International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I2P113

Volume 69 Issue 2, 85-92, February 2021

Original Article

Convergence of IT and OT – Cybersecurity Related Challenges and Best Practices

Prashant Tyagi[1]

[1] *IEEE Senior Member, IEEE Computer Society Member, Scottsdale, USA.*

Received Date: 05 January 2021
Revised Date: 22 February 2021
Accepted Date: 25 February 2021

Abstract - *Over the past decade, Industries and Organizations, are increasingly embracing digital-first business strategy as they are reinventing their organizations, adopting and implementing newer technologies to help them succeed, gain a competitive advantage in an ever-changing business climate, increase the productivity of their employees, automate their processes and strive to provide a better and enriching customer experience. Digital Transformation initiatives in organizations and continuous automation of traditional manufacturing and industrial practices using smart modern technology have caused the blurring of boundaries between Operational Technology(OT) and Information technology(IT) and have catapulted organizations into the fourth Industrial Revolution (Industry 4.0). With this fusion of OT and IT, an organization's mission-critical systems face unprecedented cybersecurity-related threats, as this has led to the expansion of the attack surface. The security landscape is ever-changing, and the risks associated with it are also constantly evolving. The work in this paper discusses the cybersecurity-related risks and challenges[1] arising out of this convergence of OT and IT and the best practices and strategies organizations can adopt on how they can protect the integrity and availability of their complex automation solutions and achieve industrial security with a comprehensive approach just beyond the network security. This paper also discusses how organizations can address their current security gaps through digital risk function(digital risk management) to minimize business disruption and financial losses.*

Keywords - *Operational Technology(OT), Information Technology(IT), Industry 4.0, Industrial Revolution, Digital Transformation, Artificial Intelligence, Industrial Internet of Things(IIoT), Internet of Things(IoT), Robotics, Industrial practices, Genetic Engineering, Sensors, Hybrid Cloud, Deployment, Integration, On-Premises, Native Cloud, Architecture, Data, Modern Data Platform, Data Lake, Data Warehouse, Applications, Legacy Systems, Infrastructure, Resilient, reliable, Operationally Excellent, Performance Efficient, High Availability, Fault Tolerance, Scalable, Environments, Infrastructure, Systems, Applications AWS, Azure, Google, VMware, IBM, API, WAN, LAN*

I. INTRODUCTION

According to a recent survey conducted by IDC [2], more than a third of organizations have already started implementing a digital-first approach to business processes, operations, and customer engagement. As per this survey, most of the industries and organizations top objectives for their digital business strategy were to improve their process efficiencies through automation, make them operationally excellent, create enhanced customer experiences, improve employee productivity, to make their systems highly available, more reliable, more resilient, fault-tolerant, to increase their bottom lines and to maintain a competitive advantage of their position in the market. The advent of Digital Transformation has trusted organizations operating critical infrastructure into the fourth Industrial Revolution (Industry 4.0). This has led to the creation of new digital business designs, which has started causing the blurring of the gap between the digital and the physical universe. "Connected devices are increasingly flourishing as predicted, with the number of connected IoT endpoints set to top 40 billion by the end of 2021 and reach 80 billion by 2025 according to IDC [2]". This has given the organizations and manufacturing firms the ability to do ground-breaking innovations, the availability of information and data for analyzing and taking quick, actionable business insights, and helping them increase their operating efficiencies but has also caused the explosion of the modern attack surface. The Operational Technology (OT) that runs the critical infrastructure in industries and organizations is now connected to the outside world through sensors and are now converging these once-isolated systems with Information Technology (IT), which forms the backbone of most organizations as the 'air gapping or the 'physical distancing' between the two realms have started to decrease. With this fusion, today's enterprise-wide infrastructure face unprecedented cyber risk and threats across both IT and OT environments. As per a recent activity alert issued by National Security Agency (NSA) and Cybersecurity and

Infrastructure Security Agency (CISA), they have warned of increased malicious activity by bad cyber actors targeting internet-accessible OT and have recommended taking immediate actions by organizations and industries to reduce their exposure to operational technologies and control systems[3].

