E. The deep web, dark web and Mariana's web

In discussing the concept of content that is not visible, it is necessary first to refer to Internet content as a whole. The overall Internet is usually represented as an iceberg, with the visible part associated with the portion of content that is visible on the traditional Internet, which is the web as most Internet users know it. For that reason, it is also called the **surface web**. The surface web is made up of content that search engines such as Google, Yahoo, Bing, and others index and offer to users via searches, much as a telephone directory would. Staying with the iceberg analogy, however, much of the content on the Internet is not indexed so that it can be offered to users because it contains technical information that requires the surface web to be used. That segment includes the databases where searches are performed, the emails stored by the providers of this service, etc. All Internet content that is not indexed, and therefore not visible, is called the **deep web**. Hence, the deep web is often called the **invisible web** or the **hidden web**.

Within this hidden portion, which represents approximately 90% of the content and which is not transparently accessible for Internet users, there is a small portion that can only be accessed by specific applications, i.e. a portion of approximately 0.1% of the content, which is intentionally hidden from normal web users. This portion, which was initially only a few pages called **darknets**, is now called the **dark web**. One of those pages is **The Onion Router** or TOR for short and is specifically used to access the content of the dark web. The aim of this project is to create a distributed communications network superimposed on the conventional web and to provide a gateway to the rest of the pages that make up the **dark web** that have been intentionally hidden owing to their

illicit content. Those pages are usually where cybercriminals offer their services and products; records obtained in data leaks, such as credit card information, passport numbers, email addresses with their respective passwords; attack services targeting institutions and companies; and pages used for drug trafficking, human trafficking, and arms sales, among other illegal content.

There is an even deeper and more hidden level in the deep web that, by analogy with the deep-ocean trench by the same name, is called the **Mariana's web**, and access is limited to a very small segment of skilled programmers through the use of complex algorithms. The illegal content that can be found in these cases is so sensitive as to be extremely dangerous.

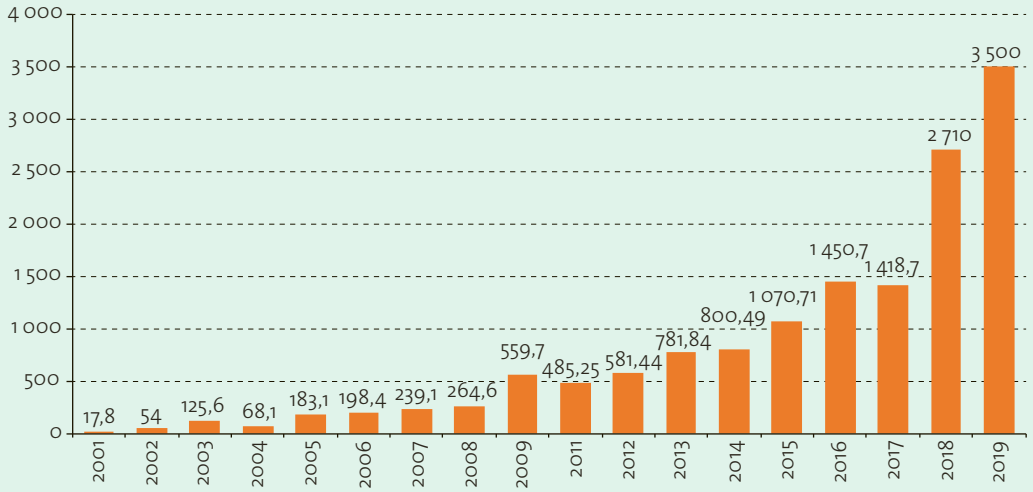
II. Recent incidents and statistical data on cybersecurity in the logistics industry

Knowledge of different incidents that have occurred, the problems, and their frequency or probability of occurrence allow us to determine the probability of its use in later risk assessments related to the security triad, which each process currently faces. From 2011 to 2013, the Port of Antwerp in Belgium fell victim to an attack commissioned by a drug cartel against the terminal's computer systems in order to release containers without the port authorities noticing. When the attack was discovered, electronic security devices were incorporated to protect the port's network perimeter, but these were again breached and actions under the attack continued. In that incident, illicit drugs and contraband worth approximately US$ 365 million were seized, as were firearms.

