International Journal for Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2024.0804210

Research Article

Vol. 8 issue 4 Oct-Dec 2024

Conceptual Security Framework to Mitigate Risks in Organizational Policies while Transforming to Industry 4.0

Saba Khalil Toor[1], Waqar Azeem[2], Mubashar Mushtaq[3], Aftab Ahmed Malik[4], Zain Ul Haq[5], Haroon Ur Rashid Kayani[6]

[1,3,5] Department of Computer Science FC College Lahore.
[2] Center of excellence in Solid State Physics, University of Punjab, Lahore.
[4] University of Kent, Canterbury England.
[6]School of Informatics and Robotics, Institute for Art and Culture, Lahore.
Corresponding Author: haroon.rashid@iac.edu.pk

Received: October 09, 2024; **Accepted:** October 24, 2024; **Published:** December 17, 2024

ABSTRACT

The manufacturing industry has undergone a radical transformation with the emergence of Industry 4.0, characterized by the convergence of Cyber-Physical Systems, Artificial Intelligence, Machine Learning, the Internet of Things, and big data. This fourth industrial revolution enables real-time monitoring and prompt decision-making. However, organizational policies pose significant challenges to its adoption, particularly regarding cybersecurity risks. This study investigates these challenges and proposes strategies for mitigation. Conducted in Pakistan, this mixed-methods research employs both quantitative (survey) and qualitative (interviews) approaches. The findings highlight the need for increased awareness, secure communication channels, interoperability, robust policies, and expert talent. Key challenges include data theft risks in global collaboration and weak organizational procedures. A conceptual framework addresses these issues, ensuring a secure and resilient transformation to Industry 4.0.

Keywords: Industry 4.0, Cyber Security Organizational policies, Risks, Artificial Intelligence, Big Data, Intelligence, Digitalization, Ecosystem.

1. INTRODUCTION

Cybersecurity is the most essential part of the industry 4.0 transformation life cycle. The key value through the transformation life cycle must be addressed at any stage. This study focuses on the organizational policies that may create issues in the transformation to Industry 4.0. and how the risk of cyber security can be lessened. It is observed that if the transformation is done without considering Cybersecurity, the product will be a disaster as Industry 4.0 is connected with all the components of the standardized industry [1]. An organization that is transforming to Industry 4.0 will have hundreds of devices connected to the network that may produce data or distribute data. These devices can sometimes be more dangerous because of any vulnerability in the network that may expose the data. In this research, current Organizational security policies are the key focus in which we also look at how these policies can be a problem in adopting Industry 4.0. As this is an evolving technology concept in the manufacturing industry, especially in Pakistan, there is much work that needs to be done in terms of policies, procedures, Regulations, and face-lifting the entire structure in both public and private sectors, and the list of work to be done goes on and on. Suppose a country like Pakistan wants to join developed countries with good footprints in intelligent manufacturing setups. In that case, it must comply with emerging technologies like Industry 4.0 to boost its performance quickly [2].

To find the results, one needs to identify the main reasons behind the weak security setups in manufacturing industries. Hence, cybersecurity risks in organizational policies were investigated while transforming to industry 4.0.

The existing organizational security policies, and how can these policies are vulnerable while transforming to Industry 4.0 were discussed. Security risks be mitigated with a robust framework were investigated.

2. LITERATURE REVIEW

The advent of Industry 4.0 has brought significant transformations to the manufacturing industry, presenting both opportunities and challenges. A critical examination of existing literature reveals key concerns in cybersecurity, interoperability, and operational technology (OT) convergence, according to Radanliev and Petrillo Industry 4.0's increased connectivity and data exchange heighten cybersecurity risks. Human resources must develop competencies and capabilities to address these risks. Companies struggle to convey cybersecurity value to customers and internally assess cyber risks [3]. Furthermore, interoperability is vital for Industry 4.0 success, enabling data exchange and knowledge sharing between systems [4]. However, proprietary protocols hinder seamless operations and security [5].