II. INDUSTRIAL 4.0 (THE FOURTH REVOLUTION)

> "Industry 4.0, also known as the fourth industrial revolution, is characterized by the end-to-end digitization of manufacturing and other industrial processes. Industry 4.0 initiatives create an interoperable and highly optimized ecosystem of machines and services, from the supply chain to the factory floor to delivery logistics. Industry 4.0 builds on the previous three industrial eras, spanning the 18th, 19th and 20th centuries, which encompassed such innovations as a division of labor, steam power, electrical power and the first stage of computer-based automation." [4]

III. OPERATIONAL TECHNOLOGY (OT) AND INFORMATION TECHNOLOGY (IT)

A. *Operational Technology(OT)*

According to Gartner Glossary [5], "Operational technology (OT) is the hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment's, assets, physical processes, devices, infrastructure, and events." Most of the shop floor and manufacturing sectors use heavy machinery and types of equipment to perform complex and a wide variety of functions like monitoring critical infrastructure, managing conveyor belts, controlling heat, temperature, and the like to control robots on the manufacturing floor. Operational Technology is the "IT word" for industrial computer systems. This form of technology is widely used in industrial settings like transportation(automated train systems), public infrastructure (controlling of flow of water through a canal), city operations (the concept of smart cities), energy services, scientific (automated weather stations, space stations), industrial services(production of materials as per batch control process algorithms), facilities and commercial buildings/office complexes (automated control valves for HVAC - Heating, Ventilation and Air Conditioning), manufacturing (controlling and monitoring of a production line), Data Centres to collect and store data to support various IT related functions (electrical rooms, generators, transformers, cooling modules used to power the data centers) just to name a few. In layman's terms, we can also refer to operational technology as the "IT in the non-carpeted areas" [6] or the IT that is used to control systems and machinery on the shop floor.

B. *Information Technology(IT)*

On the other hand, Information Technology (IT) refers to all aspects related to computer technology, including hardware like servers, network adapters, storage adapters, switches and software applications, emails, utility tools, services to store retrieve, manage, manipulate, transmit, deliver information such as data, video, voice, etc. Information Technology often constitutes the technological backbone of most organizations and companies. These type of devices, programs, algorithms, applications, and systems are managed by a group of people constituting the IT department, usually consisting of system engineers, maintenance and support engineers, architects who design systems, Extract Transform Load (ETL) developers, analysts[7] and data citizens who work with and manage data.

C. *Components of Operational Technology (OT)*

Industrial Control Systems (ICS) are the main component of operational Technology. ICS constitutes different types of devices, systems, controls, networks, and programs that manage a variety of complex industrial processes and functionalities. "The most common are supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS)" [8]. SCADA is a computer system used for gathering and analyzing real-time critical data. SCADA systems are used to monitor and control plant types of equipment, heavy machinery in manufacturing industries or other industrial settings like oil and petrochemical refineries, transportation and logistics, water and energy, environmental services and waste collection, telecommunications, just to name a few. How SCADA systems work is that as they detect a failure or abnormal functioning of a critical component (like a faulty valve, overheating of a component) in a piece of equipment or machinery, they report about this component failure to the main controlling home station, carrying out the necessary analysis and control, to determine if the unexpected behavior of the failed component is critical and displaying the information in a logical and a structured manner typically in the form of a graphical interface. SCADA systems can be relatively simple, such as the one that controls and monitors the environmental conditions like heat and temperature in a small office setting, or they could be increasingly complex to controlling the entire batch processing in a paint shop of an automobile manufacturing plant, or controlling all activities in a nuclear power plant or managing municipality activities like that of water, gas and power supply for the entire city[9]. On the other hand, "distributed control systems are digital automated industrial control systems that use geographically distributed control loops throughout the factory, machine or control area in the shop floor. A DCS has several local controllers located throughout the area that are connected by a high-speed communication network" [10]. DCS is also extensively used in industrial settings wherein there are no central operator supervisory controls such as in chemical plants, oil and gas refineries, water treatment plants, environmental control systems, nuclear power plant, packaging factories, waste, and recycling facilities, just to name a few.

D. Industrial Internet Of Things (IIoT)

The Internet of Things or IoT has most commonly being referred to as when numerous devices are being connected via physical objects called sensors over the internet, which makes sharing and access of information possible, in near real-time without any manual intervention. Because of the omnipresence nature of the wireless network and the widespread availability of inexpensive computer chips, adding sensors to these physical devices has caused a reduction in the gap between digital and physical realms. These devices can range from as small as a motion-activated or a smartphone-controlled lightbulb to something as big as the smart cities connected by billions of devices to control and understand the environment in an efficient manner. On similar lines, one can think of the Industrial Internet of Things or IIoT as interconnected devices with an array of sensors, actuators, controllers, monitors, and other technologies like remote processing units (RPU), programmable logic controllers(PLC)[7] that connect heavy machinery, types of equipment over Wide Area Network or over multiple Local Area Networks [10] and connected to the internet through internet devices such as routers.