In June 2017, the shipping company MAERSK sustained a ransomware attack that caused an operational disruption that resulted in losses of US$ 264 million. The investigation into this incident showed that the infection was due to the installation of uncontrolled software on the laptop of a commercial employee in Ukraine. In July 2018, the port of San Diego in the United States was also the target of a ransomware attack that used a piece of software that caused administrative and port permission disruptions. Later that year, COSCO was attacked with operational disruptions at its United States headquarters in Long Beach. In September 2018 the port of Barcelona in Spain was the victim of ransomware attacks that cause administrative disruptions; no information about the financial harm caused by the attacks has been disclosed. In February 2019, GPS jamming attacks were reported on the United States Navy Coast Guard in New York Harbour, and in July off the port of Shanghai. Recently there were reports of a case that affected the shipping company MSC, in which a piece of malware disrupted the disintermediation systems known as MyMSC, affecting access to services by end-users.

As figure 1 shows, the financial losses resulting from cybersecurity attacks are rising as the digitalization of processes advances, as shown in figure 1. It is important to keep in mind that these figures only cover reported events, despite the fact that it is well known that many incidents that occur are not reported but dealt with privately in order to avoid harm to the company's reputation.

Figure 1
World: Annual economic losses due to cybercrime
(Millions of dollars)



Source: Federal Bureau of Investigation (FBI), *2019 Internet Crime Annual Report*, US Department of Justice, 2020 [online] https://pdf.ic3.gov/2019_IC3Report.pdf.

It is often thought that cybersecurity attacks occur less in Latin America and the Caribbean, given the scale of the organizations and because there is less use of new technologies compared to other parts of the world. However, a recent CheckPoint study in July 2020 shows that the region is just as likely to be attacked as others, and even that some countries, such as the Bolivarian Republic of Venezuela, Colombia, Ecuador, Mexico, Nicaragua, Peru and the Plurinational State of Bolivia, have an above-average likelihood. Similarly, the real-time threat map from the firm Kaspersky's Lab shows that the region's countries are in the top 25% of most attacked countries in the world, with Brazil being the third most attacked country worldwide.

These statistics include companies and institutions involved in logistics and transport, a sector that in 2019 showed a year-on-year growth rate of 78% in attacks that on different parts of supply chains, with the result that it ranked third with 10% of total attacks worldwide. This ranking for logistics and transport, which has also remained among the top ranked over the years, highlights the growing value of data from this sector for the cybercrime industry. That ranking, behind financial markets and retail, is explained by the value of electronic assets and the possibility of manipulating data in distribution chains, not to mention the domino effect on other sectors and services, which enhances and multiplies the damage caused by incidents.

The logistics and transportation sector is also highly attractive for access to high-value assets for inter-state espionage, such as biographical information, passport numbers, frequent flyer programs, credit card data, travel itineraries, and shipping manifests, among other elements that are usually handled in the industry.

With regard to the type of techniques used to attack facilities, the three main initial attack vectors are phishing (31% of cases), vulnerability scanning and exploitation (30%), and theft of access credentials (29%). It is striking that most of the attacks that exploit existing vulnerabilities in hardware or software systems are common vulnerabilities and exposures (CVE) that have existed for up to two years;[7] in other words, vulnerabilities that are public knowledge. More than 80% of the attacks carried out in the first half of 2020 could have been prevented by applying update patches that have been available since 2017 or earlier, many of which are free. This shows not only how difficult it is to keep up with security

[7] CVEs are contained in a list of recorded information about known security vulnerabilities, where each entry has a CVE-ID number, a description of the vulnerability, the software versions affected, possible fixes for the fault (if any) or how to configure to mitigate the vulnerability, and references to posts or forum or blog entries where the vulnerability has been made public.