OT and IT convergence require distinct cybersecurity methodologies due to unique constraints and

cultures. Additionally, Industry 4.0 adoption faces challenges, including investigation and learning demands, data management, worker conversion, and cyber-physical attacks Petrillo [6] [7] [8].

Effective Industry 4.0 transformation necessitates addressing cybersecurity Radanliev and according to Petrillo, Horváth, Stouffer and Cyberattacks applies to interoperability and OT convergence challenges. Companies must prioritize building competencies, ensuring interoperability, and securing OT systems to harness Industry 4.0 benefits [9-16].

The advent of Industry 4.0 has brought significant transformations to the manufacturing industry, presenting both opportunities and challenges. A critical examination of existing literature reveals key concerns in cybersecurity, interoperability, and operational technology (OT) convergence.

2.1. Cybersecurity Concerns

Industry 4.0's increased connectivity and data exchange heighten cybersecurity risks Human resources must develop competencies and capabilities to address these risks. Companies struggle to /convey cybersecurity value to customers and internally assess cyber risks [2].

2.2. Interoperability Challenges

Interoperability is vital for Industry 4.0 success, enabling data exchange and knowledge sharing between systems. However, proprietary protocols hinder seamless operations and security [4] [5].

2.3. Operational Technology Convergence

According to Joseph and Prinsloo OT and IT convergence require distinct cybersecurity methodologies due to unique constraints and cultures [8-9].

2.4. Additional Challenges

According to Petrillo Industry 4.0 adoption faces challenges, including investigation and learning demands, data management, worker conversion, and cyber-physical attacks. Effective Industry 4.0 transformation necessitates addressing cybersecurity, interoperability, and OT convergence challenges. Companies must prioritize building competencies, ensuring interoperability, and securing OT systems to harness Industry 4.0 benefits [6].

3. RESEARCH METHODOLOGY

The research methodology is mixed-mode and consists of qualitative and quantitative research methods. In the quantitative method, a survey was created and circulated among software developers working in the software industry. The purpose was to learn about their understanding of and knowledge of issues in Industry 4.0 and their recommendations for mitigating risks in Industry 4.0. Moreover, in the qualitative research method, two interviews were conducted with the experts of Industry 4.0 service providers to seek more knowledge about Industry 4.0 from their experience.

In the quantitative method, a survey

was created based on the issues identified in the literature review. That survey was shared with two technical persons, as a pilot study, to have their feedback about the survey question. After the positive feedback, the survey was circulated via Google Forms to the software developers in different software houses in Lahore to know their understanding and knowledge of issues/risks in Industry 4.0 and their recommendations to mitigate these issues/risks. This survey has 31 questions that contain the Nominal scale and Ordinal scale. The objectives of this survey were:

- To seek the developer's current understanding/awareness of Industry 4.0
- To know about the issues that exist in Industry 4.0.
- To know their perspectives about the improvement in Industry 4.0.

In addition, to investigate those issues further, there was a need to interview some experts, especially those who provide Industry 4.0 services in Pakistan. For that, two interviews were conducted with experts in Industry 4.0. the objectives of the interview were:

- To seek in-depth knowledge and understanding of issues/problems identified in the literature review chapter.
- We used the qualitative data collection method to reduce ambiguity in the results obtained from the survey respondents.

1st Interview was conducted face-to-face with the company's CEO, providing Industry 4.0 services. The second interview was conducted online via Microsoft Teams with a company's technical expert who provided I4.0 services. All those issues were written as open-ended questions. Before the interview, permission was taken from the interviewees to record the session for further proceedings. Upon their approval, the first interview was recorded via a Mobile sound recorder, and the second interview was recorded via the Microsoft Teams recording feature. After the interviews, all recorded data was transcribed, and the vocals were transformed into the text format. This activity was done via the online transcribe tool OTTER. Then, all these transcriptions were read very carefully, and the critical notes and the prominence points were related to the desired answers. Then, the exact nature of the labels separated and grouped formed the categories.

