Advances in Wireless Communications and Networks
2019; 5(1): 33-40
http://www.sciencepublishinggroup.com/j/awcn
doi: 10.11648/j.awcn.20190501.15
ISSN: 2575-5951 (Print); ISSN: 2575-596X (Online)

Bases, Challenges, and Main Dangers for Deploying Cybersecurity in Industry 4.0

Pedro Ramos Brandao

Interdisciplinary Centre for History, Cultures and Societies, Evora University, Evora, Portugal

Email address:
pb@pbrandao.net

To cite this article:
Pedro Ramos Brandao. Bases, Challenges, and Main Dangers for Deploying Cybersecurity in Industry 4.0. *Advances in Wireless Communications and Networks.* Vol. 5, No. 1, 2019, pp. 33-40. doi: 10.11648/j.awcn.20190501.15

Received: July 27, 2019; **Accepted**: September 6, 2019; **Published**: September 20, 2019

Abstract: Cybercrime is making waves bigger and bigger in the global economy. Attack companies are adding up, as advances in the scanning of production and work processes make their data easier to prey. Hackers are forming their sights, especially in companies with business models dependent on the availability of digital infrastructures and content. Since the digitization of production and products is constantly deepening the integration, both inside and outside companies, the task of connecting any gaps to protect data availability, integrity and confidentiality increasingly devours the management of time and money. All manufacturing companies are potentially exposed to the risk of cyberattacks, as the root cause of each threat is a new form of addiction. All industrial production chains depend increasingly complex and interconnected, often digital goods, as well as the constant exchange of data, information and knowledge. There is no doubt the benefits of this smart network give companies up and down the value chain. The downside is that it leaves them more vulnerable to digital attacks as the number of points of contact with the outside world increases. In this paper we introduce the context of the problem at hand, ie the cybersecurity challenges for Industry 4.0. Next, we present aspects resulting from a bibliographic study on the subject, which highlights an example of an algorithm that provides security and information stored in Cloud Computing. I develop a topic on current Cybersecurity assessment scenarios, emphasizing an example of a deeper approach. The biggest security risks for Industry 4.0 are presented, where the most commonly used methods for cyber-attacks in Industry 4.0 are spelled out. A set of defense methods are exemplified. It summarizes a set of strategic principles for building a security system. Finally, the main layers are cybersecurity to Industry 4.0.

Keywords: Cybersecurity, Industry 4.0, Networks Security, Networks Dangerous

1. Introduction

Industries, particularly those that are of critical manufacturing, are recognized as potential targets for cyber-attacks. The aggressor's motivations cover a wide range, including intellectual property robbery as well as of trade secrets, sabotage of processes and exit, extortion and malicious damage to networks and information systems. Recent cyber-attacks patterns confirm that while financial services, public administration and public services are the most targeted economic sectors, manufacturing is a significant target. Within manufacturing, the automotive, chemical, computer and electronics industries are the most searched. Cybersecurity firms such as Kaspersky, McAfee, Trend Micro and Symantec do track the origins and types of threats, their goals and targets, and how they change over time. In general, the number of so-called zero-day vulnerabilities, in other words a vulnerability in software that is unknown to the vendor, have decreased by approximately 20 percent from 2014 to 2016. New vulnerabilities were discovered in 2016 in 16 different SCADA applications from 15 different vendors. As these vulnerabilities are closed, intruders change strategies for using email-attached malware and hidden in legitimate administrative tools to gain access to targeted systems. Specifically, for the manufacturing industry, 1 in 130 e-mails contains malware, which is roughly equal to the average in all areas, but the number of phishing emails sent to manufacturers was 1 in 3,171, significantly above average. Another type of directed attack at manufacturers seeks to alter automated production processes with the intention of destroying production equipment or compromising it enough to make production unusable. At