IV. CONVERGENCE OF OT AND IT - PARADIGM SHIFT TO ENTERPRISE IoT

Organizations want to be able to analyze the data coming from these IoT devices connecting the critical infrastructure and be able to collate it with the data emerging from other systems and applications, store them in a hybrid-cloud, private/public cloud, on-premises datacentres, or a combination of both[10] and gain a holistic view of that data to gain critical business information and quick, actionable business insights. By embracing "smart and intelligent" technologies and sensors based on IoT, industrial and manufacturing companies are able to adopt various digital transformation strategies and initiatives, embrace disruptive technologies to help them make breakthrough innovations that are very pivotal to maintaining their continued strategic position and competitive advantage in this ever-changing business environment.

Artificial Intelligence (AI) and Machine Learning (ML) facilitate seamless communications between systems enabling them to make autonomous decisions without human interventions, and this is broadly labeled as M2M or Machine to Machine technology. In the new realm of the digital world, the terms IoT, IIoT, Big Data, M2M are now concurring towards Enterprise IoT. Organizations and Industries have various enterprise-wide systems like Enterprise Resource Planning (ERP),[7] Customer Relationship Management systems (CRM), Human Capital Management Systems (HCM), Supply Chain Management Systems (SCM) to support their processes, products, and services. Organizations want to encompass the synergies of convergence of OT and IT and create an Enterprise IoT platform to extend themselves from "not just optimizing the processes around production and distribution of the products and services but optimizing the products and services itself" through coherency and interconnectedness [12] to achieve operational efficiencies and performance excellencies. Enterprise IoT platforms in industrial settings then, due to the coaction and co-existence of OT and IT, can create rippling effects and encapsulate on the newer opportunities such as predictive maintenance, enriched customer experience leading to increase customer acquisition and customer retention rates, increase in Net Promoter Score(NPS), newer business models (pay as you go model as in the public cloud)[10] and easier data sharing across connected devices as shown in Fig.1.

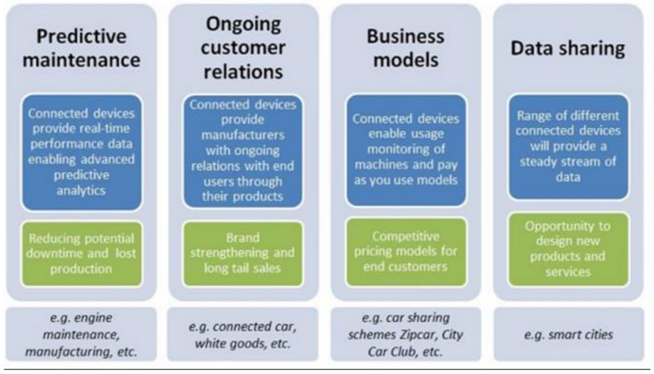
Predictive maintenance
Connected devices provide real-time performance data enabling advanced predictive analytics
Reducing potential downtime and lost production
e.g. engine maintenance, manufacturing, etc.
Ongoing customer relations
Connected devices provide manufacturers with ongoing relations with end users through their products
Brand strengthening and long tail sales
e.g. connected car, white goods, etc.
Business models
Connected devices enable usage monitoring of machines and pay as you use models
Competitive pricing models for end customers
e.g. car sharing schemes Zipcar, City Car Club, etc.
Data sharing
Range of different connected devices will provide a steady stream of data
Opportunity to design new products and services
e.g. smart cities

Fig. 1 Synergies developed by Enterprise IoT due to convergence of OT and IT[12]

V. CYBER-SECURITY RELATED CHALLENGES DUE TO THE CONVERGENCE OF OT AND IT

Traditionally, operational technology (OT) security was not that relevant in the past as OT systems were not connected to the internet. The recent advances in internet technology have caused the physical devices to be "smart," and as organizations and manufacturing industries bolted on specific point solutions to address specific business challenges or pain points which helped them to achieve operational efficiencies and increase throughput, it has also caused the 'air gapping between the industrial control systems like the Supervisory Control and Data Acquisitions(SCADA), Distributed Control Systems(DCS) and the information technology systems to decrease and thus adding more cybersecurity vulnerabilities into the systems and processes and a hack of the Enterprise IoT environment could cause lasting damage and have a crippling effect.

