Chapter 16
Overview of Cyber Security in the Industry 4.0 Era

Beyzanur Cayir Ervural and Bilal Ervural

Abstract The global development industry is in the midst of a transformation to meet today's more complex and highly competitive industry demands. With the rapid advances in technology, a new phenomenon has emerged in the current era, Industry 4.0. The integration of information technology and operational technology brings newer challenges, especially cyber security. In this chapter, one of the most popular topics of recent times, cyber security issue, has been investigated. The occurrence of the Internet of Things (IoT), has also dramatically altered the appearance of cyber threat. Security threats and vulnerabilities of IoT, industrial challenges, main reasons of cyber-attacks, cyber security requirement and some cyber security measures/methods are discussed with a global perspective involving both the public and private sector in the IoT context.

16.1 Introduction

Industrial revolutions are the most important milestones that have changed the course of human history. According to many researchers, the industrial revolution affects people's lifestyle even more than the science revolutions (Wendt and Renn 2012).

After the discovery of steam power, revolutions have evolved with a rapid change parallel to the needs of each era. Other subsequent revolutions have emerged as electric energy-driven mass production in the early part of the twentieth century, and the use of highly efficient electronic automation in the industrial environment in the 1970s, and finally recently emerged as, Industry 4.0, which has

B.C. Ervural (✉) · B. Ervural
Department of Industrial Engineering, Faculty of Management, Istanbul Technical University, 34367, Maçka, Istanbul, Turkey
e-mail: cayirb@itu.edu.tr

B. Ervural
e-mail: bervural@itu.edu.tr

A. Ustundag and E. Cevikcan, *Industry 4.0: Managing The Digital Transformation*, Springer Series in Advanced Manufacturing, https://doi.org/10.1007/978-3-319-57870-5_16

come with data-driven production systems, more specifically cyber-physical systems or Internet of Things (IoT) (Rüßmann et al. 2015).

In the present era, the world is at the beginning of the fourth industrial revolution based on IoT. The IoT relies on a variety of enabling technologies such as wireless sensor networks (WSNs), machine-to-machine (M2M) systems, big data, cloud services and smart applications as well as radio frequency identification (RFID) systems (Yang et al. 2010).

The novel change in industries, also known as Industry 4.0, take a great interest from manufacturing companies. It is crucial for manufacturing companies around the world with operational efficiency, productivity and customization features. Industry 4.0 provides dealing with huge data volumes, developing human-machine interactive systems and improving communication between the digital and physical environments (Frost and Sullivan 2017).

Industry 4.0 includes three essential stages: Firstly, getting digital records through sensors that attached to industrial assets, which collect data by closely imitating human feelings and thoughts. This technology is known as sensor fusion. Secondly, analyzing and visualizing step includes an implementation of the analytical abilities on the captured data with sensors. From signal processing to optimization, visualization, cognitive and high-performance computation, many different operations are performed with background operations. The serving system is supported by an industrial cloud to help to manage the immense volume of data. Thirdly, the stage of translating insights to action involves converting the aggregated data into meaningful outputs, such as additive manufacturing, autonomous robots and digital design and simulation. In an industrial cloud, raw data is processed with data analytics applications and then turns into practically usable knowledge.

With Industry 4.0, the interconnected era also dawns. Interconnection provides a link between partners, customers, employees, and systems to accelerate business performance and create new opportunities with collaborating on a shared platform. Interconnection is a requirement for instant access to interdependent and real-time data between industries or between different geographies. The industrial cloud provides a common platform to store data and to collaborate users from various geographies.

Increasing data density with Industry 4.0 and the fusion of information technology and operational technology brings with it newer challenges, particularly of cyber security (Frost and Sullivan 2017). Cyber security is the core issue that all governments follow at the highest level of importance. It is a protection of business information and precious knowledge about a subject or system in digital shape against abuse, unauthorized access and thefts (Kaplan et al. 2011). With expanding network connections, cyberattacks have become more prevalent due to the rising prone to misuse data for different purposes such as financial and strategic reasons.

The boom of new technologies and the increasing societal dependence on globally interconnected technology, the automation, and commodification of the tools of cyberattack, the sophisticated hacker attacks and the low safety measures in the cyber market, are undoubtedly important (Weber and Studer 2016). With the number of potential attackers and the growing size of the network, the tools that

potential attackers can use are becoming more sophisticated, efficient and effective. Therefore, it needs to be protected against threats and vulnerabilities in order to achieve the highest potential of IoT (Kizza 2009; Taneja 2013; Abomhara and Kien 2015).

The widespread use of connected devices and services at the IoT has brought about new forms of cyber defense in order to ensure robust security (Sathish Kumar and R. Patel 2014; Abomhara and Kien 2015). Cyber-attacks and threats have increased tremendously in the last decades. Any stakeholder that uses IoT systems is directly or indirectly affected by this matter. Especially large companies are exposed to malicious attacks that result in serious financial burdens in addition to immeasurable losses such as data corruption, system crashes, privacy breaches, prestige, customer, reliability and market losses.

In many organizations, cyber security is primarily considered as a technology issue. Public and private company executives/authorities are aware of the danger, and do not want to allow attackers to access critical business information and employee and customer-specific information (Kaplan et al. 2011). Generally, organizations not officially report the cyber-attacks they are subjected to. To be honest, businesses do not tend to disclose security vulnerabilities that they have to pay ransom for cybercriminals (Kaplan et al. 2011). Most large companies have considerably strengthened their cyber security capabilities in recent years. Millions of dollars have been spent to develop new strategies with technological investments in information technology (IT) security to reduce the risk of cyber-attack.