times referred to as cybersabotage, this type of cyberattack is exemplified by the Stuxnet computer worm that targeted ICS at Iran's nuclear facilities in 2010. Since then, Stuxnet variants have been found in the industry, notably Duqu a Trojan found in Europe, that was designed to collect information on ICS, another variant was discovered in 2010, it exploited a Microsoft Windows vulnerability to attack SCADA systems. No security company or product can take the necessary steps to strengthen cybersecurity in manufacturing. Mechanisms for intra and inter-industrial collaboration will be required. Threats are constantly changing. Effective action in industry in general is not responding quickly as it should, in relation to cybersecurity dangers. "As computers and automation led the charge through the last few decades, companies, organizations and governments focused their efforts on revitalizing the IT infrastructure in the period also referred to as Industry 3.0. Today, however, the focus has shifted to technologies like Internet of Things (IoT), Artificial Intelligence (AI), blockchain, robotics, etc. which are defining the new work culture across almost all industries. Industry 4.0 primarily merges automation with advanced manufacturing to reduce direct human effort and resources. Effectively, these technologies make the manufacturing system a "smart networked factory", where all activities are digitally controlled and are thus, immutable. As a result, utilization of resources, both financial and material, is more efficient. Industry 4.0 (I 4.0) can be the catalyst of changes in different fields like governance, management and administration of smart cities and other applications which are driving the vision of Digital India. Examples of such centers of innovation include the IIT Delhi and Mumbai Centers for Smart Manufacturing and another center at the Central Manufacturing Technology Institute, Bengaluru. Capacity building for I4.0 is carried out by the SL Kirloskar Centre of Excellence for IoT. With so much dependence on data flow and communication between processes, components and sub-systems, data integrity and systems integrity assume critical dimensions. Manual supervision of various processes is neither feasible nor effective. Even patching security flaws from time to time is not practical – data by itself needs to be both abstracted and secured through different tools and techniques. Following secure design principles and guidelines such as in ISO 21827 is critical to secured system design. Securing Industry 4.0 requires a de-novo approach which is explained in next section." [1]

2. State of Art

Collaborative Cloud development products are an inevitable trend in industry 4.0. to optimize the resources architecture, the products' development companies have been increasing significantly their products design for collaborative environments in Cloud Computing. Consequently, the protection of industrial products, particularly those with sensitive information, has been a huge challenge and information is shared in Cloud Computing. Encryption has been one of the most commonly used tools.

"*Data encryption is an important approach for information protection in a network environment. Effective approaches can prevent the sensitive information to be obtained by unauthorized users. In the early time, any files representing in binary formats are regarded as encrypted. Later, content based encrypted approaches based on the encryption of the basic content elements appeared. Based on that approaches, the encrypted file could be open. However, the content cannot be distinguished correctly by unauthorized users (such as the image encryption). As thus, content-based encryption can be used to protect the information of CAD model when it is being shared in cloud computing*" [1].

The requirements for physical cybersecurity in different advanced digital manufacturing processes substantively in innumerable ways of traditional security in traditional IT systems. IT cybersecurity in layers under defence pressure in central servers' cores and with less attention on peripherals is a problem. In digital manufactures, particularly we must protect both layers, servers and peripherals, as well as all remote systems involved in the manufacturing network. Increased threats indicate that industrial control systems are a real target for malicious cybernetic intrusions. Nowadays, manufacturing data must be kept confidential, and their integrality must be ensured. On the other hand, the great challenge to maintain availability has significantly increased. Distributed manufacturing processes require extensive security-based monitoring and control as a function in itself. The specific manufacturing processes security is a challenge to maintain the integrity of information in multipolar development environments.

Current manufacturing architectures do not meet the requirements for today's challenges. The current design of separation between production environments with regard to equipment is out of order in relation to the desirable integration of all processes with industrial equipment. As a result, there are shortcomings, for example, in relation to subcontractors, equipment suppliers and mainly in the supply chain of servers without the precaution of controlling their architectures.

"*A more holistic approach to managing cyberphysical security threats in manufacturing is communicating such data directly with the relevant manufacturing device. The fundamental problem is one of authentication and authorization: is the request to the manufacturing device authentic and is the actor requesting it authorization. We need to supply a couple of concepts. The first concept is asymmetric encryption keys. A manufacturing security enforcement device located close to or the manufacturing device would cryptographically ensure the integrity of the transmitted data. From a security standpoint, it is just as important to know the origin of a part as it is to control how a part is produced*" [2].

