I. J. Computer Network and Information Security, **2020, 1, 1-12**
Published Online February 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2020.01.01

A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem

Ahmet Ali Süzen
Isparta University of Applied Sciences, Department of Information Security, Isparta, Turkey
E-mail: ahmetsuzen@isparta.edu.tr

Received: 09 January 2020; Accepted: 23 January 2020; Published: 08 February 2020

Abstract—The development of technology and uses increases the interconnected digital ecosystem. This is accompanied by dense data usage. Wherever digital data is available, cyber-attacks are threatened and increase the need for cybersecurity prevention. The fact that Industry 4.0 basic fuel is data indicates that the risk of cyber-attack will continue to increase in Industry 4.0. In this study, the sources of cybersecurity threats in the Industry 4.0 ecosystem are examined in the corporate and end-user dimensions. The cybersecurity vulnerabilities most evident in Industry 4.0 systems have been determined to consist of vulnerabilities in control systems protocols, unprotected thing connections, neglect of periodic infiltration tests, inability to manage network devices effectively and untrained personnel. The cyber defense strategies and requirements for these vulnerabilities have been determined. At the same time, corporates and end-users have been told how to implement these preventions. As a result, it is not possible to completely prevent cyber-attacks within the Industry 4.0 ecosystem. Preventing the vulnerabilities identified in the study will ensure that the damage is minimal in attacks.

Index Terms—Cyber Security, Cyber Attack, Defense Strategies, Risk-Assessment, Industry 4.0.

I. Introduction

Centuries ago, industry 1.0 had emerged with the invention and use of steam engines [1]. Industry 2.0 had emerged with the development of electrically powered and mass-produced devices [2]. Industry 3.0 had emerged with the use of robots and computers on the production line [3]. The final step Industry 4.0, called the fourth phase of the industrial revolution, is a period of intelligent manufacturing in which human influence is minimized in the manufacturing process, along with artificial intelligence, the Internet of things, and big data. Industry 4.0 is based on the principles of interoperability, virtualization, independent management, modularity, and real-time [4]. Today, the impact of the great industrial revolution, called Industry 4.0, continues to increase worldwide [5]. It is likely that the dream of creating a super-intelligent society and the desire to make zero mistakes will also be the cornerstones of Industry 5.0.

Cyber-Physical Systems (CPS) are the whole of structures that include intelligent manufacturing systems and provide communication and coordination between the Internet of Industrial things (IIoT) and the physical world, which is also used in Industry 4.0 [3]. CPS is used in manufacturing, research-development, design and sales processes in Industry 4.0. While intelligent manufacturing systems provide serious convenience in our lives, they also lead to the emergence of significant risks such as cyberattacks [6]. In Industry 4.0, all intelligent systems are interconnected with wired or wireless networks by their own identity. Cyber-attacks to these networks will cause irreparable production failures or serious damages. To minimize cyber risks, manufacturers adopting Industry 4.0 must address cyber risks and identify cybersecurity strategies [7]. Instead of applying defense strategies against cyber-attacks to an existing system, implementing during the installation phase of Industry 4.0 would be more helpful in minimizing cyberattack risks [8].

This study describes how cyber-attacks on Industry 4.0 occur and the defense strategies to be prevention against attacks. The layers in Industry 4.0 and their vulnerability were fixed to determine defense strategies. Corporate and personal measures were then determined for these vulnerabilities. It was also evaluated how accurately the current assessment was applied. As a result, the study aims to provide the truest solutions to counter cyberattacks in the Industry 4.0 ecosystem. Therefore, it is envisaged to minimize damage in possible attacks.

The first part of this study describes cyberspace architecture and the Internet of things, which are the data sources of the Industry 4.0 ecosystem. CPS's cyber-attack risks, which the cornerstone of Industry 4.0and the concepts necessary for the creation of cyber defense strategies are also discussed in this section. The second part of the study describes cybersecurity preventions and how these preventions should be implemented for defense strategies to be taken against cyber-attacks. In the final section of the study, the most common cybersecurity weaknesses in Industry 4.0 systems are described. Which layer and how to do cyber-attacks that may occur in institutions, and what kind of effects may occur in institutions as a result of these attacks is stated. In this context, the preventions and strategies which can be taken in creating cybersecurity policies are presented. Today, the transition to Industry 4.0 with full meaning has not

yet occurred. In this study, the shortcomings that exist in terms of cybersecurity during the transition process and how defense preventions should be taken are explained in detail.

II. Related Works

In this section of the study, studies on cybersecurity within Industry 4.0 networks in the literature were examined. In Industry 4.0, cyber-attacks are carried out on IoT [9], Cyber-Physical Systems (CPS) [10], manufacturing [11], and network layers [12]. Solutions have been developed to prevent attacks on these layers [13].

Although there are different security vulnerabilities in CPS, zero-day vulnerabilities have been addressed. These have been investigated in all layers of information exchange. In particular, the security vulnerabilities of SCADA systems are as follows [13].

- Application and database servers
- Human machine interfaces
- Program logic controllers (PLC))
- Remote terminal units
- Communication and network protocols

Secure transfer of data is an important issue in communication between devices. Production problem is caused because of Its modification, deletion or interruption of this data [14]. The literature focuses on DDOS protection and encryption preventions for secure communication [15]. In particular, the safety features of IoT devices need to be considered without purchase. Strong and unique passwords must be identified for the accounts of these devices. It is also recommended to use VPN when accessing wireless networks [16].

As a result, cyber-attacks cause corporations to reduce their productivity and competitiveness. In addition, end-users suffer financial losses and theft of their personal data in these attacks. When studies in the literature are examined, solutions have been proposed or developed to prevent cyber-attacks. But these solutions are aimed at single or specific layers. Prevention covering the whole industry 4.0 ecosystem has not been introduced. Our study covers solutions for the whole industry 4.0. This aspect is projected to be a reference to companies and end-users for cybersecurity.