4. DATA ANALYSIS

4.1. Quantitative Data Analysis

For quantitative research, 40 participants responded to survey questions. Cronbach's alpha reliability test was performed on the survey results to check the consistency and calculate the instrument's reliability.

4.2. Knowledge of Industry 4.0

Out of 40 respondents. 35 % knew Industry 4.0. That means the awareness level of Industry 4.0 is low. as indicated in Table 2.

4.3. Global Collaboration

27.5 % of 40 respondents were sure

there are high chances of data exploitation while sharing info online. 13 and 32.5% also agreed that this could be a problem. In comparison, 35 % of respondents needed clarification on this. That means the majority of people have the idea that cybersecurity risks exist in global collaboration as indicated in Table 3.

Need for Strong Security Communication Channel

As shown in Table 4, 55 % of the 40 respondents favored building a secure communication bridge. That will mitigate the risk propagation. Moreover, 40 % of respondents needed clarification on this. Moreover, 5 % of respondents negate this fact. As Industry 4.0 works online with the help of sensors-based IoT devices, Artificial Intelligence, Machine Learning, and many emerging technologies, any weak connection/channel between two devices or systems may lead to malfunctioning and worse consequences.

Table 1: Cronbach's alpha reliability statistics result

Reliability

Scale: All variables Case processing summary:

Cases	**N**	**%**
Valid	40	100
Excluded	0	0
Total	**40**	**100**

Reliability statistics

Cronbach's Alpha	Cronbach's Alpha based on standardized items	Number of items
.939	.940	19

Table 2: Knowledge of Industry 4.0

		Frequency	**Percentage**	**Valid Percentage**	**Cumulative Percentage**
Valid	Yes	14	35.0	35.0	35.0
	No	26	65.0	65.0	100.0
	Total	40	100	100	

Table 3: Global Collaboration

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Disagree	2	5.0	5.0	5.0
Disagree	0	0.0	0.0	5.0
Neutral	14	35.0	35.0	40.0
Agree	13	32.5	32.5	72.5
Strongly Agee	11	27.5	27.5	100.0
Total	40	100.0	100.0	

Table 4: Need for a strong security communication channel

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strongly Disagree	1	2.5	2.5	2.5
Disagree	1	2.3	2.5	5.0
Neutral	16	40.0	40.0	45.0
Agree	16	40.0	40.0	85.0
Strongly Agree	6	15.0	15.0	100.0
Total	40	100.0	100.0	

.

4.4. Qualitative Data Analysis

Two in-depth interviews with Industry 4.0 experts in Pakistan were conducted to get a deeper understanding of ground realities regarding Industry 4.0. after analyzing the qualitative data following are the key findings:

4.4.1. Definition and Conceptualization of Industry 4.0

Industry 4.0 represents a technical shift and transformation in the manufacturing industry. It involves the integration of cyber and physical systems, leveraging big data, artificial intelligence, and cloud computing.

4.4.2. Awareness and Readiness

Awareness of Industry 4.0 is lacking at the ground level in Pakistan. Educational institutions need to update curricula to include Industry 4.0 concepts. Furthermore, Industry readiness is hindered by concerns about data security and cloud adoption.

Security Concerns

Secure communication channels and data protection are crucial in Industry 4.0. Experts emphasized the need for cybersecurity frameworks and regimes.

4.4.3. Efficiency and Productivity

Experts emphasized that Industry 4.0 can double efficiency and productivity through predictive maintenance and digitization.

4.4.4. Challenges and Recommendations

Pakistan's industry faces challenges in

adopting Industry 4.0 due to cost and planning concerns. Experts recommend government support, education, and training programs to promote Industry 4.0 adoption.

4.4.5. Operational Technology (OT) and Cybersecurity

OT professionals must stay updated with rapidly evolving technologies to ensure security.
The study highlights the need for increased awareness, education, and training to facilitate Industry 4.0 adoption in Pakistan. Experts emphasize the importance of cybersecurity, secure communication channels, and data protection. Government support and collaboration with industry stakeholders are crucial for promoting Industry 4.0 growth in Pakistan.

