IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

Safeguarding Industrial Automation: A Comprehensive Overview of Cybersecurity Measures

Vishvesh H. Khisty

CSE Icon Inc Works, USA

ABSTRACT: The rapid integration of advanced technologies in industrial automation has revolutionized manufacturing processes, enabling enhanced efficiency, productivity, and innovation. However, the increased connectivity of industrial systems has also exposed them to a wide range of cyber threats, with recent studies revealing alarming statistics on the prevalence and impact of cyberattacks on industrial control systems (ICS). This article provides a comprehensive overview of the cybersecurity challenges faced by industrial automation systems, including legacy systems, interconnected networks, insider threats, remote access vulnerabilities, and supply chain risks. The article also presents a detailed analysis of effective cybersecurity strategies, such as risk assessment, defense-in-depth, access control, encryption, continuous monitoring, and employee training, along with relevant industry standards and case studies. The financial and operational consequences of cyberattacks on industrial organizations are examined, highlighting the critical need for robust cybersecurity measures to ensure the resilience and security of industrial automation systems.

KEYWORDS: Industrial Automation Cybersecurity, Cyber Threats and Vulnerabilities, Cybersecurity Strategies and Best Practices, Stuxnet and WannaCry Cyberattacks, ISA/IEC 62443 and NIST Standards

I. INTRODUCTION

Industrial automation has become an integral part of modern industrial processes, driving efficiency, productivity, and innovation across various sectors. The rapid adoption of Internet of Things (IoT) devices, cloud computing, and interconnected networks has transformed the industrial landscape, enabling real-time monitoring, remote control, and data-driven decision-making. However, this increased connectivity has also exposed industrial systems to a wide range of cyber threats. According to a thorough study by Kaspersky Lab, cyberattacks targeted a startling 41.2% of industrial control systems (ICS) in just the second half of 2020 [1]. This alarming statistic highlights the growing risk of cyber threats to industrial automation systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

The consequences of cyber attacks on industrial automation systems can be severe and far-reaching. Operational disruptions caused by cyber incidents can lead to production downtime, equipment damage, and supply chain interruptions. In 2017, the NotPetya ransomware attack impacted several industrial organizations, including Merck, a pharmaceutical giant, resulting in a production shutdown that lasted for weeks and financial losses exceeding $310 million [2]. Another major worry is data breaches because cybercriminals may obtain sensitive industrial information like intellectual property, trade secrets, and customer data. The Verizon Data Breach Investigations Report 2021 revealed that the manufacturing industry experienced a 156% increase in data breaches compared to the previous year [3].

The financial impact of cyber attacks on industrial organizations can be staggering. In 2019, the average cost of a data breach in the industrial sector reached $5.2 million, according to the IBM Cost of a Data Breach Report 2020 [4]. This figure takes into account various factors, including loss of productivity, remediation costs, legal expenses, and reputational damage. Furthermore, the Ponemon Institute's study on the cost of cybercrime found that the average cost of cybercrime for industrial companies increased by 13% in 2019, reaching $11.35 million per organization [5].

To address these growing cybersecurity challenges, industrial organizations must prioritize the implementation of robust cybersecurity measures. The National Institute of Standards and Technology (NIST) has developed the Cybersecurity Framework for Critical Infrastructure, which provides guidelines for identifying, protecting, detecting, responding to, and recovering from cyber incidents [6]. The framework emphasizes the importance of risk assessment, access control, continuous monitoring, and incident response planning. Industry-specific standards, like the ISA/IEC 62443 series, also have detailed rules and instructions on how to protect industrial automation and control systems (IACS) [7].