III. The Attack Goal in Industry 4.0

Industry 4.0 is an industrial revolution in which manufacturing and manufacturing processes are carried out by intelligent systems. In this production process, stages from design to production can be controlled and managed from anywhere [17]. Industry 4.0 also provides an environment in which product and production can be carried out through simulations [18]. Industry 4.0 is generally based on the principles of interoperability, virtualization, autonomous management, real-time, service orientation, and modularity [19].

In order to develop defense strategies against cyber-attacks, the sources of the attack need to be identified. Attacks are targeted on CPS and IoT in Industry 4.0 [20].

A. Cyber-Physical Systems (CPS)

The Industry 4.0 ecosystem is connected to each other through the physical world and the internet through cybersecurity systems (Cyber-Physical System, CPS). In addition, CPS collects traces of sensors and actuators in space and allows them to interact with each other. The CPS model consists of devices that interact with each other and communicate with the physical world [22]. CPS applications can be found in many areas such as manufacturing systems, smart grids, robotics, transportation systems, medical devices, military space, intelligent buildings, including Industry 4.0 concept [23].

The first step in developing CPS systems in the industry is the retrieval of accurate and reliable data from objects. The important point to be made here is that the data comes directly from sensors or from production systems such as ERP, MES, SCM, and CMM. In the information-data transformation step, significant information is extracted from the read data through various tools or methodologies. Cyber architecture is the information center of the CPS [22]. Here, it is carried out processes such as building machine networks, recording their performance and predicting their future behavior. At the fourth level of the CPS, data is presented to expert users, machine situations are visualized and decisions about the process are made. At the final level, feedback is provided to the physical space and the machines are reconfigured. Corrective and preventive decisions are taken at this level [24].

B. Internet of Things (IoT)

IoT is the real-time communication and management of sensors, actuators, control systems and machine networks in the industry, ranging from production to marketing [26]. IoT architecture consists of 3 layers. These are detection, communication and application layers respectively [25]. The risks and threats that may occur in layers of IoT systems are given in Table 1.

Table 1. Risks and threats at IoT layers

IoT Layer Type	Security Threats
Detection	Wireless Signals, Physical Attack, IoT Topology
Network	Traffic analysis, hidden listening, passive monitoring, differences of network hardware and protocols
Application	Security Policies, Authentication Systems

The communication technologies used to connect IoT devices and their standards are given in Table 2. These communication technologies are often used in the data-binding layer, the network layer, the communication layer, and the application layer [27.]

Table 2. IoT communication technologies and standards

Communication	Standard
WiFi	IEEE 802.11 a/c/b/ d/g/n
WiMAX	IEEE 802.16
LR-WPAN	IEEE 802.15.4 (ZigBee)
Z-Wave	Z-Wave Alliance ZAD12837 / ITU-T G.9959
Cellular	2G-GSM, CDMA 3G-UMTS,CDMA2000 4G-LTE
Bluetooth	IEEE 802.15.1
LoRa	LoRaWAN R1.0
NFC	ISO/IEC 18092:2004, ISO/IEC 18000-3
Sigfox	Sigfox
Neul	Neul
6LowPAN	RFC6282
Thread	Thread, based on IEEE802.15.4 and 6LowPAN
LAN	Local Area Network (LAN)

The expansion of plug-and-play devices that make our lives easier on the end-user side brings with it a growth that is difficult to predict. The number of IoT devices available from the internet is approximately 10 percent of the total number of IoT devices, according to queries from the Internet of things search engine Shodan (Sentient Hyper-Optimized Data Access Network-shodan.io). Accordingly, the number of IoT devices, which is 6 billion in 2016, is projected to exceed 20 billion in 2020 [28]. The biggest problem that this growth brings is that the space created by things is not secured [29]. These devices face a serious security threat when the default passwords are not changed.

Things within the ecosystem and connected to the internet need to have pre-determined security strategies. The rapid inclusion of devices in the ecosystem of the Internet of things is leading to a reduction in security prevention. The topics to be considered in determining the security strategies of things used in Industry 4.0 space are summarized below [29].

Privacy: The data generated by the objects have to be accessible only by the authority (user or other devices). Communication of interconnected things must be made over a specific topology.

Integrity: Ensuring that the data comes from the right place and end-to-end safely without being changed.

Usability: To ensure the availability of the data needed by the devices or services in the network within the system.

Authorization: It is the identification of things within the network and the editing of the verification mechanism.

Lighting Solutions: It is the determination of the compatibility of IoT features such as the number of devices in the network and power capacity in determining security solutions.

Heterogeneity: Represents that things with different manufacturers have collaborative working architectures.

Policy: Establishing IoT standards for the management, protection, and communication of data within IoT.

Encryption System: The identification of encryption algorithms for the protection of data during devices data communication.

IV. Cybersecurity

Cybersecurity is the protection of security and privacy against cyber-attacks because of vulnerabilities and specific risks. The priority of cybersecurity is to protect the accessibility, integrity and privacy of data [30]. Any activity that prevents the provision of cybersecurity is seen as a cyber- attack. The goal of cyber-attack is unauthorized access, service blocking, and data tampering (modification, destruction, disclosure, sharing). Cyber-attack are grouped into 5 basic groups within cyberspace [31]. These basic groups and techniques of groups are given below.

- Service blocking attacks: DoS and DDoS attacks
- Malicious software: virus, worm, Trojan, Keylogger, Adware, Spyware, Bot and Scareware
- Phishing
- Unsolicited E-Mail: Spam
- Listening to Network Traffic: Sniffing

A. Vulnerability and Penetration Tests

In order to accurately identify cybersecurity risks within the Industry 4.0 network that vulnerabilities in the system need to be identified. Vulnerability is a problem that allows a network or a process in the network to intervene [31]. Security or vulnerability analyses identify weaknesses in the network that could lead to an information security breach. Vulnerability analysis is to show the effects of detected vulnerabilities by entering the systems in the network. It differs from penetration testing with this feature [32].

Penetration testing is the legal detection of logic errors and weaknesses in a system requested by internationally accredited penetration testing experts. The main purpose of penetration tests is to ensure that the vulnerability is detected without damaging the system [33]. The types of penetration or vulnerability tests that used to perform cybersecurity analyses of Industry 4.0 systems consist of the following headings [34].