Having said that, the operational technology (OT) also faces the same cybersecurity-related challenges and threats like cloud risks, commodity ransomware threats, malware, spear-phishing to obtain initial access to the organization’s information technology(IT) network before pivoting to the OT network, DDoS (Distributed Denial Of Service) attacks, fragmented approach to vulnerability and identity access management across the enterprise. Typically, what we have seen till recent times in industrial settings is that OT networks and IT networks were kept separate, resulting in two separate security teams, each having their own siloed approach to managing and mitigating security vulnerabilities within their own network. This kind of isolated approach makes it an excruciating task then to identify what is happening across the entire modern attack surface to gain a holistic view of the network and the threat landscape and access the cybersecurity-related security posture of the environment. The benefits of IT and OT convergence are clear and so too is the need for IT and OT security. With greater connectivity, interrelatedness and interactions come greater risks, and they have to be managed and mitigated in a proper manner. Below we will look at some of the most common and important cybersecurity-related challenges manufacturing industries encounter when dealing with Enterprise IoT environments:

A. *Technical Skills Gap*

According to an online survey conducted by NTT security[13], lack of technical know-how and ownership are some of the top challenges facing operational technology(OT)security. “According to recent research by the Department for Digital Culture, Media & Sport(DCMS), around 6,53,000 organizations (48%) in the UK are unable to carry out basic tasks defined by the Govt Cyber Essentials Scheme like setting up the firewall, storing data, etc. The report claimed that 4,08,000 businesses (30%) are lacking advanced cybersecurity skills like Penetration Testing, forensics, etc. The report also says that 25% had complained that this had impacted their business.” [14]. Some organizations who have the right skills and resources to tackle these cyber threats and mitigate them face the new challenge of lack of ownership on whose areas of work would the OT security fall under -would it be the Engineering department or the IT security department? Organizations are investing heavily in their Customer-Digital initiatives and robust technologies but implementing these newer and advanced technologies requires access to highly-skilled, hands-on experienced, and trained technical resources.

B. *Artificial Intelligence - A Double-Edged Sword*

Implementation of artificial neural networks (ANN) and advanced machine learning algorithms into convolutional neural networks(CNN) have helped data citizens to build simulations and modeling to mimic the threat patterns and train the model to observe different behaviors in the vulnerabilities and identify the corrective and preventive measures that need to be taken and implemented. While this is a boon and can be used as a defensive tool, unfortunately, the same techniques can be used by hackers, phishers, or bad actors to re-engineer a crippling cybersecurity attack. A cyberattack on an OT physical device could have catastrophic and devastating consequences for organizations, not only causing the specialized equipment to be damaged (leading to expensive damage repairs), but also the damaged equipment/device could pose a safety and a health hazard[14]. Food packaging companies, for instance, could end up shipping unsafe food, or pharmaceutical companies could end up shipping expired medications and vaccines.

C. *Cloud Risks – Data Security*

As organizations are increasingly embracing disruptive technologies to support their digital-first business strategy and initiatives, they are moving their legacy data centers, applications, and systems to the native cloud, or a public/private cloud deployment models or a Hybrid-Cloud deployment model to make their systems highly available, fault-tolerant and resilient. Companies then still need to pay attention to the data security and encryption of that data, be it at client-side or server-side while at rest or in transit from one application to the other application or in between on-premises and in cloud-environment[11] as they may be dealing with highly confidential data, personally identifiable information (PII) and keeping this data safe could prove a very daunting task. A single data breach could mean vast amounts of high critical information going to the hands of malicious entities, foreign adversaries, bad actors like criminals, business rivals, and the like.

D. *Keeping physical devices and supporting applications patched and regularly updated*:

The physical devices and equipment in the shop floor or manufacturing facility may be connected with IIoT devices, sensors, and actuators that are connected to the internet, but they also have the underlying applications which receive this data from the sensors and stores them in the backend databases to present the information and data sharing to the analysts and citizens. These applications need to be maintained by IT or the OT security by applying regular patches, updates, hotfixes, releases to keep the applications and software up to date for supporting the front end physical OT devices and equipment's so that this software is not vulnerable to cyber-related threats and attacks.