Year	Statistic	Value
2020	Percentage of industrial control systems (ICS) targeted by cyberattacks (Kaspersky Lab)	41.2%
2017	Financial losses from NotPetya ransomware attack on Merck	$310 million
2021	Increase in data breaches in the manufacturing industry compared to the previous year (Verizon Data Breach Investigations Report)	156%
2019	Average cost of a data breach in the industrial sector (IBM Cost of a Data Breach Report)	$5.2 million
2019	Increase in the average cost of cybercrime for industrial companies (Ponemon Institute)	13%
2019	Average cost of cybercrime for industrial companies (Ponemon Institute)	$11.35 million

Table 1: Impact of Cyberattacks on Industrial Automation Systems [1-5]

II. CYBERSECURITY CHALLENGES IN INDUSTRIAL AUTOMATION

Legacy Systems:

Many industrial facilities continue to rely on legacy automation systems that were designed and implemented without adequate security considerations. These systems often lack built-in security features, such as strong authentication mechanisms, encryption, and regular security updates, making them vulnerable to cyberattacks. According to a thorough survey by Fortinet, 78% of businesses in the industrial sector still use legacy systems [8]. These outdated systems leave significant security gaps that cybercriminals can use to gain unauthorized access to crucial infrastructure.
The difficulty of upgrading or replacing legacy systems further increases the risks associated with them. Industrial organizations often face challenges in terms of compatibility, downtime, and financial constraints when attempting to modernize their automation systems. A study by Cisco found that 46% of industrial organizations cite the inability to

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

integrate legacy systems with new technologies as a major barrier to implementing effective cybersecurity measures [9].

Interconnected Networks:
The increasing convergence of operational technology (OT) and information technology (IT) networks has created new vulnerabilities in industrial automation systems. Traditionally, OT networks were isolated from external networks, but the demand for real-time data exchange and remote monitoring has led to the integration of OT and IT systems. This interconnectivity has expanded the attack surface, providing hackers with multiple entry points to infiltrate industrial networks.

According to a report by Trend Micro, the number of vulnerabilities discovered in industrial control systems (ICS) increased by an alarming 25% in 2020 compared to the previous year [10]. Threat actors may take advantage of these flaws to obstruct industrial processes, steal confidential information, or physically harm equipment. According to the Purdue Enterprise Reference Architecture (PERA) model, which helps create and run safe industrial networks, separating OT and IT networks is very important to make it harder for attackers to move from one network to another [11].

Insider Threats:
Malicious insiders, such as disgruntled employees or contractors, pose a significant threat to industrial automation systems. These individuals have privileged access to critical infrastructure and can exploit their knowledge and credentials to cause harm intentionally. According to the Verizon Data Breach Investigations Report 2021, insider threats account for 30% of security incidents in the industrial sector [12]. This highlights the need for robust access control mechanisms, employee monitoring, and behavioral analytics to detect and prevent insider attacks.
Insider threats can have severe consequences for industrial organizations. In 2020, a former employee of a water treatment plant in Kansas was charged with remotely accessing the facility's computer system and attempting to tamper with the water supply [13]. This incident underscores the importance of implementing strict access controls, regular security audits, and employee training to mitigate the risk of insider threats.

Remote Access:
The widespread adoption of remote monitoring and maintenance capabilities in industrial automation systems has introduced new security risks. Remote access allows authorized personnel to monitor and control industrial processes from remote locations, improving efficiency and reducing downtime. However, if it is not properly secured, attackers may use remote access to gain unauthorized access to crucial systems.

A study by Kaspersky revealed that remote access vulnerabilities were responsible for 37% of ICS-related incidents in 2019 [14]. Attackers can exploit weak authentication mechanisms, unpatched vulnerabilities, or stolen credentials to compromise remote access points and infiltrate industrial networks. The NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, tells you how to keep remote access safe by suggesting things like using virtual private networks (VPNs), two-factor authentication, and regular security checks [15].

Supply Chain Risks:
Industrial automation systems rely heavily on third-party vendors for hardware components, software, and services. This dependency exposes industrial organizations to supply chain risks such as counterfeit products, malicious code injection, and compromised vendor networks. According to a Ponemon Institute study, 56% of organizations have experienced a data breach due to a third-party vendor [16]. These breaches can have cascading effects on industrial operations, leading to production disruptions and financial losses.

