International Journal of Scientific Research and Management (IJSRM)
||Volume||10||Issue||03||Pages||EC-2022-747-754||2022||
Website: www.ijsrm.in ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v10i3.ec01

Cybersecurity risk management in the industry 4.0

Pedro Ramos Brandao (PhD) [1], Paulo Duarte Branco (PhD) [2]

1 Instituto Superior de Tecnologias Avançadas (ISTEC), Lisbon, Portugal
2 Instituto Superior de Tecnologias Avançadas (ISTEC), Lisbon, Portugal

Abstract
a referential and abstract model will be presented to be applied in risk management on cloud computing and industry ICS platforms in general. we are looking at the types of assessments that are out there, we explore the different approaches and techniques behind information technology systems risk assessments and complexity of conducting industrial control system safely at-risk control level.

Keywords - Cybersecurity; Industry Security; Security Framework; Industry Risk Management.

I. Introduction

The global cybersecurity market is defined by market sizing estimates that range from $ 71 billion in 2014 to $ 155 billion in 2019. Worldwide information security spending should have reached $ 71.1 billion in 2014, with the data loss prevention segment experiencing the fastest growth, at 18.9%, according to a forecast by Gartner, Inc. Total information security spending is expected to grow by more than 8.2%, in 2015, to reach US $ 76.9 billion. The 2015-2025 Cyber Security Matket report: Visiongain's leading network, data, endpoint, applications and cloud security, identity identity management and security operations indicate that the cybersecurity market was worth $ 75.4 billion in 2015 (a small percentage difference compared to Gartner's estimate for 2015), as the high demand for information security and infrastructure solutions continues, mainly for Industry 4.0 [1].

The cybersecurity market is estimated to grow to $ 155.74 billion by the end of 2020, according to a report by Markets and Markets. North America is expected to be the largest market, while the Asia-Pacific (APAC) and Europe, Middle East and Africa (EMEA) regions are also expected to experience significant market growth. Next-generation cybersecurity spending can range from $ 15 billion to $ 20 billion over the next 3 years [2].

These data show and prove a trend towards the problem of dangers in relation to cyber-attacks and in relation to security processes in the industry.

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 attack types prove that while banks and financial, public services, and the public are the most targeted economic sectors, manufacturing is a significant target. Within manufacturing, the automotive, chemical, computer, and electronics industries are the most searched.

At times referred to as cyber sabotage, 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 companies take the necessary care cybersecurity in manufacturing with proper instrumentation. 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.

Taking these scenarios into account, it is important to consider the issue of risk analysis in Industry 4.0, as an essential part of cybersecurity processes. Also considering that part of the Industry today is in one way or another, connected to the Internet or connected to Cloud Computing systems. In this study will get into the details of risk assessments.

II. State Of Art

H. Khalid (2020), We can say that we are facing a new industrial revolution, (4.0), with new challenges. One of the biggest challenges is cybersecurity. Currently, industrial systems are full of sensors, networks, Internet access, integrated communications, IoT, and all of these systems are easy to attack at the level of cybersecurity [3].

H. Khalid (2020), “Cybersecurity issues are one of the most important challenges to address in the Industrial System 4.0” [3]

The main pillars that we have to guarantee in terms of security for Industry 4.0 are Confidentiality, Integrity, and Availability [3] these are a standard for the whole society but very particularly for the industry because of a failure in one of these pillars can put concerned all industrial system.

A. Silva (2019), affirms that the industrial control systems denounced SCADA, are for all the industry, being fundamental to the functioning of the same, however, they are extraordinarily easy to suffer an attack or sabotage. Their main characteristic is that they are not isolated, therefore susceptible to being manipulated maliciously. Most cyber-attacks are done through this system [4].

“Overall, implementing strong cybersecurity controls requires business involvement through proper governance, levels of security technology, management, education skills and vigilance that go far beyond the demands of regulatory compliance, complementing states om ISAC paper Governance os cybersecurity” [4].