In the last decades, structured big-time analyses have had a major impact on health care and medical care. Norway's healthcare system was among the first to adopt digital clinical data, and quickly moved into a situation of huge

digital health records database. Nowadays healthcare industry uses systematically and in great volume the digitization of health data. This entails huge security issues. It's absolutely required to implement, in this case, strong security platforms, hence the stored data in these digital database structures are extremely sensitive. Data encryption is absolutely imperative here.

"*Once data is transferred from applications to cloud computing data centers it needs to be store efficiently. Norway's, a number of data provisions has increased, such as high throughput instruments, telescopes, sensors networks and streaming machines and these environments produce huge amount of data. Hadoop Distributed File System is used in this phase to store such huge amount of data. This phase also categorizes data into different level and store them into different datacentres*" [3].

To protect information in these databases is fundamental to use strong security algorithms. This is one of the most used algorithms in these circumstances as well as to provide security to Meta Cloud Data storage:

/*Process the Audit Log File to check the logged in user's details like his/her/AI Machine track status, last Logged in time etc.*/

Select customerid, password, last_loggedin_time, current status, geolocation, browser type, ipconfig, sysdate from update_audit_log;

//If any malicious user tried to login application

{

Insert into Threat_updated values (customerid, password, geolocation, browsertype, geolocation, sysdate);

Return -1;

}

Else {

List 1 = Select DataStorageproviderName, DataScope from MetaDataStorageCloud where Customer_loggedin_ApplicationID = ?;

If (1.DataStorageprovidername =="amzoncloud" &&1.datascope =="critical")

{

Goto -> Amazon Cloud data Storage

Select * from AmazonCloudStorage where Customer_loggedin_ApplicationId =?;

}

Elseif(1.DataStorageproviderName =="googlecloud" &&1.datascope =="sensitive")

{

Goto -> Google Cloud Data Storage

Select * from GooglaCloudStorage where Customer_loggedin_ApplicationId =?;

}

Elseif (1.DataStorageproviderName =="xcloud" &&1.datascope =="normal")

{

Goto -> x Cloud data storage

Select * from XcloudCloudStorage where Customer_loggedin_ApplicationId =?;

}

}//end else [3]

By significantly applying and evaluating Cybersecurity's controls impact on Direct Digital Manufacturing (DDM) it is a permanent and troubling challenge to the entire DDM community. This issue has grown exponentially in relation to DDM technologies, since these have moved to Internet platforms. The power of DDMs to quickly provide prototypes by networks and redesign them on demand exposes sensitive information to potential risks. It is necessary to get security mechanisms to DDM platforms.

"*DDM systems store data, process data with network connectivity and suffer similar cyber risks to corporate networks, laptops and mobile devices. These traditional cyber risks combined with DDM market growth presents attackers with new and potentially valuable targets. New attack opportunities include disrupting processes and facilitating theft, counterfeiting, and enabling sabotage. Cyberthreats to manufacturing enterprises may be motivated by espionage, financial gain or other* [4]".

Supervisory Control and Data Acquisition (SCADA) is an extensively used system in automation industries or process control, and enables remote monitoring of devices. They are widely used in Water and Treatment Stations, oil and natural pipelines, gas distribution stations, electrical stations, defence systems and therefore it is used in highly critical structures. These systems were designed to be robust, but not to be safe. Therefore, there is an urgent need to provide these security systems at all levels.

"*The Stuxnet and BlackEnergy attacks are good examples of a APT malware affecting cyber physical devices. The Stuxnet malware sabotaged the Iran Nuclear Program activities at the Natanzuranium enrichment plant. Most analysts speculate that the initial compromise occurred via an infected removable drive*" [5].

Industry 4.0 requires the maintenance of strict access to confidential data as well as to digital services and physical processes that are linked to complex cyberphysical systems that must not fail. Agile and fast security measures, capable of adapting to rapid attacks changes, nowadays need to be systematically implemented so that industry 4.0 is more efficient.

