Cybersecurity of Industrial Systems—A 2023 Report

Janusz Pochmara and Aleksandra Świętlicka *

Abstract: The article explores the importance of cybersecurity in Industry 4.0, specifically focusing on safeguarding industrial automation systems from cyberattacks. It discusses essential security measures, network monitoring, and employee training, emphasizing the significance of risk management for ensuring industry stability. Adherence to industrial security standards, such as ISA/IEC 62443, is crucial (ISA—International Society of Automation, IEC—International Electrotechnical Commission). The article outlines cyberthreat challenges and their impact on various sectors, including healthcare and finance, as well as the risks faced by large industrial enterprises. Additionally, it elucidates evolving cybersecurity strategies and principles, underscoring the necessity for continuous, multi-layered protection. Collaboration with operators, strict information security policies, and robust incident response plans are emphasized. The importance of risk monitoring and adaptability to ever-changing threat landscapes is highlighted, emphasizing the collaborative and flexible nature of cybersecurity in the face of escalating digital threats.

Keywords: access control; monitoring; cybersecurity chain; network security; end-user security

1. Introduction

Currently, the primary goal of Industry 4.0 is to implement protective procedures to secure industrial automation systems from cyberattacks. This involves implementing security measures, monitoring network traffic, segmenting networks, providing regular cybersecurity training for employees, and maintaining contingency plans to respond quickly to incidents. Preventing attacks and proper risk management are crucial for maintaining stability and security in the industry.

To protect industrial automation systems from cyberattacks, it is necessary to implement appropriate security measures. This includes, among other things, network security, regular software updates, monitoring network traffic, access authorization, and cybersecurity training for staff. It is also important to strictly adhere to industrial security standards, such as the ISA/IEC 62443 standards [1].

The ISA/IEC 62443 standards are a series of international standards and technical reports developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) for industrial automation and control systems (IACS) security [1]. These actions help minimize the risk of attacks and enhance the resilience of industrial automation systems against cyberthreats.

A cyberattack on industrial automation systems is an attack aimed at disrupting or disabling the operation of industrial control systems, such as SCADA (Supervisory Control and Data Acquisition) systems or industrial control systems. Such attacks can have serious consequences, including production failures, data loss, and even threats to the safety of people and the environment.

To write this report we have incorporated statistics from online news sources and official reports to capture real-time developments and industry insights. By including information from these sources, you can provide a more holistic view of cybersecurity trends, encompassing both academic discourse and practical applications in industry.
This multi-faceted approach ensures that your research reflects the dynamic nature of cybersecurity and its evolving landscape within the Industry 4.0 paradigm.

Furthermore, our research method combines several sources of data to analyze current trends in cybersecurity within the context of Industry 4.0. We have utilized Google Trends to gather statistics on the popularity of relevant search queries, providing insights into the public interest and awareness regarding cybersecurity topics. Additionally, we aggregated data from scholarly databases such as Web of Science, MDPI, Scopus, and IEEE Xplore to quantify the volume of articles published on cybersecurity and its intersection with Industry 4.0. This approach allows for a comprehensive examination of academic research output in the field.

The article is organized as follows. In Section 2, the importance of cybersecurity in Industry 4.0 is described, outlining six key categories: access control, encryption, monitoring and threat detection, risk management, physical security, and employee training. Section 3 underscores the pivotal role of artificial intelligence (AI) in transforming the cybersecurity landscape, emphasizing its capabilities in advanced threat detection, predictive analysis, real-time response, behavioral analytics, user authentication, and automated incident response, highlighting the strategic necessity of integrating AI for robust and adaptive defenses against evolving cyberthreats. Section 4 discusses the impact of Industry 4.0 on manufacturing, integrating technologies like Internet of Things (IoT) and Artificial Intelligence (AI) for enhanced efficiency, and highlights escalating cybersecurity concerns, emphasizing the need for robust measures due to increased connectivity, potential data breaches, and threats to critical infrastructure, with recommendations including AI and ML integration for protection against cyberattacks. Section 5 discusses common types of cyberattacks on industries, including phishing, malware, ransomware, and denial-of-service attacks. It highlights the top targeted industries in 2022, such as healthcare and financial services, and provides specific examples of cyberattacks on companies and organizations, emphasizing the global impact of these incidents. Section 6 underscores the importance of adapting strategies as the digital threat landscape evolves to protect data and ensure operational stability for organizations. Finally, conclusions are provided in Section 8. Additionally, in Figure 1 there is a diagram that presents the article’s structure.

![Diagram of the article’s structure](image-url)
2. Materials & Methods

2.1. Definition of Cybersecurity

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring confidentiality, integrity, and availability of information [2]. It seems that everything, including communication, now relies on computers and the internet [3,4]. It is best to present it in six categories:

1. Access control: access control to data and systems is a critical component of cybersecurity. This means that only authorized individuals or systems have access to protected resources. This can be achieved through the use of strong passwords, two-factor authentication, digital certificates, and more.