S. Samtani (2019), states that hacker attacks in the industry usually start by exploiting vulnerabilities in information systems, these flaws that these cybercriminals find in the industry are equivalent to more than a trillion dollars a year in terms of losses, so it is lawful to say that we are facing a major problem. Companies' attitude towards cybersecurity must change [5].
"Systematically reviewing dozens of CTI platforms revealed the CTI industry remains one that is rapidly emerging and growing and not one which has reached saturation" [5]. "Systematically reviewing dozens of CTI platforms revealed the CTI industry remains one that is rapidly emerging and growing and not one which has reached saturation" [5].

A. Creery (2015), comments that the systems of the type PLCs, DCs and RTUs, that control devices at the level of the current industry, are normally controlled and monitored by human interfaces called HMI. Most HMIs use commercial operating systems. This fact favors the possibility of finding natural flaws in the systems, adding to this fact that in the industry there is no improved care to update these systems. If normal computer systems are frequently attacked successfully, these systems implemented in the industry are still more easily attacked [6].

"The worm migrate through a VPN connection to a company's corporate network until it finally reached the critical supervisory control and data acquisition (SCADA) network. It infected a server on the control-center LAN that was running MS-SQL. The worm traffic blocked SCADA traffic "[6].

J. Vykopal (2020), states that today's industry uses Industrial Control Systems (ICS) systematically, which are fundamental to the production process, from electricity, water systems, transport, and health. However, these systems are deeply exposed and are connected to other systems, including in many cases the Internet. These connections reduce costs in the operation of the systems, however, they become a dangerous vulnerability, increasing the risk of attacks and consequently losses at this level [7].

“ICSs are made to maintain the integrity and availability of production processes and to sustain conditions of industrial environments. Their hardware and software components are often custom-built and tightly integrated. However, IT systems use off-the-shelf hardware and software and have different operational characteristics and security objectives [7].

S. Karnouskos (2015) expresses the opinion that security processes are fundamental to avoid serious cybersecurity problems in Industry 4.0, and mainly to mitigate and control security risks. If a safety accident occurs it is necessary to identify the risks that led to the dangerous exposure. The use of security agents for risk control and management is a tried and tested method with good results. Log analysis, monitoring all systems, detecting anomalies can help prevent a cybersecurity disaster. Traditional systems of firewalls, honeypots, classic scanning systems are important but not sufficient, risk management is a fundamental component [8].

“Effective security can be achieved at high degree when security considerations and good practices can be integrated in the lifecycle of the industrial Agent solution [8].”

S. Klongnaivai (2020) states that the increase in the Internet of Things at an industrial level and its connection to industrial devices increases enormous cybersecurity risks. Bearing in mind the need for good risk management systems applied to Industry 4.0 [9].

“The amount number of business fail to handle the attack” [9].

M. Nunes (2021) affirms affirmatively that the massive use of the new industrial systems of the ICPS type brought with them new technological bases of computing, which in themselves are beneficial for the industry but that due to the integration with other systems impact on the level of cybersecurity, leading to possible serious cybersecurity problems if there is no excellent cybersecurity risk management and risk prevention system [10].

“We argued about the datasets, testbeds, machine learning techniques, security policies that will shape the future of ICPS security [10].”

D. Bhamare (2019) Industrial Control Systems (ICSs) are widespread across the industry, and today instead of being equipment for production control, they are a source of cybersecurity concerns. These systems can make the industry a serious problem. In the case of critical infrastructures, such as nuclear power plants, electricity and water stations, transport systems, etc. the concern is heightened. These systems (ICS) are currently connected to other systems and are no longer isolated as they were two decades ago, connections to other systems enhance intrusions and the implementation of malware, in addition to the hypothetical control of the infrastructures themselves. The security systems have to cover ICS, the SCADA systems, and the DCS. In other words, cybersecurity, in the industry, the so-called logic controllers must be highly concerned. In this process, good risk management is essential [11].