"*Advanced manufacturing systems are not secure like traditional systems. Cybersecurity has become a critical challenge in IoT enable CPS, which could be threatened by a wide variety of cyber-attacks ranging from criminals and terrorists to hacktivists. As a consequence, Cybersecurity is critical for the success of Smart Manufacturing*" [6].

Traditionally cybersecurity has security architectures which incorporate mechanisms that provide confidentiality, privacy, authenticity, integrity, access control, and non-repudiation. These services are extensively used to prevent intrusions and attacks on computers and networks. Nonetheless, the security landscape of the modern Internet is characterized by large, constant and very fast attacks, persistently and highly sophisticated attacks. These characteristics impose very significant challenges in

preventive security services. Consequently, methodologies that provide automatic detection and response to cyberattacks shall be synergistically employed with prevention techniques in order to achieve defence-in-depth and robust cybersecurity systems.

"*Cyberattack detection systems require algorithms that collect and analyze data generated by various events occurring within a cyber environment. The objective of a detection algorithm is to accurately discover suspicious activities based on the analysis of event data. This objective is fundamentally important as it forms the core of any attack detection system*" [7].

3. Cybersecurity Assessment

Cybercrime has increasingly a major and negative impact on the global economy, this is a reality for all economic sectors and in particular for industry. Attacks on companies are systematically increasing. The digitalization process that has occurred and which still occurs, immeasurably facilitates the improper capture of companies' data and files. Cybercriminals use companies whose core business depends on digitizing information to train their hacking capabilities.

Nonetheless, there must be a general awareness, and especially in industry in which risks are general and real.

As production and product digitization is constantly deepening systems integration, the task of bridging gaps to protect availability, integrity, and data confidentiality is taking organizations more and more time and money.

Cybersecurity approach shall be based on the following strategic key pillars:

3.1. Deeper Approach

Cybersecurity means having to make sustainable, rapid, and accurate changes in the business structure to improve security. Foremost, it is required that decision-makers and managers be made aware of the intervention's urgency, from which the necessary technical updates will necessarily follow. Deploying hardware and software is only a means to an end.

3.2. Persistence

Cybersecurity means finding and establishing long-term solutions - and adjusting them regularly. Security-related changes can not be carried out at once, everything that has to do with security is a dynamic process always in transformation, security itself must be seen as a process in itself. The best approach consists of three fundamental principles and five active factors.

3.3. The Dangers of Cyberspace

The warnings of increasing threats are daily. A highly regarded publication by American experts Peter Singer and Allan Friedman postulates the following assumption: "97% of the Fortune 500 companies were hacked and... probably the other 3% too, they just do not know that." However, more recent studies point to even more worrying scenarios.

All manufacturing companies are potentially exposed to cyberattacks risk hence the root cause of any threat is a new form of addiction. Industry-wide value chains increasingly depend on complex and often interconnected digital assets, as well as on the constant exchange of data, information and knowledge. Companies store and share research findings in digital format and use computer-aided processes to develop products and manage their production networks and services online. However, the associated data and communication streams can only be controlled to a certain extent. Their safety depends on the degree of awareness that industrial administrators have of the problem, and awareness is probably not yet very large.

4. Industry 4.0: The Major Risks

Industry 4.0 includes the use on an industrial scale of digital technologies focused on the production processes, the emergence of cybernetic systems forces the connection between all of them. These network clusters accelerate production, promote a high level of self-organization, and thus facilitate a more efficient and flexible deployment of production resources. The benefits that this smart network offers to businesses are unquestionable. The downside is that this makes companies more vulnerable to digital attacks as the number of points of contact with the outside world increases.

The threat to businesses is also a threat to their products, which are increasingly more intelligent, connected and exposed to various hazards, including industrial espionage. The spectrum of hazards ranges from intelligent sensors that control air conditioning systems to automatic access control systems as well as vehicle position control units, and even systems, etc. Nowadays most customers expect manufacturers to take responsibility for their products security and to do everything in their power to protect functionality and personal data.

The scenarios studied so far allow us to conclude that: the threat is greater for industrial companies with high quality products and technological systems, but the risk also extends to other companies with supposedly fewer sensitive goods and services. That's because they also use large amounts of the most critical raw material in the digital age: data.