2. Encryption: data encryption is important when storing, processing, and transmitting data. Encryption involves transforming data in a way that is readable only to authorized users. Examples include disk encryption and communication encryption using HTTPS or VPN protocols.

3. Monitoring and threat detection: Monitoring and threat detection systems (such as antivirus programs and intrusion detection systems) are essential for identifying potential attacks on data and systems. They enable real-time responses to threats.

4. Risk management: risk management involves the identification, assessment, and management of potential threats and taking actions to reduce risk. This is a process that is an integral part of cybersecurity strategy.

5. Physical security: protecting digital data often requires physical security measures, such as access control to server rooms, CCTV monitoring systems, or protection against hardware theft.

6. Employee training and awareness: often, the biggest threat to data security comes from people. Therefore, it is important to train employees in cybersecurity and raise their awareness of potential threats, such as phishing or social engineering.

Protecting digital data requires a holistic approach that takes into account all these elements. Ensuring data security in the three main contexts—storage, processing, and transmission—is crucial for effective cybersecurity.

Stored data are tackled by information security elements. Processed data are tackled by application security and operational security elements. Transmitted data are processed by network security.

Network security aims to protect the data transmitted among all devices on a computer network. In Figure 2, we present elements of cybersecurity in the industry process. The increase in the number of attacks and threats in cyberspace has underscored the need for providing information security services (cybersecurity) in both the public and private sectors. The growth of cyberthreats has led to an increasing demand for services that help protect computer systems, data, and infrastructure from cyberattacks. Both the public and private sectors must invest in cybersecurity solutions to safeguard their assets and ensure protection against potential cyber incidents or security breaches.

![Elements of Cybersecurity](image)

*Figure 2. Elements of cybersecurity.*

2.2. Cybersecurity Chain

Cybersecurity consists of six key elements that protect digital data [5], which exists in three main manners: stored, processed, or transmitted (see Figure 2). Therefore, a
separate element handles each manner. Stored data are tackled by information security elements. Processed data are tackled by application security and operational security elements. Transmitted data are processed by network security.

2.3. Network Security

This level of protection introduces procedures to prevent unauthorized access to individuals’ data from outside the industrial process. This includes authenticating each user [5]. Subsequently, network firewalls verify the rules and allow services for that user [6]. Finally, antivirus programs examine the content of installed programs to detect malicious software. The primary goal is to protect data transmitted between access points.

2.4. Application Security

Application security is the process of developing, adding, and testing security features in applications to prevent security gaps from threats such as unauthorized access and modifications. It works at each phase of the software development life cycle [7].

2.5. Information Security

At this level, information and documentation, and product-related data (industrial process), as well as employee and customer data are protected. Organizational structure and solutions used for the process execution purposes are employed.

2.6. Operational Security

At this stage, information and documentation, and product-related data (industrial process), as well as employee and customer data are protected. Organizational structure and solutions used for the process execution purposes are employed [8].

2.7. Disaster Security

Data and information can be stored as copies locally or with an external provider. When data are lost, there is a possibility to restore backup copies, which are recovered without affecting the system’s operation. Maintaining data with an external operator provides additional security guarantees. This is a natural form of what is known as a backup.

2.8. End-User Security

End-user security involves imparting knowledge about cybersecurity and its components to the users. It is crucial for users to understand what occurs in their cyberspace. End users should be able to recognize attacks, avoid threats, and report incidents as quickly as possible [6]. Most attacks, particularly those involving unauthorized access, are carried out using social techniques, where it appears that humans are the weakest link.

3. AI in Cybersecurity

The rapid development of technology in industry has brought transformational changes in various sectors, and artificial intelligence (AI) has become a key factor in transforming the cybersecurity area. AI has become a milestone of modern cybersecurity strategies, offering a range of capabilities that significantly improve the detection, prevention, and response to cyberthreats.

The integration of AI into cybersecurity is driven by several compelling reasons, each of which contributes to more robust and adaptive defenses against the cyberattacks. The integration of artificial intelligence in cybersecurity is not just a technological trend, but a strategic necessity. As cyberthreats become more sophisticated, AI offers a multilevel approach to detecting threats. One of the main motivations for using AI for cybersecurity is its unrivaled ability to perform advanced threat detection. Traditional security measures often rely on static rules and rules, trying to keep up with the dynamic and evolving tactics of cybercriminals.
Artificial intelligence is crucial for quickly analyzing big data sets and identifying patterns that indicate potential threats [9]. Incorporating machine learning as a subset of artificial intelligence increases operational efficiency. This chain is adopted for analyzing big data sets to identify disturbing patterns that may indicate cyberthreats.