To mitigate supply chain risks, industrial organizations must implement rigorous vendor risk management programs. The ISA/IEC 62443-2-4 standard guides security requirements for industrial automation and control system service providers [17]. This includes conducting thorough vendor assessments, establishing secure communication channels, and regularly monitoring vendor performance. Additionally, implementing technologies such as blockchain can enhance supply chain transparency and traceability, enabling the detection of counterfeit products and unauthorized modifications [18].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

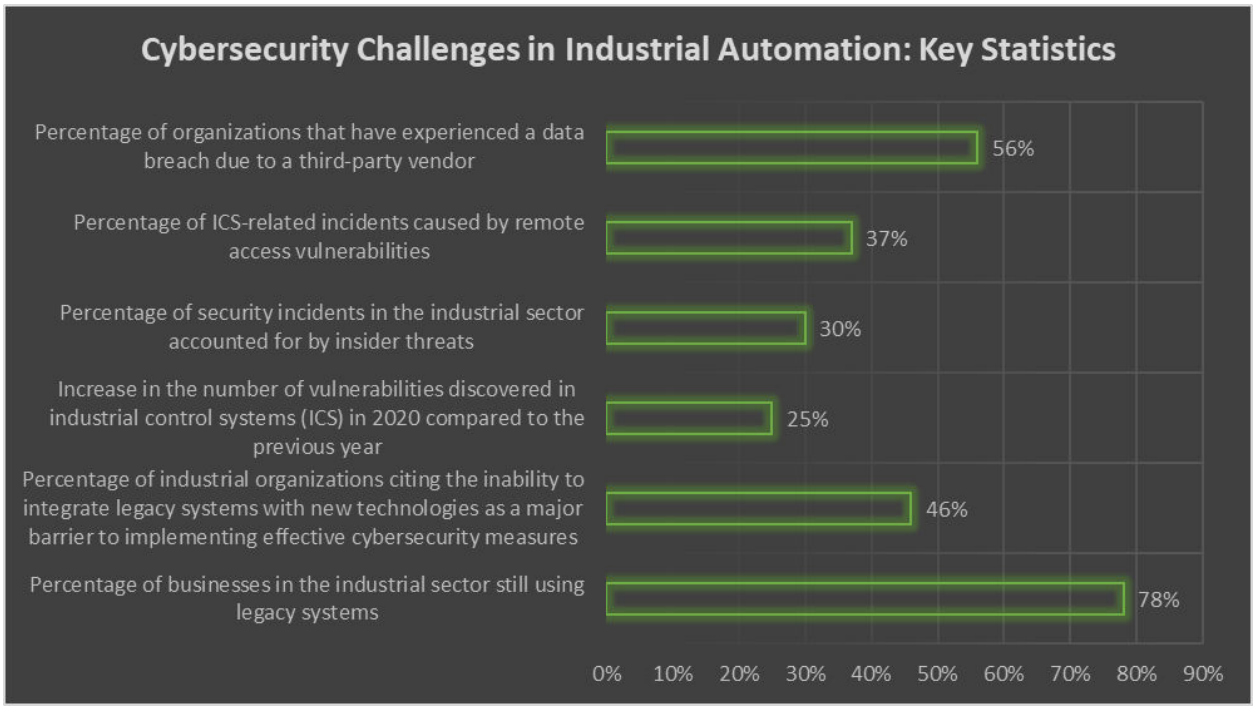

Fig. 1: Key Vulnerabilities in Industrial Automation Systems: A Statistical Overview [8-18]

III. CYBERSECURITY STRATEGIES FOR INDUSTRIAL AUTOMATION

Risk Assessment:
Conducting comprehensive risk assessments is a crucial step in developing effective cybersecurity strategies for industrial automation systems. By identifying and prioritizing potential vulnerabilities, organizations can allocate resources efficiently and implement targeted security measures. The ISA/IEC 62443 standard provides a framework for assessing and managing cybersecurity risks in industrial environments [19].

A study by the Ponemon Institute found that organizations that regularly conduct risk assessments experience 29% fewer data breaches compared to those that do not [20]. Risk assessments should consider various factors, such as the criticality of assets, the likelihood of cyber threats, and the potential impact of successful attacks. The IEC 62443-3-2 standard guides conducting risk assessments for industrial automation and control systems (IACS) [21].