“Existing defenses such as firewalls and VPNs have repeatedly proven inadequate on their own, especially with the increasing usage of cloud platforms for ICS. On the other hand, various research works have argued and demonstrated that data encryption alone is not sufficient for network security. Recently there has been a trend in the applications of machine learning techniques in developing the intrusion detection systems (IDS) for ICS [11].

P. Mahesh (2020) states that industrial distributed systems that are physically connected require innovative care in relation to cyber-attacks, being necessary to develop new approaches and methodologies even within the limits of technological possibilities since industrial control systems are deeply vulnerable, from simple malware cybercrime to high-level sabotage. It is necessary to have a robust risk management and analysis system and to have solutions that permanently analyze the security of the systems [12].

“The motivation of the attacker, resources available, and the damage caused in each category can be different and should be a part of the threat analysis [12].”

V. Mullet (2016) it is very important to incorporate a set of cybersecurity mechanisms in industry 4.0 to keep industrial systems safe, namely production control systems. Since cybersecurity must be divided into several areas, this author proposes that it be done in industrial facilities and that various levels of physical security are created, according to the risk, obviously for this there must be a roaring management and analysis system of risks. security levels in an industrial installation can and should be a mix of physical and virtual or logical security levels [13].

“Any cybersecurity solution needs support from multiple actors to be included in the comprehensive strategy of an Industry 4.0 factory, and all users need to be trained and made ware of cybersecurity risks. [13]”

G. Culot (2019) demonstrates that proceeding with the complete security of an industrial company, today, is practically impossible, since there are highly interconnected distributed systems that in themselves create an enormous possible attack surface. Even with the use of machine learning and cryptography it is extremely difficult to ensure control of the systems concerning cybersecurity. That is why there must be a well-defined business strategy for cybersecurity encompassing risk mitigation management [14].

“Its impossible to protect companies from all possible cyberattacks. The real question is about risk prioritization and mitigation. Managers can be supported by revised risk management tools [14]”

III. Industrial Control System (Ics) – Risk Assessment

Most attacks to access ICS can be divided into two phases:

a) Phase 1: attempt to access the ICS network at all costs to get to phase 2. In phase 1, there are attempts to gain access to the company's internal system, trying to find weaknesses for access. It should be included in this phase, especially nowadays, the use of company employees, which facilitates all the intrusion work of this phase 1.

b) Phase 2: this is the exploration phase of the ICS, this phase included activities to explore the ICS enterprise network and checking the implementation model as well as the existing vulnerabilities. The purpose, as a rule, like acts of sabotage that impact the company's production process or acts of industrial espionage.

It is for this reason that there is a well-structured defense plan in relation to Phase 1, discard existence and implement safety instrumentation. in relation to phase 2. It is in this context that it is essential to have a risk assessment. This is the first step towards a correct cybersecurity plan. We'll show you an example in this work. 3 – Risk assessment.

Definition of Risk Assessment: discovery, state of play of the risk situation involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk.
In other words, risk assessment in terms of industrial security refers to the processes of find something wrong in a particular situation that jeopardizes security, such as the bad configuration of a network-system. If we discover the vulnerabilities of a system in time, the possibility of something is not correct and impact the production process, we can be to determine the predictable damage and resolve the problem in advance.
Full description of possible risks:

- A threat source is the beginning of an attack, with the designation of threat actor;
- A threat event is the act of exploiting a vulnerability or attack on the system under consideration (SUC);
- A threat vector is the avenue of attack or the delivery technique to execute infected thumb drive or using a phishing email to deliver a malicious payload.
- A vulnerability is a flaw in the SUC, such as misconfigured service, easily guessed password, or a buffer overflow programming error in an application.
- Likelihood is the chance for the found vulnerability to become a threat event;
- A target is the system under consideration.
- A consequence is the direct result of successful threat event, such stop the service or the installation of a malicious program.
- The impact is the result of in the prestige of the company [15].