E. Spear phishing and Malware attacks

Saboteurs may send phishing emails containing a malevolent link with the motive of gaining initial access to the organization's network or hack the network over which the manufacturing company's mission-critical infrastructure and physical OT types of equipment are connected. Generally, such links will be accompanied by a social engineering test and would require the user to actively click or copy-paste a unique resource link(URL)[15] into the web browser leveraging users' subconscious nature of the execution process. There is also specific nature of spear-phishing emails, which contain links when clicked upon by the user, would instantly download malware into the user's system, which would slowly crawl into the interconnected systems via the network, thus installing the bad virus into the company's network.

F. Ransomware Threats

As per the recent activity alert warning issued by the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA)[3], one of the other top cybersecurity risks is the ransomware threats. A ransomware attack would completely block access to the system or network, and once the hacker has been able to achieve this would then demand a payoff depending upon the criticality of the data, the company's business operations, and the size of the organization itself. Some ransomware would also encrypt data on the target systems or a large number of applications/systems in a network to initiate an interruption in the availability of the data or the service and the network resources. The attackers can withhold the decryption key and render the data stores in the databases (on promises/hybrid-cloud) and make the data inaccessible to anyone within the company. In such cases, besides the organization or the victim incurring substantial financial, productivity, and operation losses, there would also be additional intangible consequences attached to it like tarnishing of the brand and company reputation/image, low employee morale, customer churn, etc. to name a few.

G. Unprotected Endpoints

When companies adopt point-in-time solutions or solutions specific to addressing their business pain points which require them to provide real-time updates to external customers and also internally to their applications (allowing them to have remote access over the devices), minimal protections provided by these devices such as password authentication and authorization may be targeted by the adversaries and may be compromised. Saboteurs may try to gain access to the industrial environments directly through systems and devices exposed to the internet for remote access from external locations rather than through external remote services using remote gateways like VPN's, network access gateways, access control lists, Citrix, etc.

H. Lack of Visibility into the attack surface

According to a ' Cybersecurity in Operational Technology' report released by Ponemon Institute[17] in 2019, about 37% of the organizations who participated in the survey from various geographical regions like the US, UK, Germany, Australia, Mexico, and Japan have revealed that they reported a 'significant disruption' in their business operations caused by malware, 33% reported a cyber-attack caused' significant downtime,' 23% reported that they had been hit by nation-state attacks(typically funded by highly capable politically influenced cyber criminals)and 60% said that disruptive cyber-attacks are the ones they are worried most about. If manufacturing firms and organizations are not securing both their IT and OT environments, it can translate to significant blind spots, leaving critical infrastructure at risk. Security teams must be better equipped to eliminate blind spots across environments, understand which threats should be considered high-risk, and prioritize those for immediate remediation.

I. Communicating using most Commonly Used Ports and Standard Application Layer Protocols

Bad actors may try to initiate command and control capabilities over the commonly application/data communication protocols like HTTP(S), telnet, RDP(Remote Desktop), OPC (Open Communications Platform) and Modbus to name a few to disguise malicious actions as non-threatening network traffic. Adversaries may also exploit commonly used ports to adopt a detour over the firewalls or the network detection systems to blend in with the normal network traffic to go un-noticed and to avoid more detailed analysis, inspection, and troubleshooting.[16]. They may use commonly open ports like TCP (Transmission Control Protocol):80(HTTP), TCP:443(HTTPS), TCP/UDP(User Datagram Protocol):53(DNS-Domain Name System), TCP:23 (telnet), TCP:502(Modbus), just to name a few.

J. Use of Vendor Engineering Software and Program Downloads[3]

Malicious users may try to perform an operation like downloading a software program or unintended program logic on a device with the objective of leaving a long term adverse persistence effect on the physical OT devices to implement custom logic to disrupt response functions from operating properly.

K. Modifying Control Logic or Intentional change of system parameters[3]

The physical devices in the manufacturing facilities operate via some program control logic that dictate these devices on how, when, and what actions needed to be performed based on the code logic and certain defined set of parameters. Adversaries may try to modify these parameters used to control the industrial control system devices or may try to place a malicious piece of code in the system, which can cause the system to malfunction.

L. The complexity involved in the Enterprise IoT environment

Integration of various industrial control systems, consolidation of siloed systems, and the data generated from these devices into the information technology setting to gain a holistic view of the data for helping manufacturing firms and organizations take quick and actionable business insights could make the Enterprise IoT very complex and minor glitches in the operations of equipment or a device in the manufacturing facility could cost time, expense, and demand highly technical skills and resources as well.