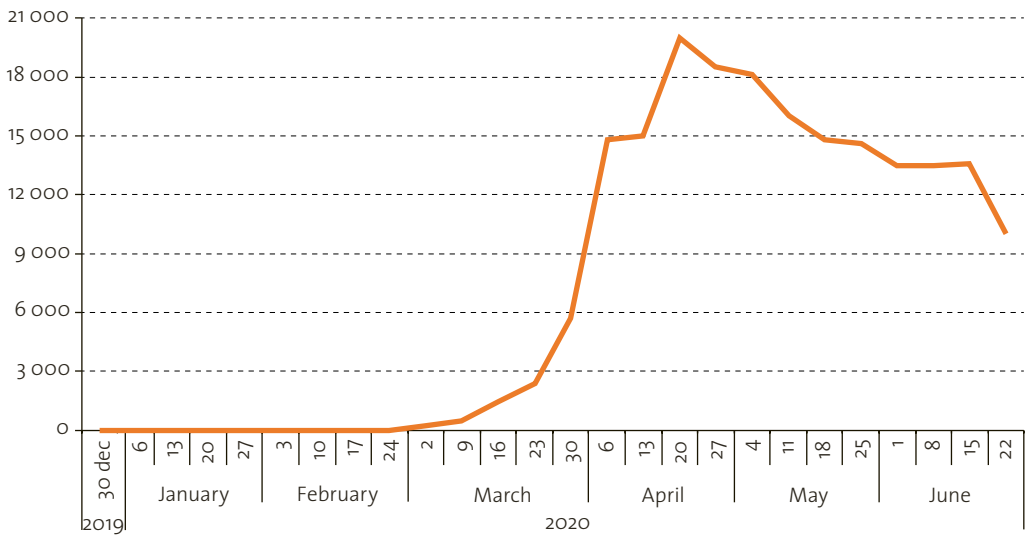
updates provided by software manufacturers, despite the large-scale campaigns they carry out and awareness efforts with technical staff in technology departments on this problem, but also how hard it is, in some cases, to replace obsolete versions of software, due to compatibility of products or applications with basic operating systems in end-user computers and central processing servers.

There is also a tendency to misinterpret that it is more problematic, or that there are not as many tools developed by third parties to exploit hardware vulnerabilities. This makes it very complex to replace certain hardware products, such as PLCs or HMIs, which have been delivered on a turnkey basis to industrial facilities, and whose replacement requires re-engineering and investment. For this reason, in addition to the need to have more and more real-time data resulting from the connection of traditional factory floor or industrial networks, cybercriminals have included in their tool kits the possibility of reaching these types of networks and infrastructure with the aim of causing operational disruptions.

It is important to mention the high incidence of critical infrastructure managed by governments and public and private institutions in the logistics chain and in people's daily lives. These organizations need to take note of cyberattacks that can seriously affect the economy as a result of dependent activities. The X-Force report shows a year-on-year increase in rate of attacks on operational technology (OT) networks of 2,000% between October 2018 and October 2019. In fact, activity in 2019 was higher than for the whole of the previous three years. Most of these attacks are on known vulnerabilities in SCADA systems,[8] as well as brute force attacks with factory passwords on industrial control systems (ICS). This fact is supported by a Symantec study which found that almost 60% of passwords used in attacks on OT networks are trivial and more than 90% of them were carried out with an insecure network protocol and plain text data transmission using a telnet service. For example, the passwords "123456" and "(empty)" were successfully used in 24.6% and 17% of (annual) IoT attacks respectively, with the telnet protocol as the avenue for 90.9% of the attacks.

It was in this existing complex cybersecurity scenario that COVID-19 appeared at the beginning of 2020, becoming a catalyst of digital transformation, as well as accelerating human beings' adaptability to new forms of work. With its arrival, as well as the urgency of information and news distribution, COVID-19-related phishing and ransomware attacks increased exponentially, as figure 2 shows.

Figure 2
World: Cyberattacks since the appearance of COVID-19
(In number of weekly attacks)



Source: CheckPoint, "Cyber attack trends: 2020 mid-year report", Check Point Software Technologies Ltd., Tel Aviv, July 2020 [online] https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

[8] Supervisory control and data acquisition (SCADA) is a concept used in making computer software for remote control and monitoring of industrial processes.

From June 2019 to June 2020, ransomware attacks increased year-on-year by 108%, while attacks on IoT networks went up 833%. This growth reflects the exploitation of exposed vulnerabilities due to the speed with which technology departments had to cover an unexpected demand to make information available by new methods, for more people and in very short time, and in that way, manage to keep operational processes running.

Finally, a fact regarding ransomware attacks that highlights a new concern and opens up a different approach is the case of a major global money management firm for travellers that suffered a ransomware attack in January 2020. It decided to apply its own recovery procedures, refusing to pay the ransom for the hijacked information, and was threatened by the group that created Sodinokibi with the disclosure of 5 Gb of customer information stolen prior to encryption, thus exposing them to a possible breach of the European Union's international personal data protection laws (GDPR).[9]