5. GAPS IDENTIFIED FROM DATA ANALYSIS

The gaps identified from the quantitative and qualitative data analysis are as follows. These gaps are split into two categories.

- Internal challenges
- External challenges

Internal challenges:
Internal challenges are those that directly affect the organization's performance and productivity. These are:

- The awareness of Industry 4.0 is not at ground level.
- Specialists' talent is lacking in terms of Competencies and capabilities.
- Transition reluctance in employees
- Internal threats (Employees, Misconfiguration of devices)
- Needs to revamp the Policies and by keeping Security as a priority.
- Lack of solid security communication channel between physical and cloud

External Challenges indirectly affect and hinder the performance of the organizations
CPS attacks include eavesdropping, denial of service (DoS), and false data injection.

- Education Curriculum in Pakistan needs to facelift.
- Lack of vibrant security policies, especially in the manufacturing sector.
- Deficiency of services (Internet and Power Supply)

Lack of security in products manufactured by OEMs.

6. PROPOSED FRAMEWORK

Based on the analysis of information, a framework is proposed. The objectives of this framework are to overcome the issues found and to make our system more Secure, Vigilant, and Resilient in terms of security.

6.1. High-Level Framework

To achieve these objectives, the proposed framework is developed. This is a high-level view of the framework.

6.2. Identification of Shortfalls

As indicated in Figure 2. Identification of shortfalls is the first phase of the process. During this phase, the current state of an organization is observed by keeping in mind security. This provides

an overview of where the organization stands right now and how mature this organization is in terms of security. This should be done by reckoning with a few questions, such as: What are the information systems that can affect the physical processes of a plant? What are the consequences if a system fails? How fast can that system be restored? What would happen if the employees were not fully aware of the technology? In this stage, all the available information or documentation is collected from the organization, including the Business Impact Analysis (BIA), Business Continuity Plan (BCP), Security policies, IT and OT network architecture (including routers, Switches, Firewall, Access Points, SCADA, and PLCs, etc.), any security standards implementation (like Information Security ISO 27001, NIST, or IEC 63443). Interviews will be conducted with the organization's stakeholders, and verification of the responses will be done with a physical Inspection of the plant. This technique is also called Ethnography.

The appropriate Cybersecurity controls are selected by taking emerging cyber-attacks and identified gaps (both internal and external) into consideration while implementing this system. The shortfalls identified in the research are Lack of Awareness, Specialist talent acquisition, organizational internal threats, Weak communication channel issues, Education, Government role, Deficiency of services (Internet and Power Supply), and OEM role. These shortfalls could be the risk in the transformation to Industry 4.0. After assessing the risks, these risks will be presented on the Risk Heat Map, which is based on Likelihood and impact. As this will be a graphical representation, identifying the potential security risks will be more convenient.

6.3. Resolution of Shortfalls

This is the second phase in the proposed framework Figure 3 indicates multiple relationships regarding the short fall and their solutions.

At this phase, the identified risks from phase 1 (Identification of Shortfalls) will be mitigated by using the following controls.

6.3.1. Awareness & Training

The major gap identified was the need for more awareness of Industry 4.0. That means the awareness still needs to be at the ground level. That is the main culprit in the transformation of Industry 4.0. How can a country transform into technology like Industry 4.0, where the awareness or knowledge of that particular domain is deficient? That is the first thing where we can make a start. As human interaction with machines is critical, they need to be more vigilant about this technology.

This framework proposed two solutions for this area. One solution is to start awareness campaigns in organizations, especially the manufacturing industries, so that the employees of that organization may be able to understand the concepts of transformation and Industry 4.0, and the latest technologies.