M. Rebuilding IT Infrastructure

Integration of IT and OT may demand a rethinking of the organization's existing infrastructure and build a Modern Data Architecture Platform [10], hybrid cloud deployment models, edge computing deployment models which will support the sub-millisecond latency data transfer and user-responses when it comes to dealing with IoT data. When organizations are dealing with the collection and processing of large amounts of financial data and confidential customer data, then they are bound by federal regulations and compliance requirements as to how much data they can process locally and what data needs to be stored in archives as per their data retention policies. Public cloud infrastructures, although they provide flexibility and high availability they often strive hard to keep pace with the high data transfer speeds and latency, and in such cases, IoT edge computing and hybrid cloud deployment models would be the go-to solutions for most organizations.

N. Longevity and Life span of the Industrial Control Systems

As an increasing number of physical devices in operational technology setting are being connected with sensors and actuators and are connected to the internet, they are being made accessible remotely, they are being seen as slow and easily obsolete as newer and better versions of the devices would be in place. Digital gadgets and physical devices typically have a short lifespan and become outmoded easily. Organizations and manufacturing companies will have to continuously upgrade their systems, adding to increase CAPEX (Capital Expenditure) along with its continued OPEX(Operating Expenses) as well.

VI. WHY EFFICIENT AND EFFECTIVE OT SECURITY IS IMPERAMENT

Operational Technology (OT) Security is no longer an option that organizations have, but it is a necessity and a mandate to help manufacturing industries and organizations remain safe and compliant with the everchanging rules and regulations issued by several regulatory authorities. Cybersecurity attack, be it in the realm of OT or in the realm of IT, can have serious consequences and devastating impacts like loss of availability of mission-critical production systems(production systems going offline), causing a disruption in their business operations, processes, loss of productivity and revenues, damage to brand trust, intellectual property and also physical safety. "Unprotected devices, hacktivists, internal accidents ranks are considered as the top three threats when it comes to the cybersecurity-related challenges posed by the convergence of OT and IT, followed by the IT integration and its related challenges itself and the external supply chain and other partner threats. Industrial Control Systems(ICS) and IT cybersecurity is the topmost priority, and organizations are strengthening their cybersecurity posture with innovative OT security technologies that provide deep visibility and control across OT and IT." [18]

VII. MITIGATION STRATEGIES AND BEST PRACTICES

In this section, we will outline a few of the imperatives and best practices for an organization's digital risk function(digital risk management program):

A. Having an Operational Technology(OT) Resilience plan in place

Since the Ukraine Cyberattack of 2015[19], organizations need to have a backup plan in place by identifying system and operational dependencies, assigning roles and responsibilities for OT network and system restoration, remove unnecessary layers of processes and additional functionality which could induce new vulnerabilities in the system, back up "gold copy/master copy resources like product keys, product licenses, system configuration information, service level agreements and contracts, programmable control logics, intellectual property and storing all such critical information off-network in lock safe. Ensuring the right governance processes and policies are in place to take regular backups of the data and test/validate these data backups and processes in the event of a rolling back or data restoration from the back up due to a data loss circumstance due to cyber activity is very pivotal to ensure that a robust digital risk plan is in place.

B. Having a Robust Cybersecurity Incident Response Program in place

Given the state of heightened integration of IT and OT and the additional risks and exposure it poses, it is of paramount importance to have a well-exercised cybersecurity incident response plan in place that is developed, mock-tested, simulated and socialized/communicated with the stakeholders before an actual incident occurs. Identifying the key decision points in the response plan and who among the executive personnel have the necessary decision-making authority will go a long way in the event of an actual malicious attack. Simulation of the actual threat in the Enterprise IoT(using threat simulation tools like SD elements from Security Compass, Attack IQ platform, Avalance, Cymulate, AWS Fault Injection Simulator, to name a few) will help organizations gain visibility to the possible cyber threat attacks and the readiness action that needs to be in place in the situation of an actual event. The motive behind this exercise is to obtain an answer to the question ‘What can go wrong?’ There is no single comprehensive list that enlists all the possible threat scenarios as the threat depends on the workload, use case under consideration, among other factors like geographical location, type of industry, and the like.