Defense-in-Depth:
Implementing a defense-in-depth approach is essential for protecting industrial automation systems against a wide range of cyber threats. This multi-layered security strategy involves deploying various security controls at different levels of the system architecture, including network segmentation, firewalls, intrusion detection systems (IDS), and endpoint protection.

The NIST SP 800-82 guide recommends adopting a defense-in-depth strategy for industrial control systems (ICS) security [22]. By creating multiple layers of defense, organizations can prevent, detect, and respond to cyber attacks more effectively. For example, network segmentation can isolate critical assets and limit the spread of malware, while firewalls can control traffic flow and block unauthorized access attempts.

A case study by Siemens demonstrated the effectiveness of a defense-in-depth approach in securing an industrial plant [23]. By implementing network segmentation, firewalls, and intrusion detection systems, the company was able to reduce the risk of cyber attacks by 85% and improve the overall security posture of the facility.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

Access Control:
Enforcing strict access control measures is crucial for protecting sensitive industrial assets from unauthorized access and reducing the risk of insider threats. Role-based access control (RBAC) and the principle of least privilege are key strategies for managing user permissions and ensuring that users have access only to the resources they need to perform their tasks.

The IEC 62443-3-3 standard provides guidelines for implementing access control in industrial automation and control systems [24]. This includes defining user roles and permissions, implementing strong authentication mechanisms, and regularly reviewing and updating access rights. A study by the SANS Institute found that organizations that implement RBAC experience 50% fewer security incidents compared to those that do not [25].

Encryption:
Deploying robust encryption protocols is essential for safeguarding sensitive data transmitted and stored within industrial automation systems. Encryption ensures the confidentiality and integrity of data, preventing unauthorized access and tampering by malicious actors.

The ISA/IEC 62443-3-3 standard specifies security requirements for industrial automation and control systems, including encryption [26]. The standard recommends using strong encryption algorithms, such as AES (Advanced Encryption Standard), and secure communication protocols, such as TLS (Transport Layer Security), to protect data in transit and at rest.

A case study by Rockwell Automation highlighted the importance of encryption in securing industrial networks [27]. By implementing end-to-end encryption using the CIP Security protocol, the company was able to protect sensitive data and prevent unauthorized access to industrial control systems.

Continuous Monitoring:
Implementing continuous monitoring solutions is crucial for detecting and responding to cyber threats in real-time. Security monitoring tools and analytics enable organizations to gain visibility into their industrial networks, identify anomalous activities, and promptly mitigate potential security incidents.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA) guides continuous monitoring for ICS security [28]. This includes deploying intrusion detection systems (IDS), security information and event management (SIEM) solutions, and network monitoring tools to detect and respond to cyber threats effectively.

A study by the Aberdeen Group found that organizations with continuous monitoring capabilities experience 50% fewer security incidents and 40% faster incident response times compared to those without such capabilities [29]. Continuous monitoring enables industrial organizations to proactively identify and address security issues before they escalate into major incidents.

Employee Training:
Providing comprehensive cybersecurity training programs for employees and contractors is essential for raising awareness about common cyber threats and best practices for safeguarding industrial automation systems. Human error remains a significant risk factor in cybersecurity incidents, and educating employees can help mitigate this risk.

A study by IBM found that human error accounts for 95% of cybersecurity incidents [30]. Regular training programs should cover topics such as password security, social engineering, phishing awareness, and incident reporting procedures. The ISA/IEC 62443-2-1 standard guides establishing and maintaining a cybersecurity training program for industrial automation and control systems [31].