Thus, the risk analysis can measure the vulnerabilities and the that impact the production of company and on the production process or on the company's services. The the completion of this type and work is the score for a discovered vulnerability. The score takes into consideration the issues in following equation [16]:

$$risk = \frac{Severity + (criticality * 2) + (likelihood * 2) + (impact * 2)}{4}$$

In the equation presented, the constituent elements of the equation mean the following:

- Severity: is a number ranging from 0-10, given to the vulnerability by a service like the N. V. Database (USA) executing an algorithm like the Common Vulnerability Scoring System (CVSS) [12] provides a system to analyze the characteristics and impacts of IT vulnerabilities [17].

- Severity: is a number ranging from 0-10, given to the vulnerability by a service like the N. V. Database (USA) executing an algorithm like the Common Vulnerability Scoring System (CVSS) [12] provides a system to analyze the

characteristics and impacts of IT vulnerabilities [17].

Criticality: is a number between 1 and 5 that reflects the importance of the SUC to the overall process [17].

Likelihood: is a number between 1 and 5 reflecting the alteration of the vulnerability becoming a successful threat event or, the chance that the vulnerability will be successfully exploited.

Impact: is a number between 1 and 5 that reflects the financial with influence on budget, damage to the image of the company, the potential impact on the environment, and the possible risk to all and public health safety in case of a compromise or failure of this system [17].

First Step of Risk Assessment – Identification and System Characterization

On a regular IT network, discovery of assets is often accomplished with scanning instrumentation, pings and ARPs. We advise the use of NMAP [18]. We can use the following command:

```
# nmap -sp 173.10.8.0/16
Starting Nmap 7.8 (https://nmap.org) at 2020-11-24 16:15 GMT
Daylight Time
Nmap scan report for 173.10.8.1/16
Host is up (0,034s latency).
MAC Address: 80:2b:89:F4:89:C8 (Liteon Technology)
Nmap Scan Report for 173.10.8.2/16
Host is up (0,56s latency)
MAC Address: 79:2b:25:F4:67:C8 (LG)
Nmap Scan Report for 173.10.8.3/16
Host is up (0,0067s latency)
MAC Address: 93:3C:27:F8:68:C9 (Microsoft)
Nmap done: 256 Ip addresses (3 hosts up) scanned in 12,56 seconds
```

We can filter out just the IP address by piping the nmap result through awk:

```
# nmap -sp -T 2 173.10.8.0/16 -oG - | awk ‘/Up$/{print $2}’
173.10.8.1
173.10.8.2
173.10.8.3
```

We basically want to find out that concludes the best way to analyze the effective risk of the asset or system getting compromise or failing.

Second Step of Risk Assessment – Vulnerability Identification

This step used threat modeling to accomplish this. Threat modeling is the process of obtaining relevant information that can be operationalized, means of threat events and risk scenarios. It is the process of obtaining information from credible sources with its motivations, capabilities, and activities. Threat information is general details like: as US-CERT [14], CVe [19], and NIST feeds [20].

The activities in this step ca be divided into the following:

1. Discover vulnerabilities in the system under consideration;
2. Gather information on the discover vulnerabilities;
3. Conceptualize threats events;
4. Create risks scenarios.

The Model of risk management (MRM) has three evolutionary stages:

Stage 1

Foundational elements
Objectives: Build elements for model risk management (MRM)
Key elements: MRM policy; Model inventory; Manual work-flow tool; Model governance and standars; MR; organization

Stage 2

Implementation and execution
Objectives: Implement robust MRM
Key elements: MRM policy; Control and process; Training for stakeholders; Automated

work-flow tool.

Stage 3

Capturing value
Objectives: Gain efficiencies and extract value from MRM
Key elements: Center os excellence for model development; Indistrialized validation; Transparency in model quality; process-efficiency tracking; Optimized resource management.