- Web Application Tests
- Network Tests
- Mobile Tests
- Client-Side Tests
- Exclusion Tests
- Wireless Network Penetration Tests
- Database Tests
- Social Engineering Tests

Vulnerability found as a result of the tests are grouped in the reporting section according to the impact of the vulnerability and the type of threat [35]. Grouping by type of vulnerability and vulnerability action are shown in Table 3.

The list of commercial, open-source or free tools used to identify vulnerabilities of digital resources within the

Industry 4.0 ecosystem is given in Table 4.

Table 3. Vulnerability types and sample actions

Vulnerability Type	Sample Actions
Critical Level	Taking full control of the server or system.
High Level	Information about the system can be seen and it is possible to search for other vulnerabilities.
Intermediate	Access to a logged-on network or account.
Low Level	Can access informative alerts.

Table 4. Tools used in tests

Acunetix	AppScan	Bup Suite
MetaSploit	Nessus	NetSparker
Nmap	OpenVAS	OWASP ZAP
Retina	SAINT	Shodan.io
Wafw00f	Wapiti	Web Inspect
Wikto	wpscans.com	OutPost24
GamaScan	Probely	Zap
Nexpose	Indusface	BeEF
Qualys	ImmuniWeb	Dradis
W3AF	PureVPN	Rapid7
Websecurify	WireShark	Hping

V. Cybersecurity Defense Strategies

Institutions wishing to implement the Industry 4.0 model need to take prevention against any activity that may lead to undesirable status regarding the privacy, integrity, and accessibility of their data in their cyberspace [36] In order to prevent this, an analysis of where cyber-attacks may come from within the organization must be done. The attacks against Industry 4.0 systems are examined in two main headings. These are human-induced threats and nature-induced threats [37] The most important factors that could threaten the organization's cyberspace are human-induced threats. Human-induced threats vary both internally and externally. In-company human threats are caused by untrained personnel, spies, malicious personnel, or IT manager errors [38]. External threats constitute unauthorized and unauthorized access to the Cyberspace of the institution from the internet environment, activities such as espionage or theft [39].

In Industry 4.0, where the human factor is minimized, the threats faced by the system as a result of cyber-attacks are more than systems in other industrial revolutions. In particular, attacks that affect intelligent production systems can have negative effects on the production activities of institutions. Figure 1 shows how organizations that implement or wish to implement the Industry 4.0 architecture can experience and impact cyber-attacks at which layer [40].

Summarized comparison of the concepts required for the formation of cybersecurity policy within Industry 4.0 on which cyber-attacks are exposed is given in Table 5.

In the act of a cyber-attack known as advanced continuous threats, the attacker may select a designated target or a random target. However, in a cyber-attack, the processes of discovery, scanning, access provision, access protection and deletion of traces are monitored. The stages of cyber-attacks are shown in Figure 2.

IoT devices with the highest vulnerability rates in the industry 4.0 architecture are likely to be more susceptible to cyber-attacks. These vulnerabilities are caused by technological and network security problems in IoT.

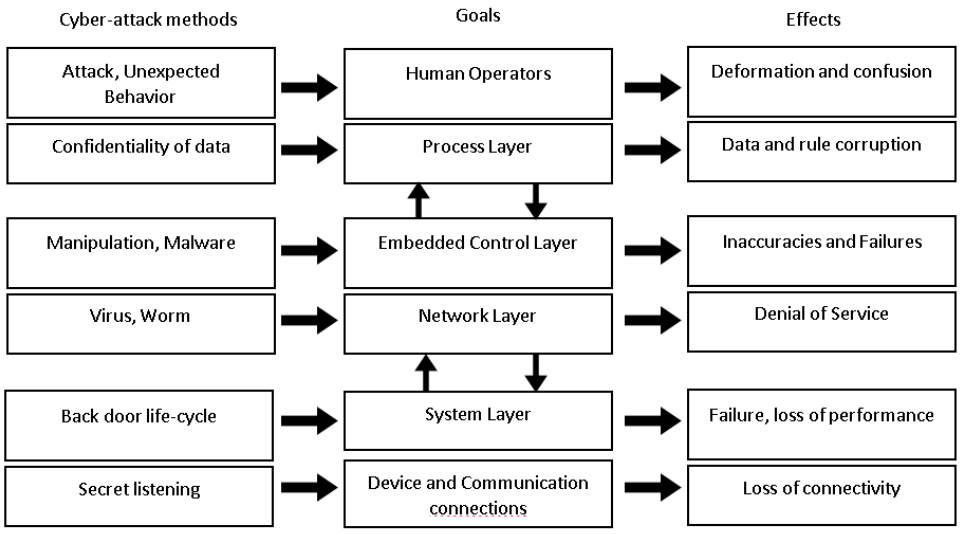

Fig.1. Targets and effects of cyber-attacks in Industry 4.0

Table 5. Classification of cyber-attacks by the way they are implemented [36]

	Cyber Attack Groups																	
	Physical - Traffic Analysis	Physical - Protocol Analysis	Physical - Frequency Jamming	Cyber - Fuzzing (Commands, Parameters)	Cyber - Command Injection	Cyber- Status Data Injection	Cyber - Driver Crash	Physical - Communication Timing	Cyber - Temporary Code Injection	Cyber - Adversary Command Support	Cyber - Command Misinterpretation	CP Component Warning Suppression	Cyber - Communication Bus DoS	Cyber-Physical Memory Readout	Cyber - Protocol Analysis	Physical Memory Write (includes erase)	Cyber - Bus Communication Bridging	Cyber - Malicious Code Removal	Cyber - Connected Devices Infection
Spoofing					X	X											X		X
Tampering									X							X		X	X
Repudiation					X	X											X		
Information Disclosure	X	X		X						X				X	X		X		
Denial of Service			X				X	X		X	X	X	X				X		
Privilege										X						X	X	X	X
Reliability										X	X	X	X			X	X	X	
Safety			X		X	X				X	X	X	X			X	X	X	
Maintainability												X				X		X	X
Availability			X				X	X		X	X	X	X			X		X	
Integrity									X		X								
Confidentiality	X	X		X										X	X				
Authentication										X	X					X	X		
Authorization										X	X					X	X		X
Nonrepudiation					X	X						X					X		
CPS' Physical Reactions		X																	
CPS-Environment Collisions					X	X													
Timing								X											
Reduced Life Time										X	X	X							
Irreparable Damage					X	X				X	X	X							
Damage Surrounding										X	X	X							
Environment Damage					X	X						X							