The second solution was proposed for the educational institutes in Pakistan. It is observed that many initiatives have already been taken. But still, there is a

disparity in what needs to be learned. They should include subjects related to Cybersecurity and introduction to emerging technologies in the course outline of all institutes. Although some educational institutes have started working on it and have introduced some courses like (AI) Artificial Intelligence, Machine Learning (ML), and some parts of digitalization, there is some disparity between what students should study. It is concluded that students should have 360 viewpoints of transformation that would make it more feasible for them to understand what issues can be faced in the time of transformation from one revolution to another, and then they can think better about their solutions. Besides awareness, training is also essential in the organization. Every authorized employee in the organization must be trained enough to mitigate the risk of internal breaches.

6.3.2. Talent Acquisition

When awareness and training campaigns are implemented at both levels (organization-level and government level), a new trend of adopting this technology will be set in society. Ultimately, more and more competent people will come forward, which may help to fill the gap of specialist talent in terms of competencies and capabilities. Besides this, the reluctance to transition within the organizations will be minimized.

6.3.3. Roles and Responsibilities

Then, there is a need to assign roles and responsibilities within the OT-enabled organizations. It is observed that the physical security of the plant is the responsibility of a Plant manager or a Safety & health manager but these people do not cover the cybersecurity part. In disparity, in an IT-enabled factory/plant, Cybersecurity is the responsibility of the Chief Information Security Officer (CISO). So, it is recommended that OT-enabled organizations assign these roles to a person who is fully aware of physical and cyber security. For this, a recommendation is for OT organizations with no security expert to temporarily assign this role to a Chief Security Officer (CSO) until this role is assigned to a CISO. Our ultimate goal should be one Chief Information Security Officer (CISO) who will look after operational and information security.

6.3.4. Vigilant culture in an organization

As it is observed from the literature most of the disruptions on a plant/factory come from inside the plant. So, the organization should implement some controls to help monitor and control any suspicious activities. For this, there is a need to implement controls on stakeholders. These controls can be Access Controls, Multi-Factor Authentication (MFA), and Artificial Intelligence-based predictions. These will allow them to access only authorized processes, facilities, and data. And with the help of these controls, a culture of vigilance can be established in a company.

6.3.5. Policies and Procedures

If we talk about the Policies and procedures, the framework of a company needs to be revamped when

the company wants to transform itself into Industry 4.0. As we know, security is an integral part of Industry 4.0. Without a proper security setup, it is not easy to survive in an Industry 4.0 environment. There should be secure access procedures that manage the stream of information. IT security policies can never be applied directly in the OT environment. The reason behind this is that IT and OT environments have different security requirements for network assets and users. These policies generally consist of Physical and environmental security, Access control, hardening, patching, backup, etc.

Now, there will be a difference if we take an example of patching. To apply a patch in the OT environment, the machine could be shut down and restarted, introducing the risk of downtime. Eventually, that will affect the productivity and efficiency of the plant. So, such activities need to be done in predefined time slots.

6.3.6. Secure Communication

This is the most crucial part of implementing the cyber-secure Industry 4.0 framework.

Data communication from the physical environment to the cloud environment should be highly secure to avoid interruption by unauthorized actors and cyber-attacks.

To achieve this goal, there is a dire need to revamp the communication architecture. In ICS, some zones, like the Control zone, consist of Sensors, Actuators, Meters, HMI, SCADA, Engineering workstation (EWS), Remote terminal unit (RTU), and PLCs, etc., and the Enterprise zone that differentiates the local Intranet from enterprise internet (that communicate with outside the organization). We know a simple firewall between these zones cannot provide the desired security. So, the proposed solution is based on existing standards like NIST SP 800-82 and ISA-99/IEC62443. Moreover, the solution is to introduce the Demilitarized Zone (DMZ) whose task is to avoid direct network traffic flow from the ICS network and Company Networks and restrict the enterprise zone users to access, interact, and exploit the control zone. Besides this, it provides distinct authentication methods and credentials for the users.

6.3.7. Government Role

The Government should take part in this revolution, too; it is observed that Pakistan lacks/needs an enabling environment. That is a very challenging situation right now. Each industry should have acceptable rights (in terms of equal and continuous services, e.g. Internet and power Supply) throughout the country. That would be the key to working on new ideas, policies, and strategies.