Only a fraction of all attacks appears in the media and catch public's attention - fortunately for the affected companies as this gives them time to fill in security loopholes and keep them connected.

Cyberattacks are, by nature, highly dynamic and sophisticated events that usually trap unsuspecting companies.

In the fight against cybercrime, responsible companies must create specific mechanisms for this and adopt new approaches.

It is crucial that companies conduct regular critical reviews of their own security solutions and continuously improve and develop these solutions as well as equating the development

of better ones. Regardless of how mature your cybersecurity solutions are, companies must be alert and ready to take action.

Clearly, cybersecurity is a complex and multidimensional topic for all organizations. The list of possible enemies is long: assaults can be launched by industrial spies, secret service agents, criminals, political activists and even internal officials. Spying methods are also becoming increasingly sophisticated. Any and all of the company's confidential and important assets, that is, data, information and intellectual property in the broadest sense, are considered potential targets for attacks. The digitalization of value chains, customer contact points, and supplier interfaces means that enterprise protection measures must extend far beyond their own facilities. Increasingly, digital products and services expose innovations and business insight to vulnerable environments. Product safety - protecting the value that products represent for the company, but also protecting customers from counterattacka while using these products - is another aspect of cybersecurity that requires particular attention.

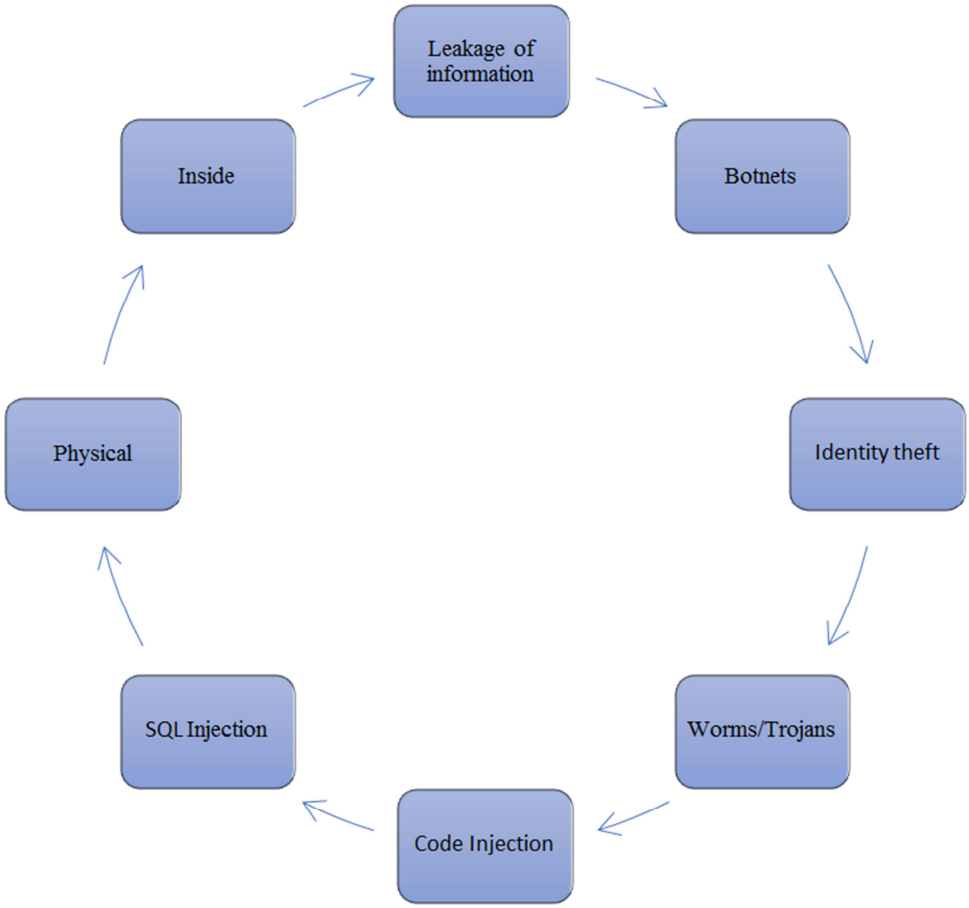

Figure 1. *Main Cyberattack Methods.*

5. Basic Principles for Defining Cybersafety

As digitalisation increasingly penetrates into products, businesses and value chains, the need to protect digital assets has increased dramatically in all areas. Companies' digital connectivity covers all their areas, from purchases and logistics to production, sales and services. This has far-reaching implications for the organization's security architecture. In many companies, IT - or a special department of IT security - is still responsible for cybersecurity. However, focusing on conventional IT systems is not enough to handle the needs of a corporate environment which is increasingly connected to multiple networks. Vulnerabilities can often be found in development units, production, and products service, and all of them, as a rule, are beyond the reach of traditional IT security. Adopting a transversal approach across all areas of the business is the only way to ensure that products and the entire enterprise receive the best possible protection.

For each company, the battle against cybercrime is a long-term task. This means (constantly) evolving into existing approaches and solutions. It is not about developing new revolutionary approaches to the company from the beginning. What differentiates the pioneers in corporate cybersecurity is that they use the existing fields of responsibility, structures, processes and systems as a starting point, developing and improving them by introducing new end-to-end solutions.

Evolutionary development requires surveillance and