Internet-based systems will become more attractive for cyber-attacks if IoT achieves a large growth by 2020 (Capgemini 2015). Several companies and organizations have predicted the number of things to connect internets in the coming years (Weber and Studer 2016). According to Gartner predictions, the number of network-connected devices is estimated at 20.8 billion, with Cisco estimated to have about 50 billion IoT connections by 2020, and finally, Huawei's projection shows that by 2025, the number of connections will reach 100 billion. Despite the differences in estimates, the most important result is to expect an important growth. The most obvious inference is that there will be a massive amount of Internet-enabled devices that require a comprehensive protection system soon (Weber and Studer 2016). Figure 16.1 shows the number of connected devices worldwide from 2012 to 2025 (Columbus 2016).

Increasing cyber-attacks in recent years, with victims ranging from individuals to governments around the world, continue to alarm. The year 2014 was declared the Year of the Breach and 2015 was renamed by some industry commentators as the Year of the Breach 2.0. (Weber and Studer 2016). As seen from the general perspective, it is obvious that the cyber-attacks have caused a great deal of damage to the whole world. To prevent cyber-attacks, organizations should educate consumers about the appropriate safety procedures that should be followed while using an IoT system (Capgemini 2015).

This study aims to discuss some issues, such as the increase in data intensity and seriously growing cyber threats due to employing information technology, in the recently emerged concept, Industry 4.0. The widespread use of IoT leads to an

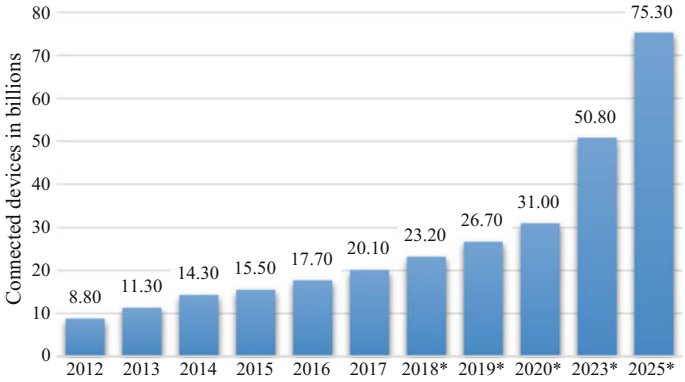

Fig. 16.1 The number of connected devices (Internet of Things) worldwide from 2012 to 2025

increase in the number of interconnected companies, which automatically results in a serious amount of cyber-attacks.

In this chapter, security threats and vulnerabilities of IoT are discussed in Sect. 16.2. Section 16.3 provides industrial challenges. Evolution of cyber-attacks is given in Sect. 16.4. Some cases focus on cyber-attacks and solution approaches are discussed in Sect. 16.5. Strategic principles of cyber security and cyber security measures/methods are respectively provided in Sects. 16.6 and 16.7. The conclusions are presented in Sect. 16.8.

16.2 Security Threats and Vulnerabilities of IoT

There is no single universal consensus on architecture for IoT. Different architectures have been proposed by different researchers (Sethi and Sarangi 2017). In general, the IoT can be divided into four main levels. Figure 16.2 shows both the level architecture of the IoT and some basic components in each level.

- *Perception (Sensing) layer*: The perception layer is also called as 'Sensing Layer'. It composed of physical objects and the sensing devices such as various forms of sensory technologies, RFID sensors. These technologies allow devices to sense other objects.
- *Network layer*: Network layer is the infrastructure to support wireless or wired connections between sensor devices and the information processing system.
- *Service layer*: This layer is to ensure and manage services required by users or applications. It is responsible for the service management and has a link to the database.
- *Application (Interface) layer*: Application or interface layer composed of interaction methods with users or applications. It is responsible for delivering application services to the user.

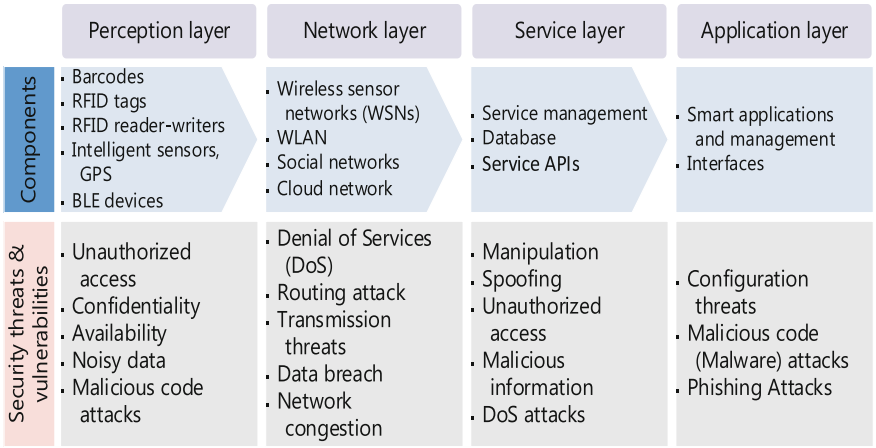

Fig. 16.2 Security threats and vulnerabilities by level

The spread of connected devices in the IoT over a vast area has created a great demand for robust security in addition to the growing demand of millions of connected devices and services worldwide (Abomhara and Kien 2015). The number and complexity of threats and attacks are increasing day by day and tools available to potential attackers are also becoming more sophisticated and effective. Therefore, in order for IoT to reach its full potential, it needs to be strictly protected against threats and vulnerabilities (Kizza 2009; Abomhara and Kien 2015).