C. Having a Trusted, Reliable Managed Services Security Provider in place

They are like the gatekeepers and the security guards of the organization’s digital footprint. This managed security software from the vendors provides unified visibility, security, control of converged infrastructures, monitoring capability of both OT and IT networks, and assesses OT assets by intelligently and smartly scanning the IT) based assets in the OT environments. These security solutions also provide some metrics based Key Performance Indicators (KPI’s) like threat-based vulnerability score optimized for both IT and OT assets by taking into account the severity of the vulnerability combined with the existence of public proofs-of-concept (PoC), Dark Web chatter, the emergence of exploit code in exploit kits and more. This rating provides greater, risk-based intelligence for security teams to prioritize remediation or mitigation of critical flaws. These tools also have the capability of conducting adaptive assessments(for gaining deep situational insights into the OT network and OT devices), extended depth and breadth of covering all OT devices, industrial controllers and security protocols, community intelligence (utilizing open source threat intelligence pulled from the security community for real-time updates). This managed security software allows organizations supporting critical infrastructure to benefit from the efficiencies and cost savings of interconnecting their IT and OT environments without introducing unnecessary and unacceptable risk. Security Analysts and other users of this software would be well equipped to face the era of IT/OT convergence by continuously managing, being able to detect the blind spots, measuring and reducing cyber risk to improve security posture.

C. IT and OT integration Software to enable Digital Thread and OT/IT System Health Monitoring

To make informed decisions and maximize business results, organizations must gain real-time visibility into every aspect of performance across their factory operations. With some software like FactoryTalk- Innovation Suite[21], manufacturers can easily access, understand and leverage the data needed to make informed decisions. This suite of software has inherent capabilities that can improve connectivity to operational technology (OT) devices on the plant floor, natively supporting the rapid, scalable, and secure connection of the most commonly used industrial equipment. Combining plant floor operations with data from information technology (IT) applications and systems, decision-makers can now have a complete digital representation of their industrial equipment, lines, and facilities from anywhere in the enterprise. This software also has coherent features which allow customers to virtually test machine and system designs in a digital twin format before incurring manufacturing and automation costs and committing to a final design. It also has remote assistant tools, which help customers avoid safety and compliance risks, accelerate problem resolution, reduce the cost of onsite technician visits, improve machine uptime and operational efficiency and overcome the pressure of the ever-increasing worker skills gap. One of the recent additions as per Factory Talk[21] is the FactoryTalk Edge Gateway, which leverages FactoryTalk Smart Object capability to automatically capture high-speed, contextualized OT data from industrial controllers, packaging the data in a common information model that can be configured by control engineers. This standard information model can be efficiently mapped to on-premises or cloud applications to generate predictive insights and operational excellence across the enterprise. This integration tool which can enable organizations to create a digital thread, allows organizations to improve their supply chain visibility, shorten production cycles and reduce production variability, inventory, and indirect labor costs.

D. Hardening Organization’s Network

Putting best practices to action like minimizing external exposure through remote connectivity to OT networks and devices, eliminate access to IP addresses that do not have a legit business reason to communicate with the OT physical device, securing all required user account, and remote access accounts using multifactor authentication[11], strong password policies(length, complexity), taking a defense-in-depth approach and adopting a multi-layered identity and security management approach can make the boundaries arduous for penetration for the adversaries. Implementing secure network architectures utilizing dematerialized zones(DMZ’s), filtering network traffic to allow only IP addresses that have genuine business needs, capturing and reviewing access logs from these OT systems, using publicly available tools such as Shodan[3] to locate internet-accessible OT devices will help manufacturing firms and organizations secure their critical infrastructure and mitigate the potential impact of the cybersecurity-related threats.

E. Having an accurate and a detailed “As-Operated” OT network map in place[3]

Using publicly available tools, such as Wireshark, NetworkMiner, Grassmarlin,[3] and/or other passive network mapping tools, documenting and validating the tools and procedures in place to identify OT asset, creating OT asset inventory, identifying all communication protocols which have been used across the OT networks, taking immediate action on illegal or unauthorized OT communication accesses and documenting all external communication and access to and from networks can help in laying a strong foundation for a sustainable cyber-risk reduction effort.