agility. When threat scenarios change, companies need to adapt their security systems to meet changing needs. In a complex and high-risk environment, no one can stand still. Companies need to prepare for new threats and make existing processes safer. In doing so, however, they should not lose sight of or even contradict their business model. Achieving greater security should always remain a means to an end.

Cybersecurity affects the entire enterprise. It is not enough that only management and safety units to address the issue. All employees across the company should play a role in implementing a new security architecture. The security level of any company is also determined by the level of vigilance between internal structures. Specific training programs and campaigns that corporately connect employees to existing resources can have an immediate and long-lasting effect, hence in many cases more conscious actions during daily routines prevent vulnerabilities from occurring in the first place.

6. Building a Cybersecurity Strategy

Cybersecurity seeks to protect Integrity, Confidentiality and Availability (ICA) of information and forms the basis of a strategy to protect data against all forms and means of violation. An effective cybersecurity strategy shall consider the following solutions.

Due to the growing reliance on the digital infrastructure, companies face a challenge in finding a balance between protection and progress, as well as privacy and governance. Compliance and governance risk challenges can arise from inadequate protection of digital assets, lack of optimization of compliance management tools, and lack of an adequate compliance framework [8]. Cybersecurity risk management involves identifying external and internal vulnerabilities in an organization's cyberspace and finding solutions to protect it. Risk management requires a detailed risk assessment, which involves identifying technological gaps. An organization may have sophisticated cybersecurity tools; however, these tools may not necessarily address specific vulnerabilities. For instance, an organization may discover, through its external evaluation, threats, namely that their employees are vulnerable to phishing scams. In such a situation, the organization shall make more efforts in training its employees to refrain from opening attachments from unknown senders. Therefore, the organization's detailed assessment of specific risks ensures that cybersecurity tools implemented by an organization are appropriate to the specific risks it faces. In addition to proactive measures, companies need to have a crisis management strategy to respond to any significant data breach or theft of critical data. Risk management plays an important role in the overall growth, stability and sustainability of an organization [9].

Unified threat management (UTM), as the name suggests, refers to a single security solution that provides multiple security functions at a single point in the network. A UTM appliance offers a comprehensive security suite - antivirus, antispyware, antispam, network firewall, intrusion detection and prevention, content filtering as well as leak prevention. UTM devices have gained strength because of increased combined threats - attacks that use combinations of different types of malware and launch simultaneous attacks on separate parts of a network. Avoiding such attacks can be difficult if an organization uses separate devices and vendors for each security task. By creating a single point of defence, UTM improves the ability to handle various threats [10].