III. Main cybersecurity challenges for transport and logistics in Latin America and the Caribbean

In relation to how the quantity and form of attacks have evolved, based on its interpretation of the statistics presented, ECLAC identifies the main challenges for the near future in the area of cybersecurity as being in activities related to transport and logistics. Among those involved in the operations of companies and institutions that make up the logistics ecosystem there is a cultural tendency to underestimate cybersecurity problems, despite their increase in recent years. This is deduced from problems having to do with the usual behaviour of individuals. Phishing and weak passwords are the initial causes of two thirds of attacks, the other third being the result of a lack of mindfulness of the need to keep systems up to date. Therefore, the human factor continues to be a deciding one in today's challenges, particularly in human capital outside technology areas. Understanding this issue is key, as developing strategies in relation to this challenge would not only benefit labour activities, but also the security paradigm shift in the whole society as we currently know it, adding its new indispensable dimension of cybersecurity.

There is a noticeable sense, based on the time it takes to react to updates and the lack of internal policies to renew equipment that is being left unsupported by the manufacturer, that security is still seen as a separate (or secondary, if not non-existent) technological innovation process that represents higher internal costs and greater operational efforts when it comes to preventing or correcting technological risks related to one or more of the components of the security triad.

In 2020 there will be four times more devices connected to the Internet than there are people on the planet; 31,000 million devices will be delivering data in real time to be used in the ecosystems of big data and artificial intelligence. Adding this information to that from other technologies, from 2020 to 2025, four times more information will be generated than in the whole of human history. This growth in the area of potential attacks will lead to increased criminal attacks on data and devices in the logistics ecosystem.

Despite that outlook, the opportunity for Latin American and Caribbean states to benefit their logistics services by implementing new technologies participating in logistics 4.0 cannot be affected, much less discouraged, by the challenges of cybersecurity. It should be remembered that the worst technological risk lies not in cybersecurity, but in lack of innovation and failure to exploit opportunities for efficiency improvements in logistics chains through the use of new technologies. The current state of cybersecurity is the result of years of systematic neglect of this problem; however, if cybersecurity is addressed as an integral part of innovation, it not only minimizes exposure to risk, but also accelerates processes of change and maximizes the end-to-end efficiency and reliability of the chain.

[9] The General Data Protection Regulation (GDPR) (Regulation 2016/679) is a set of rules by which the European Parliament, the Council of the European Union and the European Commission seek to strengthen and unify data protection for all individuals within the EU.

Therefore, it is necessary immediately to initiate action plans to minimize technological risks, since otherwise they will become a major enemy of the development of logistics 4.0 and, consequently, of the economy derived from this important activity in the countries that make up the Latin American and Caribbean community.

IV. Action plan to secure the path to logistics 4.0

In a global economy with historical recession figures resulting from the pandemic triggered by COVID-19, the cybercrime industry remains as lucrative as ever and is increasingly active. It is imperative, therefore, to develop a strategic plan aligning measures consistent with the extent of the problem.

As this is an issue that goes beyond the traditional dimensions of physical security and transcends international borders, there is a need to strengthen cooperation between nations and public and private cybercrime investigation agencies in order to establish organizations and policies that can address the problem of cybersecurity in a globally coordinated manner.

In that regard, important efforts have been made to improve logistics security, such as the security recommendations made by the International Maritime Organization (IMO),[10] based mainly on international standard ISO/IEC 27001, which is generally applicable to information and communication technologies.

Lack of regulation of such matters in countries can affect the effectiveness of these measures. It is advisable therefore for governments to analyse the benefits that would accrue to their economies if the activity were governed by compliance rules similar to those in place in the financial sector. Administrative action in that regard would strengthen the confidence of international markets in the sustainability of the activity. Without it, the efforts and recommendations set out below would depend on the appetite and duty of individual members, who would assuredly do so for their own benefit but would continue to depend on the same duty and appetite of their counterparts, for the sustainability of their own process and the benefit of regional economies.

A. Lines of action of the strategic plan

Following the recommendations contained in international standard ISO/IEC 27001, it is advisable for actions overall to target three main lines of action: Processes, Technology and People. To that end, concrete actions have been selected from it that will allow the fundamental steps in these guidelines to be taken.

1. Process-based actions

The initial approach to processes should be framed within a general policy that clearly expresses the commitment to cybersecurity of the highest entity in the organization, clearly stating the general reasons why the institution considers it important to address the problem in a comprehensive manner with due adherence by all members of the institution.