IV. Discovering Vulnerabilities

There are two main methods in accomplishing this task: by comparison and by scanning. The method that takes all running software, firmware, and OS versions and compares them to online vulnerability databases, searching for known vulnerabilities.
Some online good resources to find vulnerabilities include the following:

1. NIST – NVD [17];
2. MITRE – CVE [18];
3. ICS – CERT [19];
4. SECURITY FOCUS [20]
5. EXPLOIT-DB [21]

The second method involves running a vulnerability scan with a tool such as Nessus [21] or OpenVAS [22], with a lots of traffic to the ICS network and, depending on the type OS scan, can have negative effects on the ICS devices.

Example of Nessus scanner package be a Terminal on the kali Linux:

```
root@GMD101010:~/Download# dpkg -I Nessus-6.10.8-debian6_amd64.deb
Selecting previously unselected package nessus.
(reading database … 445678 files and directories currently installed.)
Preparing to unpack Nessus-6.10.8-debian6_amd64.deb …
Unpacking nessus (6.10.8) …
Setting up nessus (6.10.8) …
Unpacking Nessus Core Components …
Nessusd (Nessus) 6.10.8 [build M20096] for Linux
Copyright © 1998 – 2020 Tenable Network Security, Inc

Processing the Nessus plugins …
[##################################################]
All plugins load (1sec)
- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to https://KVM0101010:8834/ to configure your scanner

Processing triggers for system (232-25)
```

This will install the Nessus scanner and indicates additional necessary procedures. The scanner is done installing, run the following command, indicate the end of the installation and star Nessus:

```
root@KVM101010:~/Downloads# service nessusd strat
```

Risk Calculation and Mitigation

We must quantify the risk to every risk scenario. Having correlated the assessment process between assets and having analysis in all points, the scoring will be relative number showing where best to with mitigation work for all anomalous events that impact on investment and where our efforts will have the most impact.

For the scoring, we will use the earlier defined formula:

$$risk = \frac{Severity + (criticality * 2) + (likelihood * 2) + (impact * 2)}{4}$$

This gives us following risk score calculation, for example:

Vulnerability severity (0-10)	Asset criticality (0-5)	Attack likelihood (0-5)	Impact (0-5)	RISK Score (0-10)
From CVE	From Step 1	(CVE combined with system specifics)	From Step 1	
7,5	4	4	3,5	7,6

Graph 1: The resulting score allows easy correlation between all discovered vulnerabilities.

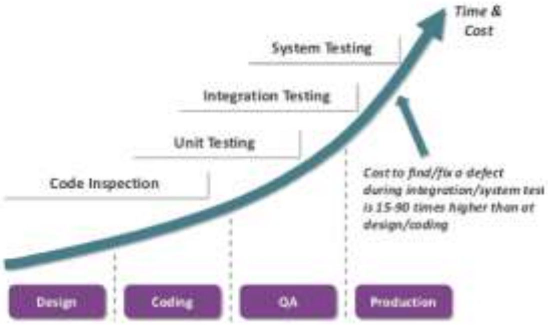
Time & Cost
System Testing
Integration Testing
Unit Testing
Code Inspection
Cost to find/fix a defect during integration/system test is 15-90 times higher than at design/coding
Design
Coding
QA
Production

Figure 1: Correlation between the discovered vulnerabilities

Obtaining the data:
These data were obtained through a laboratory test, consisting of two domain controllers with a DNS server and client computers, one of which was exposed to the Internet and could serve as a gateway.

V. Framework With Best Practices

For the purpose of risk control, we propose a framework based on CIS 20 (Critical Security Controls) [23] that outlines best practices for internet security and cyber threats applied to the industry. These 20 critical security controls are broken down into three buckets – basic, foundational and organizational. The CIS 20 is acclaimed by many to be one of the best cybersecurity frameworks. These best practices empower organizations to push past compliance and holistically secure their organization. One of the biggest benefits of CIS20 is that it helps users easily prioritize. The controls in the basic bucket are the most critical and have high payoff. These controls are your starting point to enabling risk reduction. This is represented in Graph 2.