The security threats on each layer are different due to its features. Security threats and vulnerabilities according to layers are presented below.

At the perception layer, the intelligent sensors and RFID tags automatically identify the environment and exchange data among devices. The security concerns are an important issue in perception layer. In the perception layer, the majority of the threats comes from external entities, mostly from sensors and other data collection devices. Most of these devices are commonly small in size, inexpensive, and unprotected for physical security (Suo et al. 2012; Kumar et al. 2016; Li 2017). Common threats and vulnerabilities in the perception layer can be summarized as follows:

- *Unauthorized access*: At first node, unauthorized accesses are important threats due to physical capture or logic attack.
- *Confidentiality*: Attackers can place malicious sensors or devices in order to acquire information from the system.
- *Availability*: The system component stops working because it is physically captured or logically attacked.
- *Noisy data (transmission threats)*: The data may contain incomplete information or incorrect information due to transmission over networks covering large distances.
- *Malicious code attacks*: Attackers can cause software failure through malicious code such as virus, Trojan, and junk message.

The network layer connects all things in IoT and allows them to be aware of their environment (Li 2017). The network layer is quite sensitive to attacks because of a large amount of data that it carries. The IoT connects different types of networks, which can cause network security difficulties. Therefore security protection at this level is very important to the IoT. At the network layer, common security threats and vulnerabilities are as follows (Ali et al. 2016; Kumar et al. 2016; Li 2017).

- *Denial of Services (DoS) attack*: Attackers continually bombard a targeted network with failure messages, fake requests, and/or other commands. DoS attacks are the most common threat to the network.
- *Routing attack*: These are attacks on a routing path such as altering the routing information, creating routing loops or sending error messages.
- *Transmission threats*: These are threats in transmission such as blocking, data manipulation, interrupting.
- *Data breach*: A data breach is the intentional or unintentional release of secure or confidential information to an untrusted environment.
- *Network congestion*: A large number of sensor data along with a large number of device authentication can cause network congestion.

In IoT, the service layer relies on middleware technology, which enables communication and management of data in applications and services. Service layer supports and contains the services using application programming interfaces (APIs). In this layer, the data security is crucial and more complicated in comparison to other layers (Li 2017). Some of the common security threats and vulnerabilities in service layer are:

- *Manipulation*: The information in services is manipulated by the attacker.
- *Spoofing*: The information is returned by an attacker to spoof the receiver.
- *Unauthorized access*: Abuse of services accessed by unauthorized users.
- *Malicious information*: Privacy and data security are threatened with malicious tracking.
- *DoS attacks*: A useful service resource is made unavailable by being exposed to traffic above its capacity.

The uppermost layer is the application layer that is visible to the end user. The application layer includes a variety of interfaces and applications, from simple to advanced. The security requirements in the application layer highly depend on the applications. The security threats and vulnerabilities in the application layer are summarized below (Ali et al. 2016; Kumar et al. 2016; Li 2017).

- *Configuration threats*: Failing configurations at interfaces and/or incorrect misconfiguration at remote nodes are the most important threats for this layer.
- *Malicious code (Malware) attacks*: These attacks are intentionally made directly to the software system in order to intentionally cause harm or subvert the intended function of the system.
- *Phishing Attacks*: In the interface layer, attackers may attempt to obtain sensitive information such as usernames, passwords, and credit card details.

The security requirements at all layers are confidentiality, integrity, availability, authentication, non-repudiation and privacy. These requirements are detailed in Sect. 16.6.

16.3 Industrial Challenges

Along with recent developments in IoT platforms, it is almost impossible for the industry to envisage the numerous IoT implementations, given the innovations in the technology, services and continuous needs in the industry (Tweneboah-Koduah et al. 2017). The current application areas include smart manufacturing, smart homes, and smart cities, transportation and warehousing, healthcare, retail and logistics, environmental monitoring, smart finance, and insurance. Investments in IoT solutions by Industry are shown in the Fig. 16.3 (BI Intelligence 2015). Accordingly, the manufacturing sector has an investment volume over 60 billion dollars. Transport and warehousing and information systems are the most invested sectors after the manufacturing sector (Fig. 16.3).

There are security challenges associated with all these application areas. Some of them are very obvious, for example, misuse of personal information, financial abuse. On the other hand, others are more specific depending on the structure of the industry.

With more and more enterprise connected devices being incorporated into the banking sector, the finance industry is faced with an increasing number of ever-evolving cyber security challenges (Craig 2016). Issues of highest concern in financial services industry include protecting privacy and data security, managing third-party risks and stifling compliance regulations.