- The general policy is the founding document of an "information security management system", which should **contain** the policy and procedure documents necessary for specific security actions.
- With an eye to disruptive technologies, it is essential to **consider** the appropriate cybersecurity activities from the outset of each digital transformation project, given that each stage has cybersecurity activities inherent in the definitions and deliverables of that stage. The longer it takes to think about cybersecurity, the more complex it becomes to manage risk.
- **Develop** a contingency plan to keep the institution's essential processes active in the event of possible incidents that could undermine the availability of technology. The

[10] See MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management.

plan should be a living, breathing document, constantly under improvement. Regular exercises and improvements not only strengthen confidence in reacting to real incidents, but become real, ongoing training. Likewise, the contingency plan should provide a list of improvements to be made and checked at its next test, thus generating a circular process of continuous improvement.

- **Subject** systems to regular third-party stress tests – Cybersecurity systems should be permanently stressed with ethical hacking or penetration tests to detect uncontrolled changes and newly discovered exposures and correct deviations, before being repeated. The importance of this process lies in the objectivity with which a specialized professional team can spot deviations from standards or vulnerabilities, which may be caused —whether intentionally or unintentionally— by the inadequate operation, integration, maintenance and design of systems.
- **Evaluate** taking out an insurance policy that allows for the transfer of cybersecurity risks.

2. Technology-based actions

- The traditional basic information system security tasks should not be up for discussion and all should be implemented. **Backing up and verifying your recovery utility**, using **firewalls** to establish logical perimeter protections, and using **up-to-date anti-virus** software are still absolutely necessary. Between the backup and the lost data in an incident, there is a time known as the recovery point objective (RPO), which should be assumed as the worst restoration status. Today's dynamic processes cannot resort to this alternative frequently, but it is still the best way to control the worst-case scenario as far as data recovery situations are concerned, such as in the event of a ransomware attack, for example.
- Many of the attacks that take place, occur with appropriate equipment installed that has been incorrectly implemented without expert review. When choosing technology for protection against specific risks, the total cost of the appropriateness of the solution must be **considered**. This includes the purchase cost, the cost and local availability of appropriate technical support for configuration and maintenance, and when the product reaches the end of its life cycle, which determines its maximum amortization. It should be emphasized that correctly implemented intermediate technology is much more effective than the latest technology implemented without oversight.
- Keep software and hardware permanently **up-to-date**, ensuring that they are within the limits of their useful life and have manufacturer support. In 2019, 150,000 vulnerabilities were revealed. Patching vulnerabilities remains a problem for many organizations and cybercriminals know it. And it will be more so if there is no manufacturer support. It is a good strategy to have controls based on competing interests between areas that deal with patching and status control of these updates. This oversight can be done with simple interpretation reports, allowing organizations with pared-back structures to assign it to the internal control or administrative areas, for example.
- **Have in place** advanced event analysis tools with online alerts 7x24x365. Ideally, have an identification and communication process to ensure that a cybersecurity incident is addressed immediately to minimize the impact. Those in charge of cybersecurity in institutions that have been victims of effective attacks underscore the importance of quickly detecting and isolating the attack and the affected systems. This process can be dealt with by using technology contained in software provided as part of a service or be implemented by humans. The latter scenario is known as a security operations centre (SOC), for which there is currently a very marked trend, due to the speed with which an incident is addressed when this process is implemented.
- Intrinsically safe technologies. Most business technologies emerged and evolved without consideration to the hyperconnected world. Cobol systems, SAPs, plant floor systems, etc., were designed for controlled network environments and low interoperability with unknown networks. A lot of effort is being put into adding to them the necessary security layer so that they can be used in today's environments. In new

innovation developments, serious **consideration** should be given to using intrinsically safe technologies, such as blockchain.

- **Consider** using two-factor authentication methods that prevent unauthorized access as a result of weak passwords.
- **Apply** a layered defence model in operational technology networks to prevent an attack on the administrative or management network from spreading and halting productive processes.

3. **People-focused actions**

- Human capital in general. **Train** all staff on a constant basis. Such training should be done with adequate induction training when person joins the work team and be reinforced approximately every 2 years. At a minimum this should include policies on data privacy, data backup, use of passwords and responsible Internet use. This training should also be reinforced monthly with short training courses that create permanent awareness about passwords, phishing, etc. It is also highly advisable to engage in ethical and controlled phishing, in order to measure how effective the awareness is.
- **Have** a copy of a non-disclosure agreement signed by each collaborator that clearly explains the objectives of the agreement and the penalties for non-compliance.
- Technology personnel should **have recurring spaces** assigned to cybersecurity developments to raise awareness.