Besides this, Industries of Pakistan should have some strategy for forming incubators that welcome young technology startups. Moreover, the Government of Pakistan should provide funding to these young startups.

6.3.8. Monitor

In this stage, monitoring of the industrial environment and assets is done effectively. Where continuous monitoring of systems, assets, networks, devices, and the environment

is done. A standard will be established to ensure the expected behavior of the network in both IT and OT environments. If there is any deviation from the standard it will be considered as non-conformity and investigated abruptly. The monitoring can be done with the use of Security Information and Event Management (SIEM) (that will detect the threats, analyze the security events, and compliance reporting), a dedicated Security Operation Centre (SOC), And AI to detect security and operational threats. The whole system design should be done by keeping redundancy in mind, which will help avoid threat propagation in the system. For this, each critical component should have a redundant part reserved. If any issue occurs, make the redundant part active and the problematic part on hold to mitigate the issues.

What will happen if an incident occurs? How fast will our system come to a normal state after the incident? Do we have regular backups of all data and the systems? All these questions lead us towards the resilient nature of the system. To achieve this goal, a robust and appropriate Disaster Recovery Plan is needed. Initially, this can be implemented using existing standards like ISO 27002. That can be matured later.

This process is iterative and will mature gradually with more and more iterations.

6.4. Evaluation of Solutions

This is the third phase of the framework The evaluation phase is taken from the ISO 27001 section 9 "Performance Evaluation". Figure 4.

It has three stages

- Monitoring, Measurement, analysis, and evaluation
- Internal audit
- Management review

In the Monitoring, Measurement, analysis, and evaluation stage it needs to decide that:

- What demands to be monitored?
- Decide the method of monitoring.
- When will the monitoring done?
- And choose who the concerned person is.

In the internal audit stage, internal audit programs are conducted in the organization to verify that the system conforms to the organization's goals and objectives.

The third stage is management review. Where the applied controls are presented to the management, their feedback should be taken. Then, the conformance of the applied controls is assessed. Are the implemented controls effective in their application, correctly implemented, operating as intended, and producing the outcomes as planned, or not? If any problem occurs in the Evaluation stage, it will directly go to the Identification of Shortfalls stage to sort the issues and implement changes in the next iteration.

7. EVALUATION OF FRAMEWORK

Both qualitative and quantitative approaches were used in data collection. The research started with Subject matter expert interviews to collect the data. 2 interviews were conducted with security experts to collect the data. These experts were from companies that provide industry 4.0 solutions. Now, when the gaps were

identified from the qualitative and quantitative data. A framework was proposed to overcome those gaps and help the organizations minimize the risks faced while transforming to Industry 4.0. Then, that framework was presented to experts who were interviewed. They suggested a few changes to look into the framework as a whole instead of just the technical side. After updating the framework, it was again presented to them, and the results of their feedback were satisfactory.