Although the cyber-attacks have become widespread in the manufacturing industry, recent reports show that energy companies are more prone to these threats, which have become more advanced over the years. At least 75% of companies in

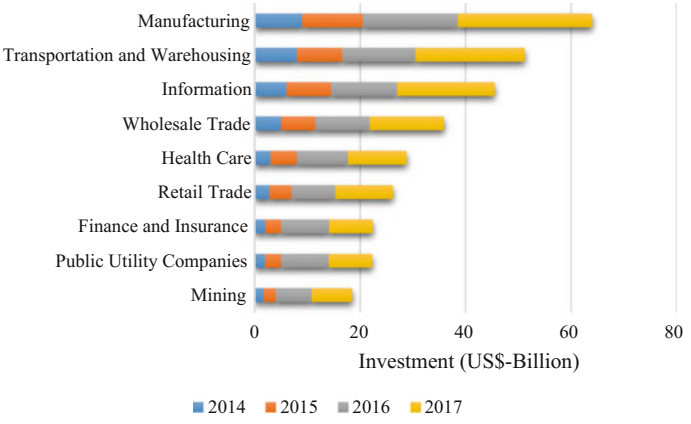

Fig. 16.3 Investments in IoT solutions by industry

the oil, gas and power sectors had one or more successful attacks in 2016. In total, more than 15% of the cyber-attacks are direct attacks on the energy sector (Frost and Sullivan 2017). Challenges of utmost concern in energy industry include protecting privacy and data security, lack of skills and awareness, the integrity of components used in the energy system and increasing interdependence among market players.

The use of IoT in healthcare applications is growing at a fast pace. Many applications such as heart rate monitor, blood pressure monitor and endoscopic capsule are currently in use (Al Ameen et al. 2012). Information security and privacy are becoming increasingly important in the healthcare sector. The storing of digital patient records, increased regulation such as Health Insurance Portability and Accountability Act (HIPAA), provider consolidation, and the increasing requirement for information between patients, providers, and payers point to the need for better information security (Appari and Johnson 2010).

In the transportation industry, rapid developments in technology and widening the connectivity of systems, networks, and devices across transport and logistics

Table 16.1 Challenges according to the industry

Finance	Protecting privacy and data security
	Managing third-party risk: Outsourcing contracts, such as cloud service agreements, impose complex data sharing regulations and generate a host of new cybersecurity challenges
	Emerging and advanced cyber threats
	Regulatory compliance
Energy	Protecting privacy and data security
	Lack of skills and awareness
	Information sharing: Many organizations do not share information about threats or cooperate externally
	Integrity of components used in energy systems
	Increased interdependence among market players
	Alignment of cyber security activities: All activities be aligned and fully integrated with national cyber security
Healthcare	Protecting privacy and data security: Healthcare organizations are required to comply with the Health Insurance Portability and Accountability Act (HIPAA), which requires healthcare vendors to ensure that the privacy of user data is not compromised in any case (Zhang and Liu 2010)
	Medical equipment issues: Healthcare organizations have specialized medical equipment that could pose particular security challenges (Korolov 2015)
	Managing third-party risk: Healthcare organizations are hesitant to move to cloud data protection to ensure that sensitive information is protected without leaving the company network (Zhang and Liu 2010)
Transportation	Protecting privacy and data security especially in the cargo industry (Xu et al. 2014)
	Emerging and advanced cyber threats (DoS attacks, Spoofing attacks) (Warren and Hutchinson 2000)

bring more opportunities in terms of cost, speed, and efficiency. As more devices and control processes are connected on internet environment, more vulnerabilities will emerge. Developing measures against these threats is at the top of the vital issues for the transport sector. Among the major problems in the transportation industry are data security and privacy and emerging and advanced cyber threats.

Some of the industry challenges facing cybersecurity experts are outlined Table 16.1 according to the industries.

16.4 Evolution of Cyber Attacks

The cyber landscape is constantly altering and evolving due to the speed of technological change, the complexity of the attackers, the value of potential targets and the effects of attacks (Weber and Studer 2016).

With the widespread use of computer networks, hackers have taken advantage of network-based services to gain personal benefit and reputation. In a threat environment where security products need to be constantly refined or updated to identify the recent exploitation, the challenge is to find a solution that provides a future-proof defense to ensure lasting network safeguard (Chemringts 2014).

Each organization has digital knowledge and many businesses maintain business transactions and trades with online systems. Most enterprises are open to cyber threats attacking from external and internal boundaries and so, your critical infrastructure needs to be protected (Sheikh 2014).

Cyber security was initially seen as a problem for the IT team, but these days it is an agenda for the entire senior executives. Cybercrime is triggered by sophisticated technologies, the use of mobility, social media, and relatively new trends in rapidly expanding connectivity—all in the hands of organized criminal networks. Under this circumstances, a smart, dynamic and evolutionary approach to cyber security is crucial to stay ahead of cybercrime and competition. Cyber security efforts require protection against a broader range of challenges. It is getting harder with new technologies, trends in mobile usage, social media, well-financed and organized enemies and 24-h attacks. Cyber risks can have a direct impact on everything from stock exchange price to brand reputation, with their more complicated structures (Deloitte 2013).

Figure 16.4 shows how cyber-attacks have evolved over the years and what industry will see in the coming years (Frost and Sullivan 2017).

At the beginning of the 1980s, general cyber-attacks began with password cracking and password guessing methods. Today, directed cyber-attacks occurs with packet spooling, advance scanning, keylogger and denial of service. In future, strategic cyber-attacks are expected to damage strategic points with bots, morphing and malicious codes. Over time, the nature of cyber-attacks has been complicated and extremely sophisticated.