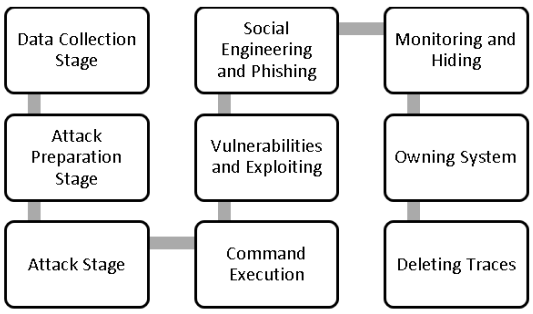

Fig.2. Stages of attack in cyber-attack [31]

According to the studies, three main problems in ensuring IoT security are identified. These problems are caused by privacy, performance and encryption techniques [39-40]. Techniques can be developed to ensure the safety of IoT devices as follows.

- Software running on IoT devices should be allowed to log on.
- IoT devices must log on to the network before data communication.
- Since IoT devices have limited processing and memory capabilities, there must be a firewall on the network to filter data packets.
- Updates for IoT devices must be installed so that no additional bandwidth is used.

Shodan.io, is the scanning engine used to search for IoT devices connected to an IP or domain. Shodan attitudes a serious cybersecurity threat to the Industry 4.0 system. When this scanning engine detects an open port, it tries to connect to the port and records it [41]. Different users who are members of the application can search through these records. If IoT devices are used within the company, The Information Security Authority is required to make IP or domain queries on such applications. Figure 3 shows an example of a query made within the Shodan application. As a result of the query, it is possible to access the open port, location, database, server status of IP or domain.

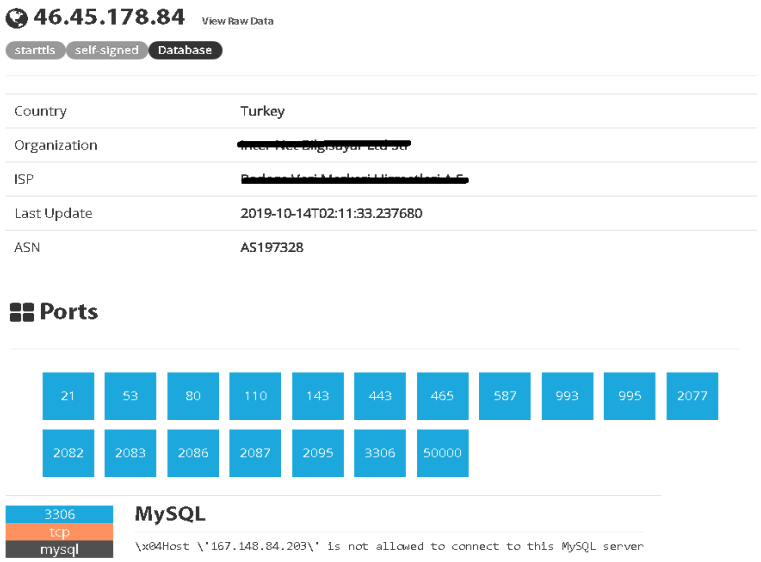

Fig.3. Shodan.io query results

Table 6. Critical cybersecurity checks

Simple Controls	Basic Controls	Administrative Controls
• Inventory and control of hardware assets • Inventory and control of software assets • Continuous Vulnerability Assessment • Controlled Use of Authority • Secure Configuration for hardware and software of mobile devices, computers, workstations, and servers • Daily records maintenance, monitoring, and analysis	• E-mail and Web Browser security • Malware Protection • Control of Network Ports, Protocols and Services • Data Recovery and backup • Secure Configuration for network devices • Environmental Safety • Data Protection • Secure and controlled access • Wireless Access Control • Account monitoring and control	• Implementation of security awareness and training • Application Software Security • Event Management • Penetration Tests

A. Cyber Attack Defense Strategies for Corporations

Cyber-attacks are an important consideration, especially for institutions and national structures using Industry 4.0. The research conducted by the Center for internet security at SANS Institute identified 20 categories under 3 main headings for the preventions of critical cybersecurity controls of institutions. This notation is given in Table 6 [42].

Reports from security firms also show that today;

- Cyber espionage activities and critical infrastructure security,
- Use of machine learning and artificial intelligence in cyber-attacks,
- Services for criminal conduct (CaaS) as a service,
- IoT security,
- Attacks on biometric security systems,
- Improved/customized malware,
- Types of ransomware,
- Threats such as predefined and weak passwords come to the fore [34].

Table 7. Prevention classification for cyber defense strategies

Privacy	Risk Management	**Authentication**	Physical Security	**Accuracy**	Virus detection and Prevention
	Platform Security		Risk Condition Management		Penetration and Vulnerability tests
	Connection Management		Business Continuity		Infrastructure Security Management
	Firewall		Emergency Management		
	Encryption				
	Password Management				
	Certificate Management				
	Personnel Safety				
	Security Policy				

In order to implement cybersecurity within cyberspace, the competencies shown in Table 7 under the headings privacy, integrity, accuracy, presence and authentication are required.

In Industry 4.0, companies need to know the vulnerability they may face in their cyberspace and how to take preventions against them. The next section of the study will explain the prevention that institutions must take to protect their cyberspace.

a. Information Security Policy

In particular, institutions that adopt the digitization policy or wish to implement the Industry 4.0 architecture need to determine information security policies and continuously monitor their applicability. It should take advantage of ISO/IEC 27001 and ISO/IEC 27002 standards when establishing internal information security policies. The ISO/IEC 27001 standard defines the information security management process, while the ISO / IEC 27002 standard includes security preventions related to the management process given in 27001. In addition, when preparing information security policies, they should include the following topics under the headings of privacy, integrity, and accessibility [43].