Figure 1: A high-level view of the framework

Figure 2: Identification of Shortfalls

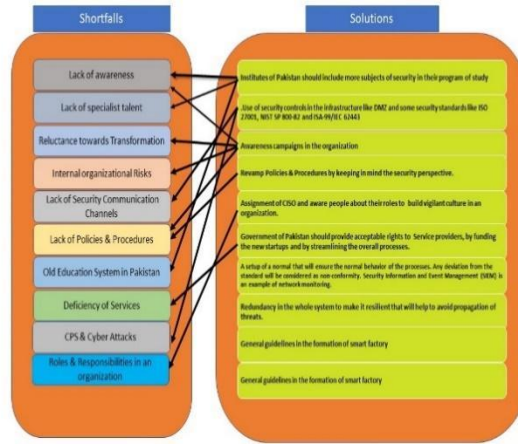

Figure 3: Resolution of shortfall

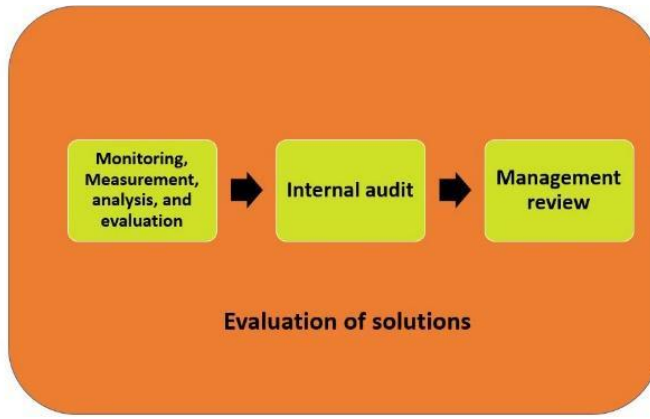

Figure 4: Evaluation

Table 5: Short falls and their resolution

Sr.	SHORTFALLS	SOLUTIONS
1.	CPS & Cyber Attacks	Implement security controls like DMZ and adhere to standards like ISO 27001, NIST SP 800-82, and ISA 99/IEC 62443
2.	Deficiency of Services	Set up monitoring systems like SIEM (Security Information and Event Management) for normal process behavior.
3.	Internal Organizational Risks	To strengthen the system and prevent the spread of threats, it should have redundancy. To strengthen the system and prevent the spread of threats, it should have redundancy
4.	Lack of Awareness	Organizational awareness campaigns
5.	Lack of Policies & Procedure	Revamp policies and procedures with a security-focused perspective.
6.	Lack of Security Communication Channels	Assignment of a CISO and educating employees about their roles to build a vigilant culture
7.	Lack of Specialist Talent	Pakistani educational institutions ought to incorporate more security-related topics into their curricula.
8.	Old Education System in Pakistan	Introduce security-related subjects in the education curriculum.
9.	Reluctance Towards Transformation	The Pakistani government should finance entrepreneurs, give service providers reasonable rights, and simplify procedures.
10.	Roles & Responsibilities in an Organization	General guidelines for defining roles in smart factories.

8. DISCUSSION

The rapid technological advancements necessitate industrial compliance with emerging technologies to enhance security, efficiency, and productivity. Industry 4.0, characterized by the convergence of cyber-physical systems, artificial intelligence, and IoT, enables increased output with reduced effort. However, Pakistan's adoption is hindered by limited ground-level awareness, primarily due to outdated educational curricula.

A significant obstacle is the lack of a comprehensive understanding of data transformation, perpetuating security concerns surrounding cloud adoption. Contrary to popular perception, cloud-based data is safer due to distributed storage across multiple silos, reducing the risk of data theft, exploitation, and unauthorized use.

As technology advances, the attack surface expands, categorizing groups into Utopian (good guys) and Dystopian (bad guys). Cyber-attacks

exploiting data can compromise physical systems, as exemplified by the devastating 2008 Stuxnet attack on Iran's Uranium Plant. This underscores the imperative for robust security measures.

Pakistan's industrial transformation requires a multifaceted ecosystem revamp, encompassing:

1. Standards and policies
2. Lawmakers and implementers
3. Incubators and startups
4. Enabling environments

Government funding for top projects is crucial. To ensure security, companies transitioning to Industry 4.0 must prioritize CIA (Confidentiality, Integrity, and Availability) across IT and OT. Given resource constraints, Pakistani companies can initiate transformation by:

1. Evaluating current infrastructure
2. Implementing security controls
3. Conducting awareness and training programs
4. Assigning roles and responsibilities
5. Establishing a vigilant organizational culture
6. Revamping policies and procedures
7. Securing communication channels using existing security frameworks and techniques

By adopting these measures, Pakistan can harness Industry 4.0 to enhance national growth, intelligence, efficiency, and productivity.