Security incident management (SIM) involves dealing with security incidents (threats) in real time. Security incidents include policy violations, unauthorized access to data (health and financial data and social security numbers), and server crashes. The SIM helps an organization to minimize the impact of a cyberattack and get back to business as quickly as possible. It is a multifaceted strategy, combining handsets, software and research oriented to the human being. It usually begins with an alert about an incident followed by involvement of the incident response team comprised of representatives from various departments including legal, communications, finance, operations and IT. Incident analysts analyse an incident and develop a plan to remove any threats or problems. The major benefit of SIM is that it allows an organization to respond to threats systematically following a consistent methodology of incident handling, thus minimizing the impact of service interruption [11].

Cloud technologies, mobility and the Internet of Things (IoT) allow companies to bypass firewall protection and to work anywhere. Even clients may interact with organizations through multiple channels. This has increased the challenges related to identity and access management (IAM). IAM places the user's identity at the centre of the cybersecurity model. It is a crucial enterprise for any company, as IAM products provide role-based access control tools that help organizations to regulate user access to critical information. Its primary purpose is to provide all users a digital identity, whether a customer or an employee. Committed user credentials are a major cause of security breaches. IAM mitigates this threat by providing single sign-on (access to multiple applications using a set of credentials), multifactor authentication (combining two or more stand-alone credentials), access management, and many other solutions. Implementing IAM with its best practices may provide an organization with significant competitive advantages. For instance, opening a network without compromising security to employees, customers, partners and vendors may improve efficiency and reduce operational costs [12].

7. Layers of Cybersecurity to the Industry 4.0

Hackers are always improving their means of discovering failures in computer networks. In 2017, we have witnessed a massive ransomware attack - WannaCry, which was the most sophisticated attack of its kind. Under such circumstances,

the best way to protect cyberspace is to create and deploy a multi-tiered security strategy.

Network Firewall: a firewall protects an organization from network-based attacks by hackers, viruses, and worms. It is the first defence line, similar to walls built around medieval castles to restrict unauthorized entry. Firewalls monitor incoming and outgoing network traffic using default rules. A firewall is an essential component of a cybersecurity strategy and should be updated regularly to prevent emerging threats. It protects a network against a wide range of attacks, such as DDoS, browser and brute-force attacks [13].

Physical Security: we protect our valuables by locking them in vaults, for instance. Equal importance should be given to physical security and monitoring of server rooms, desktops and external hard drives. This can be done by installing surveillance systems, blocking server rooms using fingerprint and face recognition technologies, maintaining control of mobile devices and using password-enabled screen savers [14].

Identification and Elimination of Loopholes: organizations shall seek help from experts and also identify vulnerabilities in their system. Common vulnerabilities include weak passwords, outdated firewalls, missing software patches, unencrypted data, outdated antivirus, unrestricted use of USB flash drives, and unprotected Wi-Fi networks. Once identified, the vulnerability must be addressed to mitigate any threats. Vulnerabilities can be corrected through regular system scans, vulnerability and threat scans, software patch application, as well as firewall and antivirus / malware software updates [15].

Data Encryption: data encryption translates the digital data into indecipherable code, so that only authorized persons with access to a decryption key (password) can access it. If a hacker can circumvent all network-based defences, data encryption systems take action as the ultimate layer of security. Interestingly, a system encryption strength is directly proportional to the size and complexity of the key. Protection against brute-force attacks (in which a hacker tries random keys until he finds the right one) requires a long and complex key [16].

Security Training: an individual is the most important element, but also the weakest link in the implementation of a cybersecurity strategy. It is entirely possible that a cybersecurity program, even when created near perfection, can fail if the person in question does not know how to operate it or take appropriate defensive measures during an attack. For instance, many malware attacks were successful because someone was browsing through unsolicited links or clicking an affected email attachment. It is extremely important that all organizations carry out basic training for all their employees so that they are aware of what constitutes a data breach and how to deal with it [17].

Business Continuity and Disaster Recovery: Business Continuity and Disaster Recovery (BCDR) is a broad term that combines a set of processes and techniques to help an organization to recover from a disaster. This is often neglected during the development of a cybersecurity strategy. The result of data loss from natural disasters or cyberattacks can be serious for a business. About 25% of organizations facing cyberattacks lose significant business opportunities after a data loss event. BCDR involves identifying potential threats (such as cyberattacks, natural disasters, IT system failures and fires) and preparing a continuity and recovery plan. Backups are an essential part of BCDR - a well-managed backup is highly effective against ransomware attacks [18].