Functions	Categories	Information
IDENTIFY		
PROTECT		
DETECT		
RESPOND		
RECOVER		

Graph 2: Framework

VI. Conclusions And Correlation In Referring I4.0 And Cybersecurity

We make the relationship of importance of cybersecurity and Industry 4.0 through an important quote by lane Schaefer:

“*A new revolution know as Industry 4.0 is occurring where countless elements comprising industrial system are being interfaced with internet communication technologies to form the smart factories and manufacturing organizations of the future. Industry 4.0 and its associated technologies are currently being driven by disruptive innovation that promises to bring countless new value creation opportunities across all major market sectors. However, existing Internet technologies are plagued by cybersecurity and data privacy issues that will present major challenges and roadblocks for adopter of Industry 4.0 technologies. Industry 4.0 will face traditional cybersecurity issues along with its very own unique security and privacy challenges*.” [24]

VII. Conclusion

With industries expanding and the exponential increase in cyber-attacks, especially industrial automation components, it is essential to have a set of risk analysis processes very well integrated and permanently able to be put into practice, the dangers of cybersecurity in the industry are currently extreme.

One of the areas of this cybersecurity strategy must be risk analysis. As we have seen, it allows us to have a clear picture of what is at stake if there is an attack and we also be able to detect attack points and vulnerabilities in the systems.

Risk analysis is one of the most important instruments in this whole scenario related to cybersecurity on the stage of industries.

Acknowledgment

Thanks to Instituto Superior de Tecnologias Avançadas (ISTEC) Lisboa

References

[1] https://www.alliedmarketresearch.com/press-release/cyber-security-market.html.

[2] http://cybersecurityventures.com/cybersecurity-market-report.

[3] H. Khalid, "Cybersecurity in Industry 4.0 context: background, issues, and future directions", Cybersecurity in Industry 4.0 context, 2020

[4] A. Silva, "Cybersecurity Readiness: an empirical study of effective cybersecurity practices for industrial control systems", Scientific Journal of Research and Reviews, 2019.

[5] S. Samtani, "Cybersecurity as an industry: a cyber threat intelligence perspective", Springer, 2019

[6] A. Creery, "Industrial Cybersecurity for power system and SCADA networks", IEEE, 2020.

[7] J. Vykopal, "KYPO4INDUSTRY: a testbed for teaching cybersecurity of industrial control systems", SIGCSE, 2020.

[8] S. Karnouskos, "Industrial Agents Cybersecurity", SAP, 2017.

[9] S. Klongnaivai, "Cybersecurity and privacy readiness in Thailand smart Industry", IEEE, 2020.

[10] M. Nunes, "Cybersecurity of Industrial Cyber-Physical Systems: a Review", IEEE, 2021.

[11] D. Bhamare, "Cybersecurity for industrial control systems: a survey", Computers and Security, Elseveir, 2019.

[12] P. Mahesh, "A survey of cybersecurity of digital manufacturing", IEEE, 2020.

[13] V. Mullet, "A review of cybersecurity guidelines for manufacturing factories in Industry 4.0", IEEE Access, 2016.

[14] G. Culot, "Addressing Industry 4.0 Cybersecurity Challenges", IEEEManagement Review, Vol. 4, nº 3, 2019.

[15] C. Bodungen, "Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets and Solutions", Singer, 2016.

[16] P. Ackerman, "Industrial Cybersecurity", Packt, 2017.

[17] https://first.org/cvss/

[18] https://nmap.org/

[19] https://us-cert.cisa.gov/

[20] https://cve.mitre.org/

[21] https://www.nist.gov/

[22] https://nvd.nist.gov

[23] https://securityboulevard.com/2020/10/top-5-cybersecurity-frameworks-to-secure-your-organization/

[24] L. Schaefer, "Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges", Cybersecurity for Industry 4.0, Springer