The main idea of AI is based on the structure of a neuron, and its functionality is similar to a human neuron. By using some of its behaviors, tools are obtained that have applications in many engineering fields, including cybersecurity. Here it is only indicated that AI consists of neural networks and machine learning (ML).

Neural networks (NN) belong to the family of machine learning algorithms, and draw inspiration from the functioning of neurons in the human brain. They are based on the assumption that, with given parameters, there is a way to connect them to achieve a specific outcome. Data pass through various layers, where a series of learning rules are applied, until they reach the final layer, where the results are compared to the ‘correct’ ones, and the parameters are adjusted based on the ‘weight’ function included in each rule. Once the network learns, it can establish its ‘weights’ and operate in memory or execution mode [9].

Machine learning is a branch of computer science and artificial intelligence (AI) that uses data and algorithms to teach and improve models through experience, sometimes inspired by the way humans naturally learn and infer [10].

3.1. Advanced Threat Detection

One of the main purposes of using artificial intelligence for cybersecurity is for advanced threat detection. Traditional security is often based on static rules and signatures, trying to keep up with the dynamic and evolving tactics of cybercriminals. Artificial intelligence is crucial for quickly analyzing massive data sets and identifying patterns that indicate potential security breaches [11]. Machine learning algorithms, a subset of artificial intelligence, are adept at analyzing massive data sets to identify disturbing patterns that may indicate cyberthreats. This enables you to detect and respond to threats.

3.2. Predictive Analysis and Risk Assessment

AI works based on data and current trends to forecast potential future threats. By analyzing patterns and identifying vulnerabilities, AI helps by actively respond to security threats before they appear in actual attacks. This predictive analytics plays a main role in setting security measures, allocating resources efficiently and creating more resilient cybersecurity.

3.3. Real-Time Analysis and Response

The dynamic nature of cyberthreats requires the ability to analyze and respond in real time. Artificial intelligence enables real-time analysis of large data sets, providing the ability to identify and respond to security events in seconds [12]. AI systems can analyze network traffic, user behavior, and system operations in real time. This allows the identification of potential security incidents as they occur, making it easier to respond immediately to mitigate the impact of an attack. Behavioral responses by AI algorithms can isolate affected systems, contain threats, and initiate predefined countermeasures without the need for human intervention. This rapid response ability is crucial in preventing many cyberthreats.

3.4. Behavioral Analytics and User Authentication

Behavioral analysis plays a main role in detecting unusual user behavior patterns. By establishing baseline behavior of users and systems, AI can identify deviations that may indicate insider threats or unauthorized access. This ability is essential for recognizing subtle, non-traditional attacks that may be missed by rule-based systems. By continuous learning from user behavior, the potential of AI increases the ability to detect anomalies that may indicate a security threat, contributing to a more comprehensive and adaptive cybersecurity defense [13].
3.5. Automatic Response to Suddenly Incidents

AI automated incident responses can analyze the nature of an attack, identify affected systems, and take predetermined actions to contain and mitigate the threat. Automated responses not only speed up response times, but also allow cybersecurity teams to focus on the more complex and strategic aspects of incident handling. Finding the right balance between automation and human intervention is essential to use the effectiveness of AI while ensuring differentiated decision making and an understanding of the broader context of a security incident [14].

4. Cybersecurity in Industry 4.0

The advent of Industry 4.0 has ushered in a new era of smart manufacturing, integrating digital technologies, data analytics, and automation to revolutionize industrial processes. However, with this increased connectivity and digitization comes a growing concern for cybersecurity.

Industry 4.0, often referred to as the Fourth Industrial Revolution, represents a paradigm shift in manufacturing. It leverages technologies such as the IoT, AI, big data analytics, and cloud computing to create interconnected, intelligent, and autonomous systems. These advancements aim to enhance efficiency, flexibility, and customization in manufacturing processes.

4.1. A Main Component of Industry 4.0

Companies are integrating new technologies, including IoT, cloud computing and analytics, and AI and machine learning into their production facilities and throughout their operations. These smart factories are equipped with advanced sensors, embedded software, and robotics that collect and analyze data and allow for better decision making. Even higher value is created when data from production operations are combined with operational data from ERP (Enterprise Resource Planning), supply chains, customer service, and other enterprise systems to create whole new levels of visibility and insight from previously siloed information [15].

Smart manufacturing is a core element of Industry 4.0, emphasizing the use of real-time data and advanced technologies to optimize the manufacturing lifecycle. It involves the integration of sensors, actuators, and smart devices, enabling machines to communicate and make decisions collaboratively. This interconnectedness enhances operational efficiency and enables predictive maintenance, reducing downtime and minimizing user resources.

The problem of Industry 4.0 is that processes are dispersed over a wide area and in such situations it is easy to attack devices from outside.