A case study by the National Institute of Standards and Technology (NIST) demonstrated the effectiveness of employee training in reducing cybersecurity risks [32]. By implementing a comprehensive cybersecurity awareness program, the organization reduced the number of successful phishing attacks by 80% and improved employee compliance with security policies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

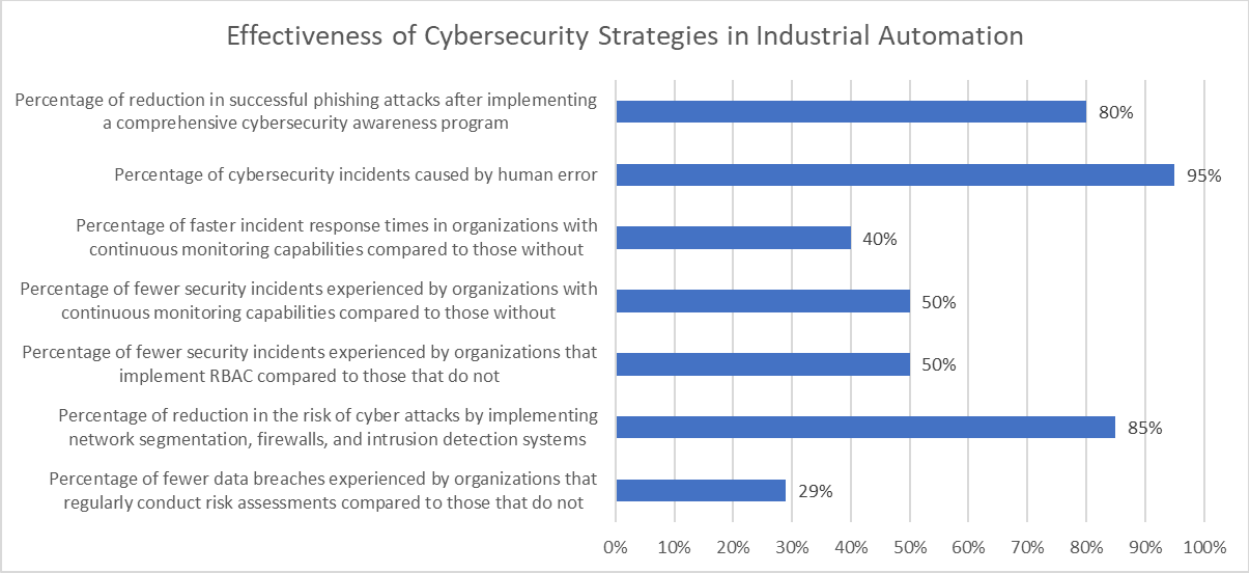

Fig. 2: Impact of Implementing Cybersecurity Best Practices in Industrial Automation [19-32]

IV. CASE STUDIES

Stuxnet Worm:

The Stuxnet worm, first discovered in 2010, is a prime example of a sophisticated cyber attack targeting industrial control systems. Stuxnet was specifically designed to target supervisory control and data acquisition (SCADA) systems used in nuclear enrichment facilities. The worm exploited multiple zero-day vulnerabilities in Microsoft Windows and Siemens Step7 software, allowing it to propagate and gain control over programmable logic controllers (PLCs) [33].

Stuxnet's primary target was the Natanz nuclear facility in Iran, where it caused significant damage to centrifuges used in the uranium enrichment process. The worm's payload was designed to subtly alter the rotational speeds of the centrifuges, causing them to spin out of control and self-destruct [34]. According to a report by Symantec, Stuxnet infected over 200,000 computers worldwide, with 60% of the infections concentrated in Iran [35].

The Stuxnet attack had far-reaching consequences beyond the immediate damage to Iran's nuclear program. It highlighted the vulnerability of critical infrastructure to cyberattacks and raised concerns about the potential for cyber warfare. The sophisticated nature of the worm, including its use of multiple zero-day exploits and its ability to evade detection, demonstrated the level of resources and expertise that could be employed in a targeted cyberattack [36].