- Access control
- Physical and environmental safety
- Clean table and clean screen
- Information transfer, communication security
- Restrictions on software installation and use
- Backup
- Mobile devices and remote operation
- Protection from malicious software
- Use of cryptographic controls
- Management of technical openings
- Information Classification
- Supplier relations
- Human resources security

Finally, in order to carry out internal policies, a staff trained in information security must be appointed as an information security officer and provide internal coordination.

b. Vulnerabilities in Industrial Control Systems Protocols

Communication protocols used in industrial control systems are divided into an open system and closed system communication protocols. Open system communication protocols are developed in such a way as to enable communication between manufacturer-independent and similar devices. Closed system communication protocols are special protocols developed to provide communication only between the manufacturer's own devices. These protocols are used in many high-scale applications such as energy, water, transportation, healthcare, banking, nuclear/chemical facilities, and communications [44].

Remote monitoring and control large-scale systems spread over large areas are provided by industrial control systems or Supervisory Control and Data Acquisition, (SCADA). Especially in Industry 4.0, SCADA systems will play an important role in monitoring and managing production processes. API 1164 security protocol was first published in the security standards of SCADA systems. The most commonly used communication protocols are DNP3, Modbus and Profinet in SCADA systems. A vulnerability in SCADA space can have far more critical or far-reaching effects than other industrial systems [45]. Table 8 given the types of SCADA vulnerabilities and their causes arising from basic SCADA functions.

Table 8. Vulnerabilities and possible causes that can access basic SCADA functions [45]

Type of Vulnerability	Source of Vulnerability
Known Vulnerabilities	Legacy or patched third-party applications added to control systems
Unpublished Vulnerabilities	Exposing the server of control systems over unnecessary services
Communication Channel Vulnerabilities	Remote access protocols for remote control of control systems
Communications Endpoint Vulnerabilities	Server applications or database vulnerabilities that are vulnerable to communication and data transfer protocols
Server Authorization Vulnerabilities	Error in server configuration security
Network Vulnerabilities	Faulty network design, poor firewall rules, and network device configuration errors

c. Staff Training

The fact that data is based on Industry 4.0 increases attacks on cyberspace. The most critical prevention to be taken here must be carried out by the corporation's IT managers. To do this, the staff need to know the source and target of the attack. System administrators and other relevant technical personnel are required to periodically provide cybersecurity training. After that, it is necessary to determine the qualifications of the personnel receiving training. There are many institutions/organizations providing corporate cybersecurity training in countries. In-corporation security staff should definitely have participated in cybersecurity certification training. In this training, they learn how to take preventive preventions on cybersecurity by using the tools and techniques used in cyber-attacks. The following are the certifications used in the field of cybersecurity which have international validity.

- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Certified Network Defender (CND)
- Cyber Security Certification: GPEN
- ISO 27001

The weakest link in a corporation's security level is the staff factor. Although technically prevention is taken, the cyber threat will continue as long as staff weaknesses occur. At this point, the most important part of information security is security awareness. In order to do

this, all staff from the lowest employee to the highest manager must have information security awareness. In order to raise awareness of information security on staff, in-service training needs to be provided. The topics that should be for information security in in-service training are given below.

- Secure password creation
- Storing personal and corporate passwords
- Where and how cyber threats can occur
- Social engineering
- Internet and email security
- File access and sharing
- Use of backup systems

d. Effective management of network assets

All cyber-crimes committed take place over networks in information technologies. Therefore, the network infrastructure of the organization or system should be used effectively. The log is the first prevention taken against cyber-attacks or cybercrime. Thus, in cases of a possible crime, these records are examined and preliminary information about the violation is generated.

No matter how powerful a company's software infrastructure is, if there is an effectively unstructured or poorly constructed network infrastructure, it will be vulnerable to cyber-attacks. The following are the steps to be taken to effectively manage network systems [46].

Inventory and Control of Hardware Assets: When all devices in the network ecosystem are registered and a new device provides unauthorized access, the suspicious device can be marked with systems such as Change Management and Source control.

Inventory and Control of Software Assets: The authorized applications within the network must be removed and safe listing must be used. Changes made to the system by software exceeding the Secure list must be logged.

Identity, Access and Authority Control: Identity and access management (IAM) applications should be used to monitor access to systems. Each staff should not be given more authority than his or her duties and their access to identification should be restricted.

Data Backup: A strict backup policy must be taken at certain time intervals for business densities, databases, and business continuity. It is especially important to have a backup against ransomware.

Configuration policy of network devices: Policy Orchestration, which controls policies on network devices and detects policies and rules that are not used at all, should be used [19].

Wireless Network Control: 802.1 X can be activated with MAC filtering to devices that log into the network wirelessly within the network.

Audit and Breach of Authority: One of the most significant attacks on user accounts is an account upgrade attack. To prevent this, accounts created, deleted or passive on the system need to be inspected [47].

e. Use of enterprise security software

One way to build defenses against cyber-attacks is by using in-corporation security software. This software provides protection against attacks against vulnerabilities in the internal network. In general, security software provides a firewall, network intrusion protection, spam filtering, and webcam protection, creating an effective firewall for in- corporation pre-security operations. Table 9 gives 2019 performance tests of enterprise-used security software conducted over 732 samples. When viewed as effectiveness, it is seen that security software performs the same task, but differs in performance and intervention effect maintenance.

Table 9. Performance tests of enterprise security software [48].