4.2. The Role of Cybersecurity in Industry 4.0

As manufacturing systems become increasingly connected and reliant on digital technologies, the vulnerability to cyberthreats also rises. Cybersecurity in Industry 4.0 is essential to safeguard critical infrastructure, sensitive data, and intellectual property. Threats such as ransomware, data breaches, and sabotage pose significant risks to smart manufacturing systems, potentially causing financial losses and operational distortion.

The main threats related to cybersecurity in Industry 4.0 based on ideas can be presented as [16–20]:

- Increased attack area: the wide range of connected devices and sensors expands the attack area for cyber adversaries, providing more entry points for unauthorized access.
- Data integrity: according to the MHRA, this is a process that is responsible for the completeness, correctness, and reliability of generated data throughout their entire data life cycle (DLC). The DLC begins with the initial generation and recording of data, through their processing, use, storage, archiving, and destruction. So-called data integrity also ensures that data are not intentionally or accidentally modified, falsified, distorted, deleted, or altered in an unauthorized manner. This applies to both data saved in electronic format as well as data in paper form.
• Legacy system risks: many companies’ facilities still operate with legacy systems
  that may lack modern security features. Integrating these systems into Industry 4.0
  requires accurate consideration of cybersecurity.

• Supply in communication chain: interconnected supply chains in smart manufacturing
  introduce new vulnerabilities. Cybersecurity must extend beyond individual factories
  to encompass the entire supply network.

Industry 4.0 offers immense opportunities for innovation and efficiency in manufac-
turing, but these benefits come with the responsibility to address cybersecurity challenges.
Implementing robust cybersecurity measures is essential to protect smart manufacturing
systems from evolving cyberthreats.

The dynamic development of Industry 4.0 makes the concept of cybersecurity crucial
when building and securing systems. It is difficult to predict and find gaps at the moment.
Intelligent systems need to be developed to help diagnose locations where access from
outside is a possibility. Therefore, the use of AI and ML is suggested for use in Industry 4.0
as a recommendation to protect against cyberattacks.

5. Results—Cybersecurity Statistics by Industry

There are several different types of cyberattacks on industries. Here are some of the
most common [5,21]:

1. Phishing: involves sending a fraudulent message in an attempt to make the recipient
  provide sensitive information, such as password credentials.
2. Malware: involves using viruses, spyware, or other malicious software to steal information.
3. Ransomware: where data are stolen and only released upon payment of a ransom.
   However, these data typically become available on the dark web regardless of payment.
4. DoS (denial of service)/DDoS (distributed denial of service) attacks deny access to
   systems, making businesses inoperable.

Tech Business News reports that the top five most targeted industries in 2022 were
as follows:

2. Financial services.
3. Retail.
4. Education.
5. Energy and utilities.

We can categorize cyberattacks’ geographical spread into different categories based on
the extent of their reach:

1. NEAR: near cyberattacks are localized to a specific geographic area or region. These at-
   tacks typically target organizations, institutions, or individuals within close proximity
   to the attacker’s location. Examples of near cyberattacks include those targeting local
   businesses, government agencies, or educational institutions within a city or town.
2. GLOBAL: global cyberattacks have a widespread impact and can affect organizations,
   businesses, or individuals worldwide. These attacks often exploit vulnerabilities in
   global networks or systems, such as the internet, cloud infrastructure, or international
   financial networks. Global cyber threats, such as large-scale malware outbreaks or
   ransomware attacks, can disrupt global commerce, compromise sensitive information,
   and affect individuals across different continents.
3. FAR: far cyberattacks target regions or countries that are geographically distant
   from the attacker’s location. These attacks may be motivated by geopolitical factors,
   economic interests, or ideological agendas. Far cyberattacks can have significant
   implications for international relations, diplomacy, and security, as they may involve
   state-sponsored actors or cybercriminal groups operating across borders.
4. MID: mid-range cyberattacks have a moderate geographic spread, impacting mul-
   tiple organizations or entities within a specific region or group of countries. These
   attacks may target industries or sectors with interconnected supply chains or shared
infrastructure, such as transportation, energy, or healthcare. Mid-range cyber threats can disrupt regional economies, critical infrastructure, and public services, requiring coordinated responses from affected entities and government agencies.

5. REGIONAL: regional cyberattacks target specific geographic regions or blocs of countries with shared economic, political, or cultural ties. These attacks may exploit vulnerabilities in regional networks, infrastructure, or industries, impacting multiple countries within a defined geographic area.

6. CROSS-BORDER: cross-border cyberattacks occur when threat actors operate across national borders to target organizations, institutions, or individuals in different countries. These attacks may involve coordinated efforts by cybercriminal groups, state-sponsored actors, or hacktivist organizations to exploit weaknesses in international networks or systems.

7. INTERCONTINENTAL: cyberattacks have a transcontinental impact, affecting organizations, businesses, or individuals across multiple continents. These attacks often exploit vulnerabilities in global communication networks, financial systems, or critical infrastructure, requiring international cooperation and coordination to address effectively.