V. The road from cybersecurity to cyberimmunity

For many years, the concept of fear, uncertainty, and doubt (FUD) has been discussed in the cybersecurity arena, which has helped to implement information security technologies. The detail that must be grasped in relation to the success of this concept is that, in a world where information technology created isolated systems or systems connected with other systems via specific points, defence systems such as antivirus software, firewalls, etc. were the solution to the main problems of electronic security and theft of confidential information. In recent years, with the advent of technologies that form the work environment known as Industry 4.0, in a hyperconnected world where systems have come to form ecosystems, to continue using the FUD principle would be a mistake that could deepen the crisis. This is because such an approach could increase the technological inequality between those who implement these changes and those who do not, leaving out of the fourth industrial revolution those institutions that out of fear do not implement technological solutions as a driver of operational efficiency. The biggest risk in a hyper-digitized and hyperconnected world is failure to take technological risks.

Recognizing that risk can never be zero and knowing that in a hyperconnected world security breaches can occur in fractions of a second,[11] at a great distances, and without the need to carry tools or weapons, sustaining an attack that violates our security is only a matter of time. Therefore, it is advisable to begin developing strategic plans so that, in the same way as the organisms of living fend off attacks, computer ecosystems are equipped with a cyberimmunity system.[12] As with living organisms, such a system takes into account that the immune systems of organizations are never perfect and can be damaged by viruses or other malignant objects that can attack functions in the organization or even the immune system itself. However, systems adapt and learn, and in that cycle of continuous learning they become more effective, incorporating new and better defences to stop new and unknown attacks. They may even be able to stop them without knowing precisely the objective of the attack or the means for carrying it out. Thinking about cyberimmunity makes it possible, in the event of being defeated by a threat, quickly to

[11] The definition of risk is the direct function of the potential harm of a threat or hazard and the probability of its occurrence.
[12] The concept was first developed by Professor Peter Wlodarczak of the University of Southern Queensland in his technical note entitled "Cyber Immunity - A Bio-Inspired Cyber Defense System" (Wlodarczak, 2017).

restore the institution's essential operational functions, thus allowing the loss triangle in the resilience curve to be reduced and normal functions to be recovered and exceeding the results prior to the incident.

VI. Conclusions

In an increasingly digital and connected world, with disruptive technologies and demanding implementation times, exposure to a cyberattack is only a matter of time. The effort must then be made to lower the chances of occurrence by means of a cybersecurity management plan that includes effective measures in relation to processes, technology and people, regardless of the size of the organization, while at the same time preparing as well as possible to deal with an incident.

It is advisable to understand the process of cybersecurity as an immune system similar to that of a biological being, comprising a number of elements with very different functions that prevent an infection or disease. Just as in living organisms, an organization's immune system is never perfect and viruses and other pathogenic microbes will find ways to deceive or even attack it. However, immune systems have one very important feature in common: they learn and adapt. They can be "educated" through vaccination against potential threats. In times of danger, they can be assisted with prepared antibodies. Through some techniques such as immediate attention to atypical events detected through permanent monitoring of technological activity, organizations can defend themselves from cyberattacks, even without having a very clear understanding of what is happening.

With this new approach called cyberimmunity, the logistics community in Latin America and the Caribbean can protect themselves individually, maintaining operational continuity and data protection in the logistics 4.0 environment. However, given the functional interdependence of the logistics chain, the unavailability of one of its components affects the entire ecosystem. Therefore, the development of regulatory bodies and mechanisms to formalize and strengthen trust among the components of the end-to-end system and improve the competitiveness and confidence of global markets cannot be neglected or delayed.

VII. Bibliography

AJOT (American Journal of Transportation) (2019), "U.S. Coast Guard warns of cyber-attack & electronic interference threats to commercial vessels", *Maritime News*, Ajot, August [online] https://www.ajot.com/insights/full/ai-u.s-coast-guard-warns-of-cyber-attack-electronic-interference-threats-to-commercial-vessels.

Baker, J. (2020), "MSC confirms website shutdown caused by cyber attack", *Maritime Intelligence*, Lloyd's List, April [online] https://lloydslist.maritimeintelligence.informa.com/LL1131957/MSC-confirms-website-shutdown-caused-by-cyber-attack.