Row	Product	Block Protection Rate	Protection Rate	Incorrect Warning
1	Kaspersky	732	100%	0
2	Bitdefender	732	100%	6
3	VIPRE	731	99.9%	2
4	Microsoft	730	99.9%	24
5	Sophos	730	99.7%	5
6	McAfee	729	99.6%	5
7	K7	729	99.6%	10
8	Avast	728	99.5%	2
9	Panda	728	99.5%	19
10	CrowdStrike	725	99.0%	8
11	Cisco, ESET	724	98.9%	3
12	SparkCognition	722	98.6%	3
13	Seqrite	719	98.6%	26
14	FireEye	720	98.4%	2
15	Endgame	719	98.2%	25
16	Fortinet	718	98.0%	5

B. End-User Cyber Attack Defense Strategies

Although Industry 4.0 being said for corporations and industry, the end users form the user part of the smart home and smart city model within the Industry 4.0 network. End-users need to know how to protect or take precautions in a home, hotel, cafe, outdoor environment or place where access to the internet is available.

a. Ransomware

Ransom viruses are a type of malware that infects computers in different ways and demands money from their victims. Ransomware encrypts files stored on the infected computer. It is known as ransomware because it asks the user for money to decode the encrypted files again [49]. After encrypting all the files on the infected system, this virus instructs the user to receive decryption software by sending a warning message that "all your files are encrypted by the virus". Ransomware can infect the computer in four different ways. These;

- Social Engineering
- Exploit Kits
- Harmful Advertising

- Drive-by Downloads

Files downloaded from the internet must be run on secure sandboxes to be created by the priority Sandbox for protection from ransomware. Sandbox software allows you to open files on a virtual space it creates and allows you to avoid potential risk situations [50]. Viruses that come with e-mail are not executable files but usually come with file extensions such as zip and rar. Therefore, the user must take prevention personally. For example, in e-mails from institutions, document files are not sent in compression programs. The PDF format is preferred for correspondence such as invoices, contracts, petitions and information. Other than that, attachments should be skeptical and should not be opened without a virus scan.

Although methods are recommended to protect your information on the digital, attacks are exposed. Information needs to be backed up to external sources to minimize damage from an attack. At this point, cloud systems offer practical solutions. Many cloud backup systems instantly transfer your system information to servers. These backups can be restored after file deletion, attack or virus threat. Table 10 lists the providers, storage areas, and supported platforms that offer free storage of data on the cloud server.

Table 10. Cloud storage providers

Provider	Free Storage	Platform
Dropbox	2 GB	Windows, Mac, iOS, Android
Google Drive	15 GB	Windows, Mac, iOS, Android
Media Fire	10 GB	Windows, iOS
OneDrive	5 GB	Windows, iOS, Android
Amazon Drive	5 GB	Windows, iOS, Android
Box	10 GB	Windows
Yandex Disk	10 GB	Windows, iOS, Android
Apple iCloud	5 GB	iOS
Mega	50 GB	Windows, iOS
IDrive	5 GB	Windows, iOS, Android
Sync	5 GB	Windows, Mac, iOS, Android
SpiderOak	2 GB	Windows, iOS, Linux
HubiC	25 GB	Windows, iOS, Android
pCloud	10 GB	Windows, Mac, iOS, Android, Linux

b. Public wireless network connections

Wireless network services are available to all, especially in hotels, cafes or outdoor settings. Getting online from places like this is pretty dangerous. The biggest threat is that the attacker is in the same network as the user. This way, instead of being targeted by the attacker, the user can access the information about the private operations that the user has done by listening to the network and following the network. In Internet networks where password-free connections are used, the prevention that can be taken to avoid being exposed to cyber-attacks is given as follows.

SSL certified web pages: In public wireless network connections, the most secure operation is performed on SSL certified sites with https connections. If the websites entered have SSL security, their addresses start with the" https:// " tag [51]. In addition, the "Always use HTTPS" option should be enabled on websites where login information should be entered in the browser. Although secure connection over https is provided, it is recommended that sensitive accounts such as Bank, university, government or organization pages are not accessed.

Virtual Private Network (VPN): VPN connections are one of the most powerful preventions that can be taken in public wireless networks. VPN provides a secure and encrypted connection to the point where the user wants to go via the internet [52]. The creation of these connections is done with software on Mac/Windows/iPhone/Android operating systems. The software that provides VPN connections usually does this with a fee. The most preferred VPN software that prioritizes privacy and internet connection are given in Table 11.

Table 11. VPN software

NordVPN	Cyber Ghost VPN	ExpressVPN	Opera
PrivateVPN	IVACY	SurfShark	TunnelBear
ProtonVPN	PureVPN	PIA	Zenmate
Hotspot Shield	Windscribe	hide.me	SaferVPN

Share Settings: Many end-users do not control the sharing settings within the operating system. Again many users have my documents, my pictures, etc. personal folders are open for sharing. The user can safely protect shared folders within his own encrypted network. But these folders pose a huge risk to public network connections. Systems within the same network access each other easily. If there are shared folders, other users or attackers can access them. To prevent such attacks, they must turn off sharing options from the "network and Sharing Center" menu in the operating system's control panel.

c. Password stealing methods

An attacker uses different methods to obtain passwords belonging to the user. These methods vary according to the method of attack and the connected network. To steal passwords of the users, methods such as dictionary attack, brute-force attack, fishing attack and social engineering are preferred.

Dictionary Attack: The dictionary attack, which is one of the classic password stealing methods, is performed by applying combinations that the attacker has created previously [53]. The most powerful way to counter such attacks is to create a strong password. In addition, it is necessary to be careful not to use personal information in passwords created.

Brute Force Attack: In this attack known as brute force attack, the characters required to create the password are randomly generated from letters, numbers, or symbols and used by trial and error. In this type attack,

there is a chance that passwords will be broken because all combinations are tried. However, depending on the length and strength of the password, this possibility can be quite difficult [54].

Passwords created must meet certain requirements in order to be strong. These requirements can be sorted as follows [55].

- Must be created from at least 10 characters.
- There must be numbers and characters as well as letters.
- Can be used in combination with uppercase and lowercase letters.
- It should not consist of personal information.
- Words found should not be used in the dictionary.

Phishing Attack: The phishing method spoofs the sites of publicly known and trusted organizations and institutions, and allows users to log into these fake sites [56]. Usually, the user is sent e-mail from fake e-mail addresses that are thought to belong to these secure sites. In these e-mails, the user is asked to sign in to the site that is opened by clicking on the link in the e-mail. Thus, phishing is carried out. All users with e-mail accounts are likely to be exposed to phishing attacks. For example, an e-mail sent to" Bank X "may steal session information, or malware found in the attachment file of an e-mail under the heading" your electricity bill " may infect your device. As a result, it can sometimes be very difficult to detect the attack from very well-edited e-mails.