8. TRANSACTIONAL: transnational cyberattacks transcend traditional geopolitical boundaries and may target entities across different regions, countries, or jurisdictions. These attacks may be motivated by financial gain, political objectives, or ideological beliefs, posing challenges for law enforcement, intelligence agencies, and cybersecurity professionals in tracking and mitigating threats across borders.

9. REMOTE: remote cyberattacks originate from locations that are physically distant from the target organization or individual. These attacks may leverage remote access tools, malware, or phishing techniques to infiltrate networks or compromise systems without direct physical proximity to the target. Remote attacks can be challenging to detect and mitigate, as they may exploit weaknesses in network defenses or human vulnerabilities from a distance.

10. DISTRIBUTED: distributed cyberattacks involve distributed or decentralized networks of compromised devices, often referred to as botnets, to launch coordinated attacks against targets. These attacks may involve thousands or even millions of infected devices located in different geographic locations, amplifying their impact and making them difficult to mitigate through traditional means.

These categories provide a comprehensive framework for understanding the geographic scope and nature of cyber threats, highlighting the diverse range of cyberattack scenarios encountered in today’s interconnected world.

Additionally, the work of large industrial enterprises is beginning to be sabotaged. Companies are often targeted by hackers who want to steal their intellectual property, such as product designs and blueprints [5].

In Tables 1 and 2, we present reports from [5]. These data clearly demonstrate that cyberattacks, including ransomware attacks and data breaches, are no longer confined solely to the internet. Organizations operating in critical infrastructure sectors are particularly vulnerable to such attacks. This underscores that cyber threats can have significant real-world consequences, including on public services, energy, transportation, and other key sectors. Therefore, protection against cyberattacks has become an extremely important component of the actions taken by organizations and governments worldwide.
Table 1. Attacks on internet, infrastructure, and telecommunication providers 2022 [5].

<table>
<thead>
<tr>
<th>Time</th>
<th>Geographical Spread</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2022</td>
<td>NEAR</td>
<td>The Port of London Authority was hit by a DDoS that took its website offline for 24 h. The attack was launched by Pro-Iran Group Altahrea [22].</td>
</tr>
<tr>
<td>May 2022</td>
<td>NEAR</td>
<td>Italian websites of the Senate, the Ministry of Defence, and the National Health Institute were targeted by a DDoS attack launched by Russian hackers with the intent of targeting NATO countries [23].</td>
</tr>
<tr>
<td>March 2022</td>
<td>FAR</td>
<td>The Israeli ISP Cellcom was the target of a large-scale DDoS attack, which resulted in government resources, that is, ministry websites, being offline for a while.</td>
</tr>
<tr>
<td>January 2022</td>
<td>MID</td>
<td>Andorra Telecom was hit by a DDoS attack that temporarily stopped communications in the country [24]. According to the media, the targets were the participants in the Twitch Rivals Squidcraft Games, a Minecraft tournament based on Squid Game. There are suspicions that the target was not the Andorra government and its citizens (they were just collateral damage) but rather some Andorra streamers who were unable to continue the game to win the top prize of $100,000.</td>
</tr>
</tbody>
</table>

Table 2. Notable ransomware incidents in 2021/2022 in big companies [5].

<table>
<thead>
<tr>
<th>Time</th>
<th>Geographical Spread</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2021</td>
<td>NEAR</td>
<td>Media Markt, a German electronic retailer, was hit by Hive ransomware, impacting 49 stores in the Netherlands. The infection caused impacts on retrieving orders and returns in the store. Interestingly, a Dutch reporter received insight into the communication between Hive and the company, revealing they had not paid the ransom [25].</td>
</tr>
<tr>
<td>December 2021</td>
<td>NEAR</td>
<td>French IT services company Inetum Group [26] suffered a ransomware attack. Although unconfirmed, the attack is attributed to ALPHV. Official statements mention only a limited impact on the business and its customers. This attack follows the BGH trend, with large corporations being targeted, as impact could cause a tickle-down effect on its customers.</td>
</tr>
<tr>
<td>December 2021</td>
<td>NEAR</td>
<td>Nordic Choice Hotels was impacted by Conti ransomware. The incident impacted the hotel’s guest reservation and room key card systems [27]. Guests reported their key cards to be out of service.</td>
</tr>
<tr>
<td>January 2022</td>
<td>NEAR</td>
<td>Ministry of Justice in France: threat actors who are using ransomware LockBit 2.0 have posted a message on their Tor-based leak website claiming to have stolen files from the Ministry of Justice’s systems [28]. February 2022 MID Swissport, an airport management services company: the BlackCat ransomware group, aka ALPHV, claimed responsibility for the recent cyberattack on Swissport that caused flight delays and service disruptions [29].</td>
</tr>
<tr>
<td>February 2022</td>
<td>GLOBAL</td>
<td>Nvidia Corp (Lapsus$ ransomware gang): ‘Lapsus$’ took responsibility for the breach on its Telegram channel and claims to have stolen 1 terabyte of information, including ‘highly confidential/secret data’ and proprietary source code [30].</td>
</tr>
<tr>
<td>March 2022</td>
<td>FAR</td>
<td>Toyota Motor suspended operations in 28 production lines across 14 plants in Japan for at least a day after a key supply chain player was hit by a suspected cyberattack. The incident affected Toyota’s plastic parts and electronic components supplier Kojima Industries on February 24. The firm said it discovered a malware infection and a ‘threatening message’ on rebooting after a file error on its server. The nature of events suggests that Kojima Industries was likely a victim of a ransomware attack.</td>
</tr>
</tbody>
</table>

