



This white paper originally appeared in Automation Alley's 2020 Technology in Industry Report

# Opportunities & Challenges of IT & OT Convergence

Written by:

**David Schippers, Sc.D, CISSP, EnCE**

*Chair & Assistant Professor, Information Technology  
Decision Sciences  
Walsh College*

**Michael Simko, Sc.D., CGEIT, CISSP, CISM**

*Adjunct Assistant Professor, Information Technology  
Decision Sciences  
Walsh College*

**Elliot Forsyth**

*Vice President, National Cyber Security Program  
Michigan Manufacturing Technology Center*

**George Pappas, Ph.D.**

*Assistant Professor, Embedded Systems & Cybersecurity  
Department of Electrical and Computer Engineering  
Lawrence Technological University*

A background image for the quote section showing silhouettes of two people in the foreground, looking at a large industrial facility with various pipes and structures. Overlaid on this are several circular icons: a gas pump, a truck, a flame, a globe, and a gear. The entire scene is connected by a network of lines and dots, suggesting a digital or interconnected theme.

“Bringing these two teams together in any project is critical not only for its success but for its ability to scale across an entire enterprise.”

– Matt Wells, Vice President, Product Management, GE Digital



**T**he lens of 2020 and Industry 4.0 illustrates an evolving digital ecosystem where traditional information technology (IT) and operational technology (OT) converge at data entry points (the edge). The Industry 4.0 environment brings new sensors, networked devices and digital components to the manufacturing process at unprecedented levels (Barrios, Schippers, Heiden & Pappas, 2019). Evolutionary forces within Industry 4.0 presents both challenges and opportunities for advanced manufacturing through convergence of IT and OT with cybersecurity and cyber resiliency (Barrios, Schippers, Heiden & Pappas, 2019).

Traditionally, IT and OT have held separate roles within organizations. IT is often associated with data protection, data assets, business applications and data privacy, ensuring and enabling business operations. OT is often associated with availability, functionality and operational capabilities, ensuring ongoing operation of manufacturing systems. As the Industrial Internet of Things (IIoT) brings the promise of enhanced production, quality and efficiency benefits to the manufacturing process and supply chain (Barrios, Schippers, Heiden & Pappas, 2019), IT and OT are merging (converging) disparate technologies, processes and devices into a unified whole. Data and data protection within IT are converging with OT control, monitoring and sensor data, creating new and digital ecosystems (environments). Convergence is associated with both physical and virtual worlds, enabling digital twins, virtual prototyping and rapid deployment to market (Schippers, 2019). The digital ecosystem and convergence of IT and OT, along with physical and virtual worlds, creates untold opportunities and challenges for Industry 4.0. IT and OT convergence impacts people, processes and technology within Industry 4.0 ecosystems.

## People

### Now

Despite technology's role as a catalyst for Industry 4.0, people choose the processes and technologies adopted in their manufacturing organization. People define the role of each technology factor within their organization to obtain perceived benefits (NIST, 2018). IT and OT practitioners have evolved over time based on their educational

backgrounds, industry demand and ongoing comprehension of protection mechanisms (Harp & Gregory-Brown, 2015). In addition to the convergence of IT and OT technologies, the convergence of people associated with IT and OT will drive the realization of benefits to manufacturers.

With OT leveraging equipment with long life, custom network protocols and infrequent updates,

OT has historically approached cybersecurity from a survivability and availability perspective, also referred to as cyber resilience. OT devices are at high risk of disruption from a cyber event. Next generation ransomware will be holding industrial control systems hostage using cyber resilience attacks.

As the IIoT has brought significant change to the manufacturing landscape (Barrios, et. al., 2019), OT's role in the enterprise is shifting from one of solely operational functionality to data sources within the connected supply chain. Custom network protocols are disappearing, merging manufacturing technology into standard IP protocols (Harp & Gregory-Brown, 2015). Confounding the overall role of OT, Industry 4.0's expansion into data gathering and utilization throughout the supply chain is fundamentally transforming manufacturers' OT roles from operational and safety to operational, safety and data acquisition capabilities. Instead of a prime focus on cyber resilience, OT is entering into the IT cybersecurity arena. With changes mirroring standard operations within the IT infrastructure, OT is being forced to assimilate new approaches in standard operations. OT networks focusing on real time communications for operation and safety are required to transmit data for analysis and process improvement (Harp & Gregory-Brown, 2015). Ironically,



OT talent is forced to assimilate IT approaches and IT talent is being forced to consider OT approaches. Fundamental shifts are pushing IT/OT personnel and leadership approaches into uncharted territories of convergence for their previously isolated pillars.

The National Defense Industry Association (NDIA) completed a study on security implementations within the manufacturing supply chain in July of 2018. The study focused on the Defense Federal Acquisition Regulations Supplement (DAFRS) based on the National Institute of Standards in Technology (NIST) 800-171 publication. Despite the study's focus on DOD regulations in manufacturing, the study provided insights into supply chain implementation of new requirements and technologies.

Within the report, most small to medium-sized suppliers do not understand cybersecurity's impact on manufacturing capabilities. The respondents understood the need to protect intellectual property and IT operations, but saw little support in securing the operational aspects of their business (NDIA, 2018).

With additional sensors and data collection points within the manufacturing process associated with Industry 4.0, security impacts convergence by enabling ongoing operations and safety within the manufacturing process. Survey respondents found the NIST cybersecurity documentation

for securing operations to be confusing (NDIA, 2018).

The NDIA (2018) provided analysis on types of adopters within the supply chain. In the book "Crossing the Chasm," Moore (2014) described different groups of adopters as: innovators, early adopters, early majority, late majority and laggards. The real fulcrum point in groups is associated with the gap between early adopters and early majority (NDIA, 2018). Early majority groups are very pragmatic in approaches and risk adverse (NDIA, 2018). When considering the implications of convergence, a lack of comprehension, financial impacts and no identified roadmap fuse into an arena of unknown risk in the minds of the early majority. Leaders in the early majority, late majority and laggards' groups are risk averse, failing on some level to comprehend both cybersecurity and cyber resilience's roles dictating successful convergence for benefit realization. Supply chains will be limited by the vulnerability of their weakest link member, which may lead to increased opportunities for business that successfully address cybersecurity and cyber resiliency.

Illustrating the "chasm" impacts, the Verizon Breach report (2014-2019) provided a view into trends. In addition to the manufacturing sector, utilities and transportation are faced with similar challenges for convergence and security enabling ongoing operational ability. (Figure 1)