Barleta, E. P., G. Pérez and R. Sánchez (2019), "Industry 4.0 and the emergence of Logistics 4.0", *FAL Bulletin*, No. 375, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

Bateman, T. (2013), "Police warning after drug traffickers' cyber-attack", *BBC News*, October [online] https://www.bbc.com/news/world-europe-24539417.

BBC News (2018), "San Diego port hit by ransomware attack", October [online] https://www.bbc.com/news/technology-45677511.

CheckPoint (2020), "Cyber attack trends: 2020 mid-year report", Check Point Software Technologies Ltd., Tel Aviv, July [online] https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

Cialdini, R. B. (2006), *Influence: The Psychology of Persuasion*, Harper Collins.

FBI (Federal Bureau of Investigation) (2020), *2019 Internet Crime Annual Report*, US Department of Justice[online] https://pdf.ic3.gov/2019_IC3Report.pdf.

IBM Security (2020), *IBM X-Force Threat Intelligence Index*, february [online] https://www.ibm.com/security/data-breach/threat-intelligence.
IMO (International Maritime Organization) (2017), "Guidelines on Maritime Cyber Risk Management" (MSC-FAL.1/Circ.3), July.
ISO (International Organization for Standardization) (2018), "ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary", Geneva [online] https://www.iso.org/standard/73906.html.
Jaimurzina, A., G. Pérez-Salas and R. Sánchez (2015), "Políticas de logística y movilidad para el desarrollo sostenible y la integración regional", *Natural Resources and Infrastructure series*, No. 174 (LC/L. 4107), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).
Kaspersky (2020), "Cyberthreat Real-Time Map" [online] https://cybermap.kaspersky.com/es/.
La Vanguardia (2018), "El Puerto de Barcelona sufre un ciberataque que podría retrasar la entrega de mercancías", Barcelona [online] https://www.lavanguardia.com/local/barcelona/20180920/451930581288/puerto-barcelona-sufre-ciberataque-y-podria-causar-retraso-entrega-mercancias.html.
Mathews, L. (2017), "NotPetya ransomware attack cost shipping giant maersk over $200 Million", *Forbes*, August [online] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#6a6794f64f9a.
Moiseev, A. (2019), "Di sí a la ciberinmunidad y no al miedo", Kaspersky Lab [online] https://www.kaspersky.es/blog/start-immunizing/19022/.
Pérez-Salas, G. (2013), "The need to facilitate and secure logistics processes in Latin America and the Caribbean", *FAL Bulletin*, No. 321k/oç, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).
SAFETY4SEA (2018), "Cyber attack hits Cosco's operations in US, July" [online] https://safety4sea.com/cyber-attack-hits-coscos-operations-in-us
Schwab, K. (2020), "The Fourth Industrial Revolution: what it means, how to respond", World Economic Forum.
Symantec (2019), *ISTR - Internet Security Threat Report*, vol. 24, Mountain View, February [online] https://docs.broadcom.com/doc/istr-24-2019-en.
WEF (World Economic Forum) (2020), *The Global Risk Report 2020*, 15 January.
Weikert, B. (2019), "The resilience of infrastructure services in Latin America and the Caribbean: A first approach", *FAL Bulletin*, No. 374, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).
Wlodarczak, P. (2017), "Cyber Immunity - A Bio-Inspired Cyber Defense System", *Lecture Notes in Computer Science*.

VIII. Publications of interest

FAL Bulletin No. 381

Digital Transformation in Latin American and Caribbean logistics

Gabriel Pérez
Luis Valdés Figueroa

This *FAL Bulletin* continues the Reflections on Disruptive Technologies in Transport that ECLAC has been publishing through this medium. The present edition analyses the importance of the digital transformation of logistics, especially in the current circumstances where the need for fluid, safe and resilient logistics calls for additional actions on traceability and process facilitation.

Available in: Spanish English

FAL Bulletin No. 375

Industry 4.0 and the emergence of Logistics 4.0

Eliana Barleta
Gabriel Pérez
Ricardo Sánchez

The fourth industrial revolution is bringing about a series of disruptive changes in both business models and the production chains that support them. Logistics, which is a fundamental element of these processes, is inevitably affected by these significant changes. This fourth industrial revolution is characterized by its speed, magnitude and depth. The changes are so dramatic that they will alter the way we live, work and relate to one other, affecting countries, companies, industries and society as a whole. Therefore, the logistics system of the future must aim for interconnected information and optimized time and resources, with significant investment in innovation and development to maintain competitiveness.

Available in: Spanish English