We must also take into consideration that the number of connected devices is expected to grow rapidly over the next several years. Cybersecurity experts expect IoT infections to grow as well. Furthermore, the deployment of 5G networks, which will further fuel the use of connected devices, may also lead to an uptick in attacks [1].

In Table 3, the industries most exposed to attacks at the moment are presented, according to [31]. The results of these types of attacks are expected to produce losses totaling about USD 538.3 trillion by 2030. This is due to the rising investments in the cybersecurity infrastructure worldwide, led by increasing awareness of cyberthreats [31].
Table 3. Distribution of cyber attacks in different industries worldwide [31].

<table>
<thead>
<tr>
<th>Industry</th>
<th>Share of Cyberattacks Recorded in the Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>24%</td>
</tr>
<tr>
<td>Finance and insurance</td>
<td>18.9%</td>
</tr>
<tr>
<td>Professional, business, and consumer services</td>
<td>14.6%</td>
</tr>
<tr>
<td>Energy</td>
<td>10.7%</td>
</tr>
<tr>
<td>Retail and wholesale</td>
<td>8.7%</td>
</tr>
<tr>
<td>Education</td>
<td>7.3%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5.8%</td>
</tr>
<tr>
<td>Government</td>
<td>4.8%</td>
</tr>
<tr>
<td>Transportation</td>
<td>3.9%</td>
</tr>
<tr>
<td>Media and telecom</td>
<td>0.5%</td>
</tr>
</tbody>
</table>

In Figure 3, we can observe the distribution of articles across various subjects retrieved from different bibliography search engines, while Figure 4 shows their percentage share in each category. For Material Sciences, Web Of Science returned 12 articles, while MDPI yielded 44, IEEEXplore 6, and Scopus 3. For Chemical Engineering, there were 2 articles from Web Of Science, 29 from MDPI, 5 from IEEEXplore, and 2 from Scopus. For Environmental Sciences, 2 articles were retrieved from Web Of Science, 59 from MDPI, 13 from IEEEXplore, and 1 from Scopus. For Psychology, there were no articles from Web Of Science, 382 from MDPI, and 2 from Scopus. Energy-related articles were plentiful, with 48 from Web Of Science, 2043 from MDPI, 52 from IEEEXplore, and 55 from Scopus. Social Sciences yielded 6 articles from Web Of Science, 263 from MDPI, 13 from IEEEXplore, and 6 from Scopus. For Decision Sciences, 7 articles were retrieved from Web Of Science, 43 from MDPI, and 8 from Scopus. Engineering subjects were well-covered, with 221 articles from Web Of Science, 2697 from MDPI, 261 from IEEEXplore, and 87 from Scopus. Lastly, Computer Science articles were abundant, with 128 from Web Of Science, 1233 from MDPI, 104 from IEEEXplore, and 11 from Scopus.

Figure 3. Number of articles in different areas of cybersecurity published in search engines: Web of Science, MDPI, IEEEXplore, and Scopus.
Based on Figure 5, it appears that interest in cybersecurity in the context of Industry 4.0 experienced a notable increase starting around 2009, with a peak in 2022. The interest remained relatively low from 2004 to 2008, gradually increasing in 2009, and then fluctuating in the subsequent years. There are intermittent spikes in interest, such as in 2012, 2015, 2016, 2018, and 2019, but the most significant peak occurs in 2022, indicating a heightened focus on cybersecurity within the Industry 4.0 landscape during that period. However, it is worth noting that there was a notable decrease in interest in 2023 compared with the previous year, suggesting potential fluctuations in attention to cybersecurity trends within Industry 4.0. The numbers on the chart represent individual interests in searches relative to the highest point on the chart. A value of 100 indicates the highest popularity of the term. A value of 50 means that the popularity of the term is half as much. A value of 0 indicates that there are not enough data available for the given term.
6. How to Protect Against Cybercrime

Cybersecurity is not a one-time process or a single solution but a continuous and multi-layered strategy. Digital threats are diverse and constantly evolving, which is why protection against them requires a comprehensive approach. Several key principles of cybersecurity include:

1. Increased investment in protection: organizations must boost their investments in solutions and technologies that safeguard against cyberattacks. This includes the procurement and implementation of advanced threat detection and response tools, as well as continuous security system updates.
2. Enhanced employee awareness: employees often serve as the first line of defense against cyberthreats. Organizations need to invest in employee education regarding cybersecurity to help them recognize and avoid potential threats, such as phishing and social engineering.
3. Strict information security policy: the implementation and enforcement of a rigorous information security policy are crucial. These encompass creating strong passwords, restricting access to critical resources, monitoring user activities, and various other security practices.
4. Rapid incident response: organizations must be prepared for an immediate response to cybersecurity incidents. This involves establishing action plans for security breaches and training teams responsible for incident management.
5. Infrastructure updates and monitoring: regular software and firmware updates for devices, along with continuous network and system monitoring, aid in detecting and mitigating potential threats.
6. Collaboration with suppliers: organizations should collaborate with software and service providers to ensure that the solutions they employ are protected against vulnerabilities and threats.
7. Access controls: implementing stringent access controls for systems and data, along with the use of two-factor authentication, helps reduce the risk of unauthorized access.
8. Network traffic controls: monitoring network traffic and applying traffic control policies assist in detecting anomalies and limiting access to potentially dangerous sources.
9. Robust recovery procedures: developing and testing recovery plans for incidents, including creating backups and restoring systems, is vital for minimizing losses and operational disruptions.
10. Risk monitoring and assessment: regularly evaluating cybersecurity risks enables organizations to adapt their security strategies to the evolving threat landscape.

Protecting digital data requires an approach that includes all these elements. Ensuring data security in the three main contexts—storage, processing, and transmission—is crucial for effective cybersecurity.

In the face of escalating cyberthreats, cybersecurity becomes a priority for every organization. Actions and investments in this area are essential to protect data and ensure operational stability.

7. Tuning Neural Network Parameters

The use of neural networks to combat cyberattacks encompasses various approaches and techniques. Below, we present concepts and patterns that can be applied in this context:
Training data collection:
- Specify the purpose of the classification, i.e., what we would like to predict using the SVM model.
- Specify the classes we want to distinguish.
- Identify the categories (classes) we want to predict.

Data preprocessing:
Initially, the data undergo noise removal, normalization, and feature engineering. This procedure aims to facilitate the optimal functioning of neural networks and the SVM algorithm.

Class mapping involves assigning unique numerical identifiers (class labels) to the categories or groups that our model needs to learn to recognize attacks. This process is crucial for data preparation in classification tasks where the primary goal is to assign objects to specific classes.

It is best to use binary notation for this purpose, which will be further processed by neural networks. For instance, the “Positive” class can be marked as 1 and the “Negative” class as 0. We present three classes of events described as Class A: \([1, 0, 0]\), Class B: \([0, 1, 0]\), and Class C: \([0, 0, 1]\).

SVM for feature extraction:
Traditionally, the support vector machine (SVM) is used as a classification algorithm, but there is an approach to using it for feature extraction:
- Training an SVM model on selected data to obtain a hyperplane that separates different classes.
- During the practical process, the SVM evaluates the weight vector, \(w\), and scalar shifts, \(b\).

Feature extraction:
Each example of data, \(x\), can be transformed into a feature vector, \(f\), using the formula:

\[
f(x) = w \cdot x + b
\]  

We obtain a feature vector that can be used as a new representation of the data. The function \(f(x)\) can be understood as the function constructed by the SVM model to assign examples to classes. If \(f(x)\) is greater than zero, the point is assigned to one class, and if it is less than zero, the point is assigned to the other class. A value of \(f(x) = 0\) indicates that the point is on the separating hyperplane. The equation of the energy function can be described as:

\[
E(w, b) = \min_{w, b} \frac{1}{2}||w||^2 + C \sum_{i=1}^{n} \xi_i
\]  

where \(\xi_i > 0\) for \(i = 0, 1, 2, \ldots, n\).

The first part of Equation (2) refers to minimizing the length of the weight vector, \(w\), and the second part refers to minimizing the sum of classification errors. These simple steps describe how the SVM works.

Feature extraction from the neural network layer:
The next step involves the algorithm collecting and preparing training data to be used for training the model on the neural network.

Data processing:
Data processing depends on factors such as the data structure, neurons, activation function, and objective function used. The choice of solution is experimental.

If necessary, the input data can be standardized or normalized to facilitate the operation of the algorithm and the interpretation of the obtained results as output.

When deciding to use the SVM algorithm for feature extraction, the classification results from the SVM are prepared as input to the neural network. These results can constitute a vector of features for subsequent neural network layers.
We create a neural network with inputs obtained from the SVM. The neural network should be designed to adapt to the characteristics of the data and effectively predict the final result.

- Classification:
The resulting set of features is used for classification, where both the SVM and the neural network influence the final decision.