9. CONCLUSION

This study addressed the research question: "How do we mitigate cybersecurity risks in organizational policies while transforming to Industry 4.0?" Through a comprehensive literature review, quantitative and qualitative data collection, and data analysis, we identified existing security policies' vulnerabilities and proposed a conceptual framework to mitigate security risks. The framework's three stages - Identification of Shortfalls, Resolution of Shortfalls, and Evaluation of Resolutions - ensure a secure, vigilant, and resilient system.

As Industry 4.0 is relatively new in Pakistan, there is significant room for innovation and research. Future studies can:

1. Implement and test the proposed framework in real-world settings.
2. Explore Industry 4.0's social and economic impacts on Pakistan.
3. Develop more sophisticated cybersecurity measures for Industry 4.0 adoption.
4. Investigate the role of government policies and regulations in promoting Industry 4.0 growth.
5. Conduct comparative analyses of Industry 4.0 adoption in different countries.

This research provides a foundation for further exploration of Industry 4.0's cybersecurity challenges and opportunities in Pakistan. Researchers, policymakers, and industry stakeholders should collaborate to address Industry 4.0's cybersecurity challenges and promote its adoption in Pakistan.

REFERENCES

[1] A. Ancarani and C. Di Mauro, "Reshoring and Industry 4.0: How often do they go together?" *IEEE Engineering Management Review*, vol. 46, no. 2, pp. 87-96, 2018.

[2] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing Industry 4.0 cybersecurity challenges," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 79-86, 2019.

[3] S. Erol, A. Jäger, P. Hold, K. Ott, and W. Sihn, "Tangible Industry 4.0: A scenario-based approach to learning for the future of production," *Procedia CIRP*, vol. 54, pp. 13-18, 2016.

[4] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *Journal of Industrial Information Integration*, vol. 6, pp. 1-10, 2017.

[5] ENISA, "Industry 4.0 Cybersecurity: Challenges & Recommendations," [Online]. Available: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations, 2019.

[6] A. Petrillo, F. De Felice, R. Cioffi, and F. Zomparelli, "Fourth industrial revolution: Current practices, challenges, and opportunities," *Digital Transformation in Smart Manufacturing*, vol. 1, pp. 1-20, 2018.

[7] G. Corera, "Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz," *BBC News*, Apr. 12, 2021. [Online]. Available: https://www.bbc.com/news/world-middle-east-56722181.

[8] V. Joseph and M. Josephs, "Challenges in Cybersecurity for Industry 4.0," in *Innovation in Manufacturing Through Digital Technologies and Applications: Thoughts and Reflections on Industry 4.0*, Birmingham City University, pp. 61, 2018.

[9] J. Prinsloo, S. Sinha, and B. Von Solms, "A review of Industry 4.0 manufacturing process security risks," *Applied Sciences*, vol. 9, no. 23, p. 5105, 2019.

[10] P. Radanliev, R. M. Montalvo, S. Cannady, R. Nicolescu, D. De Roure, J. R. Nurse, and M. Huth, "Cybersecurity framework for the Internet-of-Things in Industry 4.0," 2019.

[11] A. Petrillo, F. De Felice, R. Cioffi, and F. Zomparelli, "Fourth industrial revolution: Current practices, challenges, and opportunities," *Digital Transformation in Smart Manufacturing*, vol. 1, pp. 1-20, 2018.

[12] D. Horváth and R. Z. Szabó, "Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?" *Technological Forecasting and Social Change*, vol. 146, pp. 119-132, 2019.

[13] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2," *NIST Special Publications*, pp. 1-247, 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[14] "What Are the Most Common Cyber Attacks?" *CISCO*, 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/securitcommon-cyberattacks.html.

[15] S. Gupta, Y. Wang, and M.

Czinkota, "Reshoring: A road to Industry 4.0 transformation," *British Journal of Management*, vol. 34, no. 3, pp. 1081-1099, 2023.

[16] S. Kinkel, "Industry 4.0 and reshoring," in *Industry 4.0 and Regional Transformations*, Routledge, pp. 195-213, 2020.