To avoid phishing attacks, it is necessary not to provide access to pages directed from e-mail content. Instead, the user should log in to the site by typing the address of that site into the browser himself. Most spam e-mails for phishing require message delivery verification to determine if the message has been received. Spam e-mails should never be responded. One of the general preventions to be taken in the last step is the use of security software with spam filtering feature.

Social Engineering: This method happens when the attacker defrauds the user with a specific scenario from the real world. The attacker using social engineering often uses his abilities and convinces the user. Such attacks are especially carried out by phone and e-mail nowadays. When social engineering attacks on users are examined, it is seen that six different techniques are applied [57]. These techniques can be sorted as follows:

- Counterfeit product and service
- Fake news sites or pages
- Phone
- Garbage mixing
- Suasion
- Trojans

The most important of the basic preventions that can be taken against attacks by social engineering method is to show a skeptical attitude towards unknown phones or e-mails. In addition, similar attacks have applied to software such as Truecaller or Dialer on mobile phones and phone numbers may have been saved. Using this software's makes you aware of recorded attacks.

d. Use of personal security software

End-users are required to use security software to protect their computers against attacks and threats. Security software provides internet and computer security of computers. Nowadays there are too many security software that have this function. The comparative results of the current software for real-world protection and malware protection made by AV-Comparatives test for 2019 are given in Table 12. The results of the security tests show that the capabilities and impact of most security software are similar. The most important factor for providing security software solutions is that the databases are constantly updated.

Table 12. Comparison of end-user security software [58].

Rank	Product	Real-World Protection	Malware Protection Testing
1	Bitdefender	100%	100%
2	Avira	100%	100%
3	Symantec	100%	100%
4	Microsoft	100%	100%
5	Trend Micro	100%	100%
6	McAfee	99.7%	99.9%
7	VIPRE	99.7%	100%
8	Total Defense	99.7%	100%
9	Avast	99.4%	100%
10	AVG	99.4%	100%
12	Panda	99.1 %	100%
13	Kaspersky	99.1 %	99.9%
14	F-Secure	98.6 %	99.9%
15	Eset	98.3%	99.9%

VI. Conclusions

In this study, the defense strategies that end-users and corporations in the Industry 4.0 space should take against cyber threats are explained. Firstly, the sources of possible attacks have been identified in order to determine defensive strategies. In these lights, suggestions for solutions were made to prevent attacks. In Corporate layers have problems that staff training, the security of IoT devices, lack of effective use of network assets. In end-user use, the lack of strong passwords and lack of security software have been identified. In the study identified all prevention to be taken against cyber-attacks. Therefore, a certain process is required for the implementation of the study results. It is easier for the end-user to take prevention against cyber-attacks. But it is imperative that corporations implement these preventions more carefully.

References

[1] Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. Business & Information Systems Engineering, 6(4), 239-242.

[2] Lee, J., Bagheri, B., & Kao, H. A. (2015). A Cyber-Physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23.
[3] Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10.
[4] Gorecky, D., Schmitt, M., Loskyll, M., & Zühlke, D. (2014, July). Human-machine-interaction in the industry 4.0 era. In Industrial Informatics (INDIN), 2014 12th IEEE International Conference (pp. 289-294). IEEE.
[5] Almada-Lobo, F. (2016). The Industry 4.0 revolution and the future of manufacturing execution systems (MES). Journal of innovation management, 3(4), 16-21.
[6] Zhou, K., Liu, T., & Zhou, L. (2015, August). Industry 4.0: Towards future industrial opportunities and challenges. In Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on (pp. 2147-2152). IEEE.
[7] Jazdi, N. (2014, May). Cyber physical systems in the context of Industry 4.0. In Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on (pp. 1-4). IEEE.
[8] Lee, J., Bagheri, B., & Jin, C. (2016). Introduction to cyber manufacturing. Manufacturing Letters, 8, 11-15.
[9] Lu, Y., & Da Xu, L. (2018). Internet of things (iot) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115.
[10] Hsu, D. F., Marinucci, D., & Voas, J. M. (2015). Cybersecurity: Toward a secure and sustainable cyber ecosystem. Computer, (4), 12-14.
[11] Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. Manufacturing Letters, 2(2), 74-77.
[12] Gupta, G. P., & Kulariya, M. (2016). A framework for fast and efficient cyber security network intrusion detection using apache spark. Procedia Computer Science, 93, 824-831.
[13] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97-110.
[14] Kogiso, K., & Fujita, T. (2015, December). Cyber-security enhancement of networked control systems using homomorphic encryption. In 2015 54th IEEE Conference on Decision and Control (CDC) (pp. 6836-6843). IEEE.
[15] Semerci, M., Cemgil, A. T., & Sankur, B. (2018). An intelligent cyber security system against DDoS attacks in SIP networks. Computer Networks, 136, 137-154.
[16] Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. IEEE Communications Surveys & Tutorials, 14(4), 981-997.
[17] Bahrin, M. A. K., Othman, M. F., Azli, N. N., & Talib, M. F. (2016). Industry 4.0: A review on industrial automation and robotic. Jurnal Teknologi, 78(6-13), 137-143.
[18] Zheng, P., Sang, Z., Zhong, R. Y., Liu, Y., Liu, C., Mubarok, K., Xu, X. (2018). Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. Frontiers of Mechanical Engineering, 1-14.
[19] Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. Engineering, 3(5), 616-630.
[20] Petrasch, R., & Hentschke, R. (2016, July). Process modeling for Industry 4.0 applications: Towards an Industry 4.0 process modeling language and method. In Computer Science and Software Engineering (JCSSE), 2016 13th International Joint Conference on (pp. 1-5). IEEE.
[21] Aksoy, B , Uğuz, S , Oral, O . (2019). Comparison of The Data Matching Performances of String Similarity Algorithms in Big Data. Journal of Engineering Sciences and Design, 7 (3), 608-618. DOI: 10.21923/jesd.467036
[22] Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010). Security issues and challenges for cyber physical system. In Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & International References Conference on Cyber, Physical and Social Computing (pp. 733-738). IEEE Computer Society
[23] He, K., & Jin, M., (2016). Cyber-Physical System for maintenance in industry 4.0, Jönköping University School of Enginering, 64p.
[24] Bagheri, B., Yang, S., Kao, H., Lee, J., (2015). Cyber-Physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment, IFAC-Papers Online, 48-3 1622–1627.
[25] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.
[26] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.
[27] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.
[28] Barnaghi, P., & Sheth, A. (2016). On searching the internet of things: Requirements and challenges. IEEE Intelligent Systems, 31(6), 71-75.
[29] Pancaroğlu, D., (2018). An Analysis on the Current State of Security in the Internet of Things, International Conference on Cyber Security and Computer Science (ICONCS'18), Safranbolu, Turkey.
[30] Von Solms, R., & Van N., J. (2013). From information security to cyber security. computers & security, 38, 97-102.
[31] Akin, M , Sağiroğlu, Ş . (2017). Gelişmiş Sürekli Tehditler. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi , 10 (1) , 1-10 .
[32] Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010, June). Using Bayesian networks for cyber security analysis. In Dependable Systems and Networks (DSN), 2010 IEEE/IFIP international conference on (pp. 211-220). IEEE.
[33] Arkin, B., Stender, S., & McGraw, G. (2005). Software penetration testing. IEEE Security & Privacy, 3(1), 84-87.
[34] STM, (2018), Siber Tehdit Durum Raporu, Access Date: 10.02.2019, Access Link: https://thinktech.stm.com.tr/uploads/raporlar/pdf/2072018175818369_stm_siber_tehdit_durum_raporu.pdf
[35] Baheti, R., & Gill, H. (2011). Cyber-Physical systems. The impact of control technology, 12(1), 161-166.
[36] Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2012, August). Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In Resilient Control Systems (ISRCS), 2012 5th International Symposium on (pp. 55-62). IEEE.
[37] Chen, C. K., Zhang, Z. K., Lee, S. H., & Shieh, S. (2018). Penetration Testing in the IoT Age. Computer, 51(4), 82-85.
[38] Dürrwang, J., Braun, J., Rumez, M., Kriesten, R., & Pretschner, A. (2018). Enhancement of Automotive Penetration Testing with Threat Analyses Results. SAE International Journal of Transportation Cybersecurity and