It is clear that both the SVM and neural networks are used in different contexts and have different advantages and limitations. The decision to use one or both depends on the specific situation, input data, and purpose of the analysis. In practice, we usually experiment with different models to find the most effective solution for a given problem.

8. Conclusions

Neglecting the protection of industrial processes from cyberattacks can lead to serious consequences, including production loss, security threats, financial losses, and reputation damage. Therefore, an increasing number of companies are beginning to understand the importance of ensuring cybersecurity in industry and are taking actions to safeguard their systems and processes. Investing in robust cybersecurity measures is typically profitable, as it can help minimize risks and reduce costs associated with potential incidents. Industrial enterprises should prioritize cybersecurity and adjust their strategies to protect their industrial automation systems from threats. Thus, it is crucial for industrial enterprises to take action to secure their industrial systems against cyberattacks. This includes implementing security measures such as firewalls, intrusion detection and prevention systems (IDPS), monitoring network traffic, access authorization, and regular software updates. Furthermore, it is important to educate staff on cybersecurity and stay abreast of the latest trends and threats in industrial cybersecurity. Only in this way can the risk be reduced, and industrial facilities protected from potential attacks.

The cost of weak cybersecurity for industrial automation systems can be not only high but also significantly exceed the expenses of implementing appropriate security measures. Therefore, investing in strong cybersecurity measures is typically cost-effective, as it can assist in risk minimization and cost reduction resulting from potential incidents. Industrial enterprises should prioritize cybersecurity and adapt their strategies to protect their industrial automation systems from threats.

Cybersecurity is an area that aims to protect digital data and systems from threats associated with the cyber domain. It consists of various elements that help secure data and infrastructure. The main six key elements of cybersecurity, as presented in [1], can be applied to protect digital data, whether they are stored, processed, or transmitted.

The continuous development of automation systems and the increasingly blurred boundary between the OT and IT worlds make proper protection of industrial installations crucial. The examples provided at the beginning of the article pertain to critical infrastructure, which not all automation professionals encounter daily. However, we should not forget that factories and businesses utilizing automation systems can also become targets of attack, whether it be for ransomware extortion, machine damage, or generating losses to gain an unfair competitive advantage, such as halting production. Therefore, these are issues that cannot be underestimated.

In our article, we prioritize the inclusion of webpages alongside scholarly articles to provide a comprehensive and up-to-date overview of cybersecurity in Industry 4.0. While scholarly articles contribute valuable insights, webpages offer real-time information, practical examples, and case studies that reflect the rapidly evolving nature of cybersecurity threats and strategies. The dynamic area of digital threats requires a nuanced approach, and webpages, often from reputable sources such as cybersecurity organizations, industry reports, and governmental bodies, provide timely and relevant content that enhances the practical applicability of our research. By combining both scholarly articles and webpages, our article aims to bridge the gap between theoretical knowledge and real-world implemen-
tation, offering a holistic perspective on the importance of cybersecurity in safeguarding industrial automation systems.

In our opinion, continuous improvement of qualifications and acquiring knowledge regarding cybersecurity and proper device protection are extremely important. In the work of automation professionals, these include not only engineering stations but also controllers, HMI panels, industrial computers, SCADA systems, and human factors.

In the future, the integration of digital twins (DTs) and multi-access edge computing (MEC) could play a major role in cybersecurity. This promising technology enables edge intelligence in 6G networks, recognized as a key factor supporting the development of the Industrial Internet of Things (IIoT). This solution could facilitate more effective monitoring and management of critical infrastructures and industrial processes, thereby contributing to increased security levels in industry and IoT sectors [32]. Another interesting solution may be the combination of the IIoT and federated learning (FL), considered promising for enabling Industry 4.0 and beyond. However, scheduling more IIoT devices involved in FL contributes to faster learning rates but results in increased learning costs in terms of energy consumption and reduced model accuracy [33].

Author Contributions: Conceptualization, J.P.; methodology, J.P.; software, not applicable; validation, not applicable; formal analysis, not applicable; investigation, J.P.; resources, J.P.; data curation, not applicable; writing—original draft preparation, J.P.; writing—review and editing, J.P. and A.ˇS.; visualization, J.P. and A.ˇS.; supervision, A.ˇS.; project administration, A.ˇS.; funding acquisition, A.ˇS.

All authors have read and agreed to the published version of the manuscript.

Funding: This research study is part of Project No. 0211/SBAD/0121 funded by the Poznan University of Technology, Poland.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References
15. IBM. IBM Industry 4.0. Available online: https://www.ibm.com/topics/industry-4-0 (accessed on 19 November 2023).
16. GMP Data Integrity Definitions and Guidance for Industry, 2018. Available online: https://assets.publishing.service.gov.uk/media/5ac4a6cc40f0b60a4be86d80/Data_integrity_definitions_and_guidance_v2_Withdrawn.pdf (accessed on 18 March 2024).


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.