8. Conclusions

Depending on the company size, the complexity of the threat situation and the level of risk, it makes sense to create a dedicated cybersecurity management system with your own full-time employees. Any alternative has advantages and disadvantages. The ability to focus attention on a topic and full-time dedication of people involved in security are two of the key arguments for a dedicated cybersecurity management system to work well. The less positive side of this approach is that it increases costs. Companies which want to substantially improve their cybersecurity quality need to make an exhaustive and critical analysis of their structures, processes and internal security culture. A check-list is a good way to begin to identify where change is needed and to what extent. Finally, commitment to data encryption is not an option, it is a mandatory requirement for sensitive data protection in today's enterprise networks and cloud computing platforms.

References

[1] R. Rishi, “Ey-cybersecurity-for-industry-4-0,” 06 Setember 2019. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-for-industry-4-0/$File/ey-cybersecurity-for-industry-4-0.pdf. [Acedido em 06 Setember 2019].

[2] S. Wang, “Customized Encryption of CAD Models for Cloud-Enable Collaborative Product Development,” em Cybersecurity for Industry 4.0, Cham, Springer, 2017, pp. 35-57.

[3] A. Wegner, “A New Approach to Cybersphysical Security in Industry 4.0,” em Cybersecurity for Industry 4.0, Cham, Spinger, 2017, pp. 59-72.

[4] G. Manogaran, “Big Data Security Intelligence for Healthcare Industry 4.0,” em Cybersecurity for Industry 4.0, Cham, Spinger, 2017, pp. 103-126.

[5] D. Glavach, “Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems,” em Cybersecurity for Industry 4.0, Cham, Spinger, 2017, pp. 173-194.

[6] Volkovlaw, “Volkov,” [Online]. Available: https://blog.volkovlaw.com/2018/01/convergence-cybersecurity-compliance-enterprise-risk-management.

[7] C. Ventures, “Cybersecurity Ventures,” [Online]. Available: https://cybersecurityventures.com/cybersecurity-500.

[8] Cbronline, "Cbronline," [Online]. Available: https://www.cbronline.com/enterprise-it/5-unified-threat-management-products-to-simplify-your-cyber-security-4902562.

[9] UGA, "UGA," [Online]. Available: https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/incident_management.

[10] P. Identity, "Ping Identity," [Online]. Available: https://www.pingidentity.com/en/company/blog/2017/08/14/what_is_identity_and_.

[11] Empo Werit, "Empo Werit," [Online]. Available: https://www.empowerit.com.au/blog/holistic-cybersecurity-7-layers-you-need-to-consider.

[12] Small Business, "Small Business," [Online]. Available: https://smallbusiness.chron.com/different-kinds-biometric-security-available-securing-server-room-69885.html.

[13] Focustsi, "Focustsi," [Online]. Available: https://info.focustsi.com/it-services-boston/the-8-layers-of-cybersecurity-needed-to-protect-your-business.

[14] D. Guardian, "Digital Guardian," [Online]. Available: https://digitalguardian.com/blog/what-data-encryption.

[15] empowerit, "empowerit," [Online]. Available: https://www.empowerit.com.au/blog/holistic-cybersecurity-7-layers-you-need-to-consider.

[16] Unitedlayer, "unitedlayer," [Online]. Available: https://www.unitedlayer.com/sites/default/files/ul-disasterrecoveryguide.pdf.

[17] R. Nair, "The Resource Usage Viewpoint of Industrial Control System Security: An Inference-Based Intrusion Detection," em Cybersecurity for Industry 4.0, Cham, Spinger, 2017, pp. 195-223.

[18] S. Tedeschi, "Practical Security Aspects of the Internet of Things," em Cybersecurity for Industry 4.0, Cham, Springer, 2017, pp. 225-242.

[19] L. Thames, "Cybersecurity for Industry 4.0 and Advenced Manufactoring Environments with Ensemble Intelligence," em Cybersecurity for Industry 4.0, Cham, Springer, 2017, pp. 243-265.