Attribute	Value
Year Discovered	2010
Target Systems	Supervisory Control and Data Acquisition (SCADA) systems in nuclear enrichment facilities
Exploited Vulnerabilities	Multiple zero-day vulnerabilities in Microsoft Windows and Siemens Step7 software
Primary Target	Natanz nuclear facility in Iran
Damage Caused	Significant damage to centrifuges used in the uranium enrichment process

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

Payload Design	Subtly alter the rotational speeds of the centrifuges, causing them to spin out of control and self-destruct
Total Computers Infected Worldwide	Over 200,000
Percentage of Infections Concentrated in Iran	60%
Consequences	Highlighted the vulnerability of critical infrastructure to cyber attacks and raised concerns about the potential for cyber warfare
Sophistication	Demonstrated the level of resources and expertise that could be employed in a targeted cyberattack

Table 2: Key Attributes of the Stuxnet Worm Cyberattack [33-36]

WannaCry Ransomware:
The WannaCry ransomware attack, which occurred in May 2017, was a global cybersecurity incident that affected organizations across various sectors, including healthcare, telecommunications, and manufacturing. WannaCry exploited a vulnerability in the Microsoft Windows operating system (MS17-010) to propagate rapidly across networks, encrypting files and demanding ransom payments in Bitcoin [37].

The impact of WannaCry on industrial organizations was particularly severe, as the ransomware disrupted operations and caused significant financial losses. The attack affected more than 200,000 computers across 150 countries, including industrial control systems in manufacturing plants, transportation systems, and energy facilities [38].

One notable example of the impact on industrial organizations was the attack on Renault-Nissan, a global automobile manufacturer. The WannaCry ransomware forced the company to halt production at several of its manufacturing plants in France, Romania, and India, resulting in significant operational disruptions and financial losses [39].

The WannaCry attack exposed the vulnerability of industrial systems to ransomware attacks and highlighted the importance of timely patching and updating of operating systems and software. The attack also underscored the need for robust backup and recovery mechanisms to minimize the impact of ransomware incidents on industrial operations [40].

In response to the WannaCry attack, industrial organizations worldwide have increased their focus on cybersecurity measures, including regular vulnerability assessments, patch management, employee training, and incident response planning. The ISA/IEC 62443-4-2 standard provides guidance on technical security requirements for industrial automation and control system components, including protection against malware and ransomware [41].

V. CONCLUSION

The increasing sophistication and frequency of cyberattacks targeting industrial automation systems underscore the urgent need for organizations to prioritize cybersecurity. By adopting a proactive and comprehensive approach to cybersecurity, industrial organizations can effectively mitigate risks, detect and respond to threats, and ensure the continuity of their operations. The implementation of robust security controls, such as network segmentation, access control, encryption, and continuous monitoring, along with regular risk assessments and employee training, can significantly enhance the resilience of industrial automation systems against evolving cyber threats. Moreover, adherence to industry-specific cybersecurity standards and frameworks, such as the ISA/IEC 62443 series and the NIST Cybersecurity Framework, provides a structured approach to managing cybersecurity risks in industrial environments. As the convergence of IT and OT systems continues to expand the attack surface, industrial organizations must foster a culture of cybersecurity awareness, collaboration, and continuous improvement to stay ahead of the ever-changing threat landscape. By prioritizing cybersecurity as an integral part of their operational strategy, industrial organizations

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

can safeguard their critical assets, protect against financial and reputational damages, and maintain the trust of their stakeholders in an increasingly connected world.