VIII. CONCLUSION

The increasing adoption of disruptive technologies has led to organizations embracing digital-first business strategy to achieve completive advantage and maintain their strategic position in an ever-changing business climate. These disruptive technologies not only have caused the expansion of the IT realm but also the OT universe, which connects industrial control systems and physical types of equipment/devices via sensors, actuators, senor communication systems, Wide Area Networks(WAN's), Local Area Networks(LAN's), embedded systems, real-time operating systems, energy-harvesting resources, micro-electro-mechanical systems(MEMs) to name a few. This had led to the convergence of the OT environment with the IT environment creating an Enterprise IoT, the synergies of which have helped companies achieve enriched customer experience and increased operational efficiencies. Nevertheless, such convergence has also caused siloed IT and OT security practices resulting in significant blind spots, thus limiting the organization's ability to detect vulnerabilities and prevent attacks. By having robust security and incident response program in place and having security practices around Governance (Strategy and metrics, education and guidance, policy and compliance), construction(assessing security requirements, threat assessment, and secure security architecture), validation(design reviews, attack simulations) and implementation(environment hardening, vulnerability management, and operational enablement), manufacturing firms and organizations can achieve a comprehensive, unified vulnerability management platform so that they can stay one step ahead of attackers and adversaries.

IX. REFERENCES

[1] Prashant Tyagi., From Project Manager (PM) To Technical Project Manager (TPM) In the Journey to an Agile Organization International Journal of Engineering Trends and Technology11(1)(2021)4. https://www.ijcotjournal.org/archive/ijcot-v11i1p302.

[2] IDG|ExecutiveResearchFirmStateofDigitalTransofrmatin(2018) https://cdn2.hubspot.net/hubfs/1624046/Digital%20Business%20Executive%20Summary_FINAL.pdf.

[3] Cybersecurity & infrastructure Security Agency National Cyber Awareness System Alerts NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems|https://us-cert.cisa.gov/ncas/alerts/aa20-205a

[4] StanGibson|TechTarget|IoTagenda|IT/OTConvergenceishardworkhere'swhyit'sworthit|https://internetofthingsagenda.techtarget.com/feature/IT-OT-convergence-is-hard-work-heres-why-its-worth-it

[5] GartnerGlossary|InformationTechnology| https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

[6] OperationalTechnology|https://en.wikipedia.org/wiki/Operational_technology.

[7] Prashant Tyagi ., Diagnostic, Descriptive, Predictive and Prescriptive AnalyticswithGeospatialData., InternationalJournalof Computer TrendsandTechnology 69(1)(2021)1822. https://www.ijcttjournal.org/archives/ijctt-v69i1p104.

[8] Fortinet|WhatisOperationalTechnology(OT)|https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security

[9] Vangie Beal|Home|Definitions|SCADA-Supervisory Control and Data Acquisition|https://www.webopedia.com/definitions/scada/

[10] TechTargetNetwork|What is distributed control systems(DCS)|https://whatis.techtarget.com/definition/distributed-control-system

[11] Prashant Tyagi, Sharada Devi P. P., A Functional View of Hybrid-Cloud Environment – Use Cases and Best Practices, Computer Science and Engineering 11(1) (2021) 9-16. doi:10.5923/j.computer.20211101.02|http://article.sapub.org/10.5923.j.computer.20211101.02.html

[12] TechTarget|IT/OT convergence is necessary, desirable but not so simple|Ehandbook|https://searchsecurity.techtarget.com/ehandbook/IT-OT-convergence-is-necessary-desirable-but-not-so-simple

[13] NTT|Optimized for agility embracing the hybrid future|https://hello.global.ntt/

[14] Ruchika Tyagi|Teceze|Digital innovation & Excellence| Cybersecurity .Challengesin2020andhowtotacklethem|https://www.teceze.com/cybersecurity-challenges-in-2020-and-how-to-tackle-them/

[15] MITRE|ATTACK|Home|Techniques|Enterprise|Phishing|Spearphishing Links|https://attack.mitre.org/versions/v7/techniques/T1566/002/

[16] MITRE|ATTACK|CommonlyUsedPort|https://collaborate.mitre.org/attackics/index.php/Technique/T885

[17] Computerweekly.com|Critical Infrastructure under relentless cyber attack|https://www.computerweekly.com/news/252461202/Critical-infrastructure-under-relentless-cyber-attack

[18] Computerweekly.com|Operational technology security improving, but attack surface continues to grow, https://www.computerweekly.com/news/252464954/Operational-technology-security-improving-but-attack-surface-continues-to-grow

[19] December2015Ukraine PowerGrid Cyber Attack, https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

[20] https://www.securitycompass.com/sdelements/

[21] RockwellAutomation|MES,AnalyticsandIIoT |https://www.rockwellautomation.com/enus/products/software/factorytalk/innovationsuite.html