Privacy, 1(11-01-02-0005), 91-112.
[39] Çakır, H , Yaşar, H . (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3 (2), 488-507.
[40] Arslan, H., Aslan, H., Karkı, H. D., & Yüksel, A. G. (2018, September). Blockchain and Security in the IoT Environments: Literature Review. In 2018 3rd International Conference on Computer Science and Engineering (UBMK) (pp. 254-257). IEEE.
[41] Han, K. H., & Lee, S. H. (2016). A Study on the Security Threats of IoT Devices Exposed n Search Engine. The transactions of The Korean Institute of Electrical Engineers, 65(1), 128-134.
[42] Micro, T. (2016). Addressing the SANS TOP 20 critical security controls for effective cyber defense. A trend Micro Whitepaper.
[43] TSE ISO/IEC 27001 Information Technology, Security Techniques, Code of Practice for Information Security Management, Access Date : 10.01.2019, Erişim Link : https://www.tse.org.tr/IcerikDetay?ID=2311&ParentID=6890
[44] Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498-506.
[45] Erkek, İ., (2018). Modbus Temelli Scada Sistemlerinin Siber Güvenliği İçin Yeni Bir Yaklaşım, Yüksek Lisans Tezi, Gazi Üniversitesi,133p.
[46] SANS / CIS, CIS Critical Security Controls, Access Date: 01.01.2019, Access Link: https://www.sans.org/critical-security-controls
[47] ÇözümPark, Siber Güvenlik İçin 20 Önemli Madde, Access Date: 01.01.2019, Erişim Link: http://www.cozumpark.com/blogs/gvenlik/archive/2017/05/28/siber-guvenlik-in-20-onemli-madde.aspx
[48] AV-Comparatives, Business Security Test 2019, Access Date: 10.10.2019, Access Link: https://www.av-comparatives.org/tests/business-security-test-2019-march-june/
[49] Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Computers & Security, 74, 144-166.
[50] Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).
[51] Hickman, K., & Elgamal, T. (1995). The SSL protocol. Netscape communications corp, 501.
[52] Demir, F. (2010). Güvenli Veri İletiminde Kullanılan VPN Tiplerinin Uygulaması ve Performans Analizi (Doctoral dissertation, Fen Bilimleri Enstitüsü).
[53] Herley, C., & Van Oorschot, P. (2012). A research agenda acknowledging the persistence of passwords. IEEE Security & privacy, 10(1), 28-36.
[54] Süzen, A., A., Şimşek, M., A., Kayaalp, K., Gürfidan, R., (2019). The Attack Methodology to Wireless Domains of Things in Industry 4.0. Nevşehir Bilim ve Teknoloji Dergisi, 8, 143-151. DOI: 10.17100/nevbiltek.557886
[55] B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L, & Christin, N. (2012). How does your password measure up? the effect of strength meters on password creation. In Presented as part of the 21st Security Symposium Security 12) (pp. 65-80).
[56] Hong, J. (2012). The state of phishing attacks. Commun. ACM, 55(1), 74-81.
[57] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.
[58] AV-Comparatives, Real-World Protection Test 2019, Access Date: 15.10.2019, Access Link: https://www.av-comparatives.org/tests/real-world-protection-test-jul-aug-2019-factsheet/

Authors' Profiles

Ahmet Ali SÜZEN is head of cyber security application and researching center at Isparta University of Applied Sciences. He completed his doctorate in computer engineering. He has program development experience cyber security, deep learning and software development. He has 4 books in the field of deep learning and software development. He has been editor-in-chief of the journal in two 2 international journals in the field of engineering. He also has project management experience, having successfully completed 2 projects about cyber security and mobile software development.

How to cite this paper: Ahmet Ali Süzen, "A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.1, pp.1-12, 2020. DOI: 10.5815/ijcnis.2020.01.01