REFERENCES

[1] Kaspersky ICS CERT, "Threat landscape for industrial automation systems. H2 2020," Kaspersky, 2021, p. 4.
[2] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, Aug. 22, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[3] Verizon, "2021 Data Breach Investigations Report," Verizon, 2021, p. 20.
[4] IBM Security, "Cost of a Data Breach Report 2020," IBM, 2020, p. 11.
[5] Ponemon Institute, "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture, 2019, p. 13.
[6] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," NIST, Apr. 16, 2018. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018
[7] ISA/IEC 62443 Series, "Industrial Automation and Control Systems Security," International Society of Automation, 2021.
[8] Fortinet, "The State of Operational Technology and Cybersecurity Report," Fortinet, 2020, p. 6.
[9] Cisco, "Securing Industrial Networks: Challenges and Solutions," Cisco, 2021, p. 3.
[10] Trend Micro, "2020 Annual Cybersecurity Report," Trend Micro, 2021, p. 18.
[11] T. J. Williams, "The Purdue Enterprise Reference Architecture," Computers in Industry, vol. 24, no. 2-3, pp. 141-158, 1994, doi: 10.1016/0166-3615(94)90017-5.
[12] Verizon, "2021 Data Breach Investigations Report," Verizon, 2021, p. 35.
[13] U.S. Department of Justice, "Former Employee of Kansas Water Treatment Plant Indicted for Tampering with Public Water System," Press Release, Apr. 14, 2021. [Online]. Available: https://www.justice.gov/usao-ks/pr/former-employee-kansas-water-treatment-plant-indicted-tampering-public-water-system
[14] Kaspersky ICS CERT, "Threat landscape for industrial automation systems. H2 2019," Kaspersky, 2020, p. 12.
[15] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82, Revision 2, National Institute of Standards and Technology, May 2015, doi: 10.6028/NIST.SP.800-82r2.
[16] Ponemon Institute, "Data Risk in the Third-Party Ecosystem," Ponemon Institute, 2017, p. 1.
[17] ISA/IEC 62443-2-4, "Security for industrial automation and control systems: Part 2-4: Security program requirements for IACS service providers," International Society of Automation, 2018.
[18] M. Mylrea and S. N. G. Gourisetti, "Blockchain for Supply Chain Cybersecurity, Optimization and Compliance," in 2018 Resilience Week (RWS), Aug. 2018, pp. 70-76, doi: 10.1109/RWEEK.2018.8473517.
[19] ISA/IEC 62443 Series, "Industrial Automation and Control Systems Security," International Society of Automation, 2021.
[20] Ponemon Institute, "The Impact of Data Breaches on Reputation and Share Value," Ponemon Institute, 2017, p. 5.
[21] IEC 62443-3-2, "Security risk assessment for system design," International Electrotechnical Commission, 2020.
[22] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82, Revision 2, National Institute of Standards and Technology, May 2015, doi: 10.6028/NIST.SP.800-82r2.
[23] Siemens, "Defense-in-Depth: A Comprehensive Approach to Industrial Cybersecurity," Siemens, 2019, p. 8.
[24] IEC 62443-3-3, "System security requirements and security levels," International Electrotechnical Commission, 2013.
[25] SANS Institute, "The Power of Role-Based Access Control," SANS Institute, 2020, p. 3.
[26] ISA/IEC 62443-3-3, "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels," International Society of Automation, 2013.
[27] Rockwell Automation, "Securing Industrial Networks with CIP Security," Rockwell Automation, 2021, p. 5.
[28] DHS CISA, "Continuous Monitoring for Industrial Control Systems," Department of Homeland Security Cybersecurity and Infrastructure Security Agency, 2020.
[29] Aberdeen Group, "The Benefits of Continuous Monitoring in Industrial Cybersecurity," Aberdeen Group, 2019, p. 7.
[30] IBM Security, "2020 Cyber Resilient Organization Report," IBM, 2020, p. 2.
[31] ISA/IEC 62443-2-1, "Establishing an industrial automation and control system security program," International Society of Automation, 2010.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306242|

[32] NIST, "Cybersecurity Awareness Training: A Case Study," National Institute of Standards and Technology, 2021, p. 4.
[33] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec Security Response, Feb. 2011, pp. 1-69.
[34] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, May-June 2011, doi: 10.1109/MSP.2011.67.
[35] Symantec, "W32.Stuxnet," Symantec, 2010. [Online]. Available: https://www.symantec.com/security-center/writeup/2010-071400-3123-99
[36] K. Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, Nov. 3, 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[37] Symantec, "What you need to know about the WannaCry Ransomware," Symantec, May 23, 2017. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack
[38] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," Computer, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.
[39] Reuters, "Renault-Nissan resumes nearly all production after cyber attack," Reuters, May 15, 2017. [Online]. Available: https://www.reuters.com/article/us-renault-nissan-cybercrime-idUSKCN18B0BO
[40] M. Ahmadian, H. Shahriari, and S. Ghaffarian, "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares," in 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Sep. 2015, pp. 79-84, doi: 10.1109/ISCISC.2015.7387902.
[41] ISA/IEC 62443-4-2, "Technical security requirements for IACS components," International Society of Automation, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details