National Conference on Robotics & AI: The Future of Cyber Security |March 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Urgency of Operational Technology Cybersecurity in Current Times

Asst. Prof. Swapnali Kadge[*], Mr. Anant Kadge [**], Dr. Prakash Bhadane[***]
[*]*Department of Information Technology , K.L.E. Society's Science and Commerce College*
E-mail: swapnali.k@klessccmumbai.edu.in
[**]*IT Industry Delegate*
E-mail: anantkadge@gmail.com
*** *K.L.E. Society's Science and Commerce College*
E-mail: prakash.b@klessccmumbai.edu.in

Abstract:

In today's interconnected world, the reliance on operational technology (OT) has grown exponentially, driving industries such as energy, manufacturing, and healthcare to depend on digital systems to manage their operations. While this technological advancement has improved efficiency and productivity, it has also made these critical infrastructure systems vulnerable to cyberattacks. This research paper explores the significance of OT cybersecurity in current times and the reason it demands immediate attention.
Operations being backbone of any manufacturing economy, safeguarding it from growing Cyber threat is one of the essential challenges for every business. Operational Technology encompasses the hardware and software systems that monitors and control physical processes in industries such as energy, manufacturing, logistics, healthcare etc. As per Statista report, Global OT industries are the most targeted for cyber-attacks.

Keywords: *Cyber Security, Cyber threat, vulnerable, cyberattacks etc.*

---

1. Introduction

1.1 Background

Operational technology (OT) is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. Operational technology systems are found across a large range of asset-intensive sectors, performing a wide variety of tasks ranging from monitoring critical infrastructure (CI) to controlling robots on a manufacturing floor. OT is used in a variety of industries including manufacturing, oil and gas, electrical generation and distribution, aviation, maritime, rail, and utilities. OT security solutions include a wide range of security technologies from next-generation firewalls (NGFWs) to security information and event management (SIEM) systems to identity access and management, and much more.Industrial control systems (ICS) are a main component of operational technology. ICS includes different types of devices, systems, controls, and networks that manage a variety of industrial processes. The most common are supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS).

2. Literature Review

Some of the latest reports which suggest the increased importance of Cybersecurity:

- Current number of connected OT devices globally of over 12 billion will more than double to 27 billion by 2025 - IoT Analytics (2023)
- 82% of organizations with OT have a common cybersecurity team that looks into their IT and OT infrastructure and system. - ASEAN report
- Large businesses faced increased security risk from unsecured OT devices - ASEAN report

The threat landscape for OT systems has evolved significantly in recent years. Malicious actors,

including state-sponsored groups, criminal organizations, and hacktivists, have recognized the

potential for economic and political disruption through attacks on critical infrastructure. Incidents like the 2022 Ukrainian State Nuclear Power attack, Greek Natural Gas Distributor Attack- 2022 and 2020 Colonial Pipeline ransomware attack are grim reminders of the real-world consequences of OT security breaches.

Many organizations are turning to AI as an answer to tackle the cyber threats through its ever-

growing computational potential and different forms of learning. AI is playing a crucial role in

enabling analysis of substantial data sets, patterns and signatures, thereby influencing user behavior, to enable automated responses and facilitate workflows for cyber compliance. Generative AI using techniques like deep learning impersonates human properties and finds applications in various domains, including cybersecurity, with potential prospects and concerns. As per Gartner, more than one-third of surveyed organizations use AI powered Application Security tools.

3.Importance of OT Cybersecurity

OT security is essential to safeguard critical infrastructure, prevent financial losses, ensure safety, protect sensitive data and defend against a range of cyber threats. It plays a vital role in maintaining the stability and security of essential services and industries. Some of the key advantages that OT security provides are:

Necessity: Given the high stakes involved, addressing OT cybersecurity is no longer an

option; it's a necessity. Organizations should take proactive steps to safeguard their OT

systems:

Risk Assessment: Identify and prioritize vulnerabilities within OT systems to address the

most critical risks first.

Defense-in-Depth: Implement a multi-layered security approach that includes network

segmentation, access controls, and intrusion detection.

Employee Training: Raise awareness among staff about the importance of OT cybersecurity

and how to recognize and respond to potential threats.

Regular Updates: Keep OT systems up-to-date with security patches and updates, even if it

requires significant effort.

Collaboration: Foster collaboration between IT and OT teams to ensure a holistic

cybersecurity strategy.

Incident Response Plan: Develop a comprehensive incident response plan to minimize

damage in case of a cyberattack.

Consequences of OT Cyberattacks:

The consequences of successful OT cyberattacks can be catastrophic that ranges from financial

losses to disruption of business operations. Such consequences not just halt the business but make a huge impact on the cyber resilience culture of an organization. Below are some of the key impacts which affect the OT security of the businesses:

Operational Disruption: Shutdowns or malfunctions of critical infrastructure can have far-

reaching consequences, affecting the economy and public safety.

Environmental Damage: Attacks on industrial systems could lead to environmental disasters,

such as chemical spills or oil leaks.

Loss of Life: In healthcare settings, attacks on medical devices or systems can endanger Patient's lives.

Economic Impact: The financial losses associated with OT cyber attacks can be staggering,

impacting both organizations and the broader economy.

Conclusion

In conclusion, the importance of OT security lies in safeguarding critical infrastructure, protecting

public safety and mitigating the real-world consequences of cyberattacks. Organizations across

industries must recognize that OT security is not merely a technical concern but a strategic

imperative for resilience and sustainability in an increasingly digital world.

The current threat landscape demands immediate and sustained attention to OT cybersecurity. The

consequences of neglecting this critical aspect of modern infrastructure are too severe to ignore.

Organizations, industries, and governments must work together to secure operational technology

systems, ensuring the continued functioning of critical infrastructure in an increasingly digital world.

References:

1. Cyber Security Control Systems for Operational Technology - Industrial Control Systems - Wiley Online Library

2. The Crucial Role of Cybersecurity in Operational Technology | IEEE Conference Publication | IEEE Xplore
3. A cybersecurity assessment framework for virtual operational technology in power system automation - ScienceDirect
4. https://ciosea.economictimes.indiatimes.com/
5. https://en.wikipedia.org/wiki/Operational_technology
6. www.wikipedia.org
7. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
8. https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack
9. https://www.wsj.com/articles/new-data-show-broad-shift-to-remote-work-during-pandemic-
10. 11663214461
11. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
12. https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-
13. percent-of-boards-of-directors-view-cybersecurity-as-a-business-risk
14. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