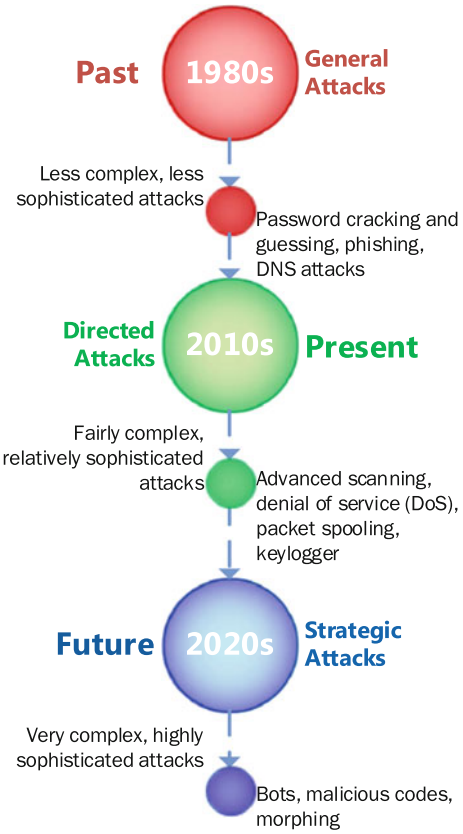

Fig. 16.4 Evolution of cyber-attacks

16.5 Cases (Cyber-Attacks and Solutions)

The cyber space is a growing community where everyone can reach each other independently of time and distance (NATO Review 2013). For this reason, some people use the cyber space for their own suspicious plans for individuals, corporations, banks, even military and government agencies. In this section, we will present some important cyber-attacks, which are large-scale cyber terrorism affecting large masses (Fig. 16.5).

– ***Flame***: Flame, also known as Skywiper and Flamer, is a modular computer malware discovered in 2012 as a virus that attacks Microsoft Windows operating system computers in the Middle East. When used by spies for espionage, it infected other systems via a local area network (LAN) or USB stick with over thousands of machines attached to others, educational institutions and government agencies. Skype conversations, keyboard activity, screenshots, and network traffic were recorded. On May 28, 2012, the virus was discovered by

Iranian National Computer Emergency Response Team (CERT), CrySys Lab and the MAHER Center of Kaspersky Lab.

- ***July 2009 Cyber Attacks***: A group of cyber-attacks took on major governments' financial websites and news agencies, both United States and South Korea, with releasing of botnet. This included captured computers that lead servers to be overloaded due to the flooding of traffic called DDoS attacks. More than 300,000 computers are hijacked from different sources.
- ***The Spamhaus Project***: Spamhaus, considered the biggest cyber-attack in history, is a filtering service used to extract spam e-mails. Thousands of Britons sent Spamhaus every day to determine whether they would accept incoming mail. Spamhaus added Cyberbunker to its blacklisted sites on March 18, 2013; Cyberbunker and other hosting companies have been tasked with recruiting home and broadband routers to hire hackers to abuse botnets to shut down the Spamhaus system.
- ***Maroochy Shire sewage spill in Australia (March 2000, Australia)***: The attacker changed the electronic data using the stolen wireless radio, the SCADA controller, and the control software, and all operations failed. It leaded to release up to one million litres of sewage into the river and coastal waters of Maroochydore in Queensland, Australia (RISI 2015).
- ***Cyber-attack on Davis-Besse power station of first energy (January 2003, The United States)***: A Slammer worm, entered a private computer network at Davis-Besse nuclear power plant in Ohio and disabled a security monitoring system for about five hours.
- ***Public tram system hacked remotely (January 2008, Poland)***: The signaling system on Lodz's tram network was manipulated by a remote control system which was designed by a 14-year old boy utilizing a TV remote control. It

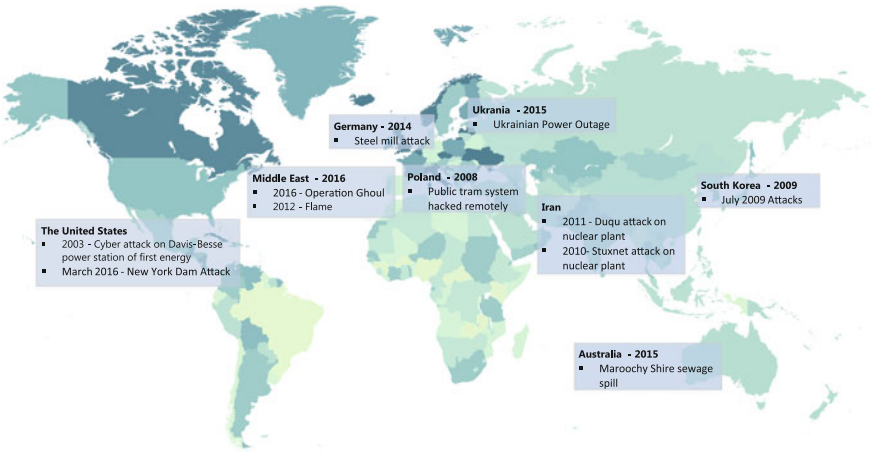

Fig. 16.5 Major industrial cyber-attacks by territories

caused the derailment of four trams and more than a dozen of passengers were injured.

- ***Stuxnet attack on Iranian nuclear plant (December 2010, Iran)***: Natanz nuclear plant in Iran was infected by Stuxnet in June 2010, this cyber worm was thought to be a joint effort of Israel and the US but no one took the responsibility of the attack. The worm destroyed 1000 nuclear centrifuges in Tehran and deeply affected the progress of the country because it went beyond just a power plant attack and infected 60,000 computers as well.
- ***Duqu attack in Iranian nuclear plant (November 2011, Iran)***: Duqu trojan hits Iran's computer systems. Experts say in a statement to Reuters that Duqu based on Stuxnet is designed to collect data that will facilitate the launch of future cyber-attacks. Stuxnet is intended to disable industrial control systems and may have destroyed some of the centrifuges Iran uses to enrich uranium.
- ***Steel mill attack (December 2014, Germany)***: The hackers attacked a steel mill in Germany. By manipulating or disrupting the control systems, it caused major damages in the foundry. Sophisticated attackers entered the steel factory's office network using spear-phishing and social engineering. The production network was reached from this network. With the actions of the attackers, control components and all production machines were cut off.

As can be seen in Fig. 16.6, the cyber-attacks on the Industrial and Commercial IT networks have shown a significant increase in both frequency and intensity over the last four years (Frost and Sullivan 2017).

Attacks targeting industrial control systems (ICS) increased 110% in November 2016 compared to last year, according to IBM management security services data. In particular, the increase in ICS traffic was related to SCADA brute force attacks using automation to guess default or weak passwords. Then attackers can remotely manipulate attached SCADA devices. The United States is the biggest target of ICS-based attacks in 2016 because this attack now has a greater ICS presence than any other country. The top 5 source and destination territories are illustrated in Figs. 16.7 and 16.8, respectively (McMillen 2016).

In the following, several important recent cyber attack cases occurred in the different parts of the world are given.

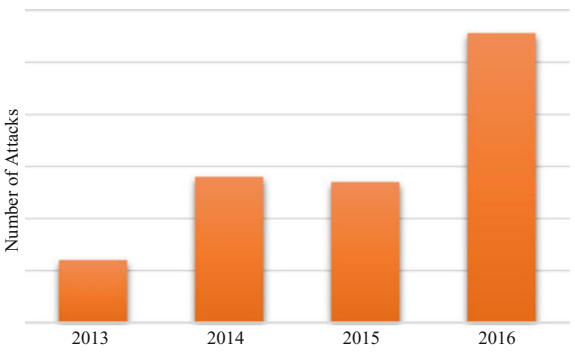

Fig. 16.6 Industrial IoT system attacks based on years

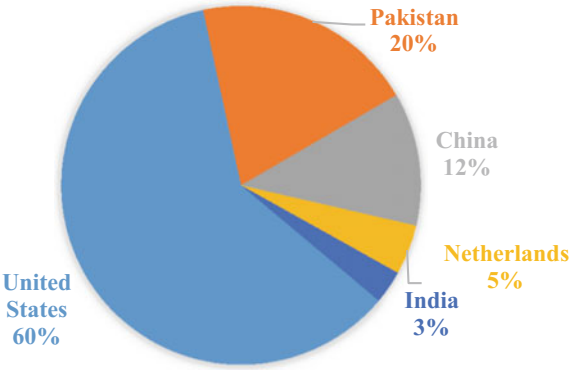

Fig. 16.7 Top 5 source countries

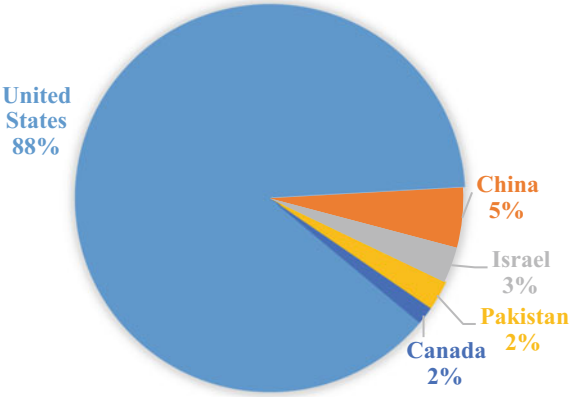

Fig. 16.8 Top 5 destination countries

- ***Operation Ghoul***: SFG malware, discovered in a European energy company network in June 2016, has created a back door for targeted industrial control systems. According to security researchers at SentinelOne Labs, the aim is to extract data from the energy network or shut down the energy network. Windows-based SFG malware is created to overcome traditional antivirus software and firewalls.
- ***New York Dam Attack***: In March 2016, computer-based control of a dam in New York was hacked by attackers using cellular modems.
- ***Ukrainian Power Outage***: In December 2015, a power company located in western Ukraine suffered a power outage that impacted a large area that included the regional capital of Ivano-Frankivsk. Three separate energy companies, known as "Oblenergos", were attacked and blocked the power of 225,000 customers. The attack was carried out by hackers using BlackEnergy malware that exploited the macros in Microsoft Excel document. The bug was planted into company's network using spam emails.

The attacks on industrial systems will continue owing to the automation and internet connection increases. This means that the number of such devastating cyber

attacks continue to rise and therefore all the damaged organizations will pay a heavy price for the attacks.

16.6 Strategic Principles of Cyber Security

The primary security principles of an efficient IoT security are addressed from six aspects. These principles must be assured for security to be guaranteed in the entire IoT system.

- **Confidentiality**: Confidentiality is the ability to hide information from people who are unauthorized to access it and thus needs protection from unauthorized access (Rodosek and Golling 2013). Confidentiality is an important security feature in IoT. In most situations and scenarios sensitive data for instance patient data, private trade data, and/or military data as well as security credentials and secret keys, must be hidden from unauthorized accesses (Abomhara and Kien 2015).
- **Integrity**: Integrity of information refers to protecting information from unauthorized, unanticipated or unintentional modification. Integrity is a mandatory security property in most cases in order to provide reliable services to IoT users. Different systems in IoT have diverse integrity needs (Abomhara and Kien 2015).
- **Availability**: Availability is the access to information whenever needed by a user of a device (or the device itself). Therefore, the IoT resources must be available on a timely basis to meet needs or to avoid significant losses.
- **Authenticity**: The authenticity property allows only authorized entities to perform certain operations in the network. Different authentication needs require different solutions. Some solutions must be strong control, for example, authentication of finance systems. On the other hand, most must be international, for example, ePassport, while others have to be local (Schneier 2011).
- **Nonrepudiation**: IoT service must provide a trusted audit trail. The property of nonrepudiation presents certain evidence in cases where the user or device cannot deny an action, for instance, payment action.
- **Privacy**: Privacy is an entity's right to determine the degree to which it will interact with its environment and to what extent the entity is willing to share personal information with others (Abomhara and Kien 2015).

16.7 Cyber Security Measures

Cyber security measures must be taken in the future to reduce cyber risks. We will explain some basic cyber security precautions/measures as much as possible to prevent all possible attacks.

- Do not allow to connect directly to a machine on the control network, on a business network or on the Internet. Organizations may not realize this connection exist, a cyber attacker can find a gap to access and exploit industrial control systems to give rise to physical damages. For this reason channels between the devices in the control system and other network devices must be removed from the center to reduce network openings (WaterISAC 2015).
- A firewall is a software program or hardware device that filters incoming and outgoing traffic between different parts of a network or between a network and the Internet. Do not allow a threat to easily reach your system by reducing the number of routes in your networks and applying security protocols to the routes. Establishing network boundaries and segments gives an organizational authority to implement both detective and protective controls on the infrastructure. The monitoring, restriction, and management of communication flows provide the practical capability for basic network traffic (especially for traffic that exceeds a network limit) and define abnormal or suspicious communication flows.
- Remote access to a network using some conservative methods like Virtual Private Network (VPN) provides big advantages to the end users. This remote access can be strengthened by reducing the number of Internet Protocol (IP) addresses that can access it by using network devices and/or firewalls to identified IP addresses.
- Role-based access control allows or denies access to network resources based on business functions. This limits the ability to access files or system parts that individual users (or attackers) should not be able to access.
- Applying strong passwords is the easiest way to strengthen your security. Hackers can use software tools that are easily accessible to try millions of character combinations to gain unauthorized access—it is called brute force attack. According to Microsoft, you should definitely avoid using personal data (such as date of birth), backwards-known words, and character or number sequences that are close together on the keyboard (BI Intelligence 2010). Create a password policy to help employees monitor best practices for security. Various technology solutions can be supported to enforce your password policy, such as scheduled password reset (Nibusiness 2017).
- Many Internet-enable devices include hard-coded default credentials. Such identity information is often freely available on the Internet and is widely known by people. Most malware targeting IoT devices is only performed by attackers using default credentials. According to Microsoft, you should definitely avoid using personal data (such as date of birth), backwards-known words, and character or number sequences that are close together on the keyboard.
- It is important to ensure awareness of vulnerability and application of required patches and updates. To protect an organization from opportunistic attacks, a system must be implemented to monitor and enforce system settings and updates. Organizations should consider updating system and software settings automatically to avoid missing critical updates.
- Your employees are responsible for helping to ensure the safety of your business. It is very important to give your employees information about safe online

habits and proactive defense and give them regular cyber security awareness and training.
- Due to the portable nature, there is a greater risk of laptop computers. It is important that you take extra steps to protect sensitive data. It is important that you take additional steps to protect sensitive data. Encrypting your laptop is the easiest way to take precautions. Encryption software changes the way information appears on the hard drive, so it cannot be read without the correct password (BI Intelligence 2010).
- Nowadays smartphones are in the center of everything, so it should be considered that they are valuable as much as company computers in case of lost or stolen. Encryption software, password protection, and application of remote wiping are very effective securing methods for smartphones to all possible attacks (BI Intelligence 2010).
- Organizational leaders generally do not know the threats and needs of cyber security. Incorporating managers into the scope of cyber security helps corporations with cyber security issues in interactions with external stakeholders (WaterISAC 2015).
- Nevertheless, administrators should not rely solely on anti-virus software to detect infections. Firewalls, intrusion detection and prevention sensors and logs from the servers should be monitored in terms of infection indication. Incident response plans are a critical but not yet sufficiently used component of emergency preparedness and flexibility. An effective cyber security measure will limit the damage, increase the trust of partners and customers, and reduce recovery costs and time (WaterISAC 2015).

16.8 Conclusion

The development of new digital industrial technology led to the emergence of Industry 4.0, the fourth wave of the industrial revolution. Industry 4.0 deals with huge data volumes, developing human-machine interactive systems and improving communication between the digital and physical environments, namely in the IoT context.

With Industry 4.0, the combination of information technology and operational technology have brought new challenges. Cyber security is the main issue that all governments in the world have made a great deal of effort against cyber security attacks. By 2020, more than 50 billion IoT devices have revealed that how important cyber security is.

In this chapter, the concept of cyber security is investigated from a comprehensive perspective, based on the context of IoT, involving many stakeholders from different sectors of the global world. The requirement of cyber security, security threats, and vulnerabilities of IoT, the evolution of cyber-attacks and cyber security

measures are discussed and supported with some graphs, figures, tables and studies in the literature.

As new platforms and operating systems for connected devices continue to evolve, security budgets are expected to grow exponentially for all organizations. The future of the cyber security strongly depends on considering threat landscapes and emerging trends in technology related to big data, cognitive computing, and IoT.

References

Abomhara M, Kien GM (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur 4:65–88

Al Ameen M, Liu J, Kwak K (2012) Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 36:93–101. doi:10.1007/s10916-010-9449-4

Ali I, Sabir S, Ullah Z (2016) Internet of things security, device authentication and access control: a review. Int J Comput Sci Inf Secur 14:456

Appari A, Johnson ME (2010) Information security and privacy in healthcare: current state of research. Int J Internet Enterp Manag 6:279. doi:10.1504/IJIEM.2010.035624

BI Intelligence (2010) 10 data-security measures. Bus. Insid. Digit

BI Intelligence (2015) The enterprise internet of things market—business insider. http://www.businessinsider.com/the-enterprise-internet-of-things-market-2015-7. Accessed 19 Jun 2017

Capgemini (2015) Securing the internet of things opportunity: putting cybersecurity at the heart of the IoT | Capgemini Worldwide

Chemringts (2014) The evolution of cyber threat and defence. UK

Columbus L (2016) Roundup of internet of things forecasts and market estimates In: Forbes. https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#7eba4b9a292d. Accessed 20 Jun 2017

Craig D (2016) Five cybersecurity challenges facing financial services organizations today. IBM Secur Intell

Da Xu L, He W, Li S (2014) Internet of things in industries: a survey. IEEE Trans Ind Inform 10:2233–2243. doi:10.1109/TII.2014.2300753

Deloitte (2013) Risk angles—five questions on the evolution of cyber security. United Kingdom

Frost and Sullivan (2017) Cyber Security in the Era of Industrial IoT. Frost & Sullivan White Paper, Germany

Kaplan J, Weinberg A, Sharma S (2011) Meeting the cybersecurity challenge. Digit. McKinsey

Kizza JM (2009) Guide to computer network security. Springer, Berlin

Korolov M (2015) Healthcare organizations face unique security challenges | CSO Online. CSO

Kumar SA, Vealey T, Srivastava H (2016) Security in internet of things: challenges, solutions and future directions. In: 2016 49th Hawaii international conference on system sciences (HICSS). IEEE, pp 5772–5781

Li S (2017) Security requirements in IoT architecture. In: Securing the internet of things, pp 97–108

McMillen D (2016) Attacks targeting industrial control systems (ICS) up 110 percent. IBM

NATO Review (2013) The history of cyber attacks—a timeline. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm. Accessed 20 Jun 2017

Nibusiness (2017) Common cyber security measures. In: nibusinessinfo.co.uk. https://www.nibusinessinfo.co.uk/content/common-cyber-security-measures. Accessed 20 Jun 2017

RISI (2015) RISI—the repository of industrial security incidents. http://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill. Accessed 20 Jun 2017

Rodosek GD, Golling M (2013) Cyber security: challenges and application areas. Springer, Berlin, pp 179–197
Rüßmann M, Lorenz M, Gerbert P et al (2015) Industry 4.0: the future of productivity and growth in manufacturing industries
Sathish Kumar J, Patel DR (2014) A survey on internet of things: security and privacy issues. Int J Comput Appl 90:20–26. doi:10.5120/15764-4454
Schneier B (2011) Secrets and lies : digital security in a networked world. Wiley, Hoboken
Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng 2017:1–25. doi:10.1155/2017/9324035
Sheikh S (2014) Evolving cyber security—a wake up call… In: Marsh National Oil Conference. Dubai
Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. In: 2012 international conference on computer science and electronics engineering. IEEE, pp 648–651
Taneja M (2013) An analytics framework to detect compromised IoT devices using mobility behavior. In: 2013 international conference on ICT convergence (ICTC). IEEE, pp 38–43
Tweneboah-Koduah S, Skouby KE, Tadayoni R (2017) Cyber security threats to IoT applications and service domains. Wirel Pers Commun 1–17. doi:10.1007/s11277-017-4434-6
Warren M, Hutchinson W (2000) Cyber attacks against supply chain management systems: a short note. Int J Phys Distrib Logist Manag 30:710–716. doi:10.1108/09600030010346521
WaterISAC (2015) 10 Basic cybersecurity measures—best practices to reduce exploitable weaknesses and attacks
Weber RH, Studer E (2016) Cybersecurity in the internet of things: legal aspects. Comput Law Secur Rev 32:715–728. doi:10.1016/j.clsr.2016.07.002
Wendt H, Renn J (2012) Knowledge and science in current discussions of globalization. In: The globalization of knowledge in history. Edition Open Access
Yang D-L, Liu F, Liang Y-D (2010) A survey of the internet of things. In: Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010). Atlantis Press
Zhang R, Liu L (2010) Security models and requirements for healthcare application clouds. In: 2010 IEEE 3rd international conference on cloud computing. IEEE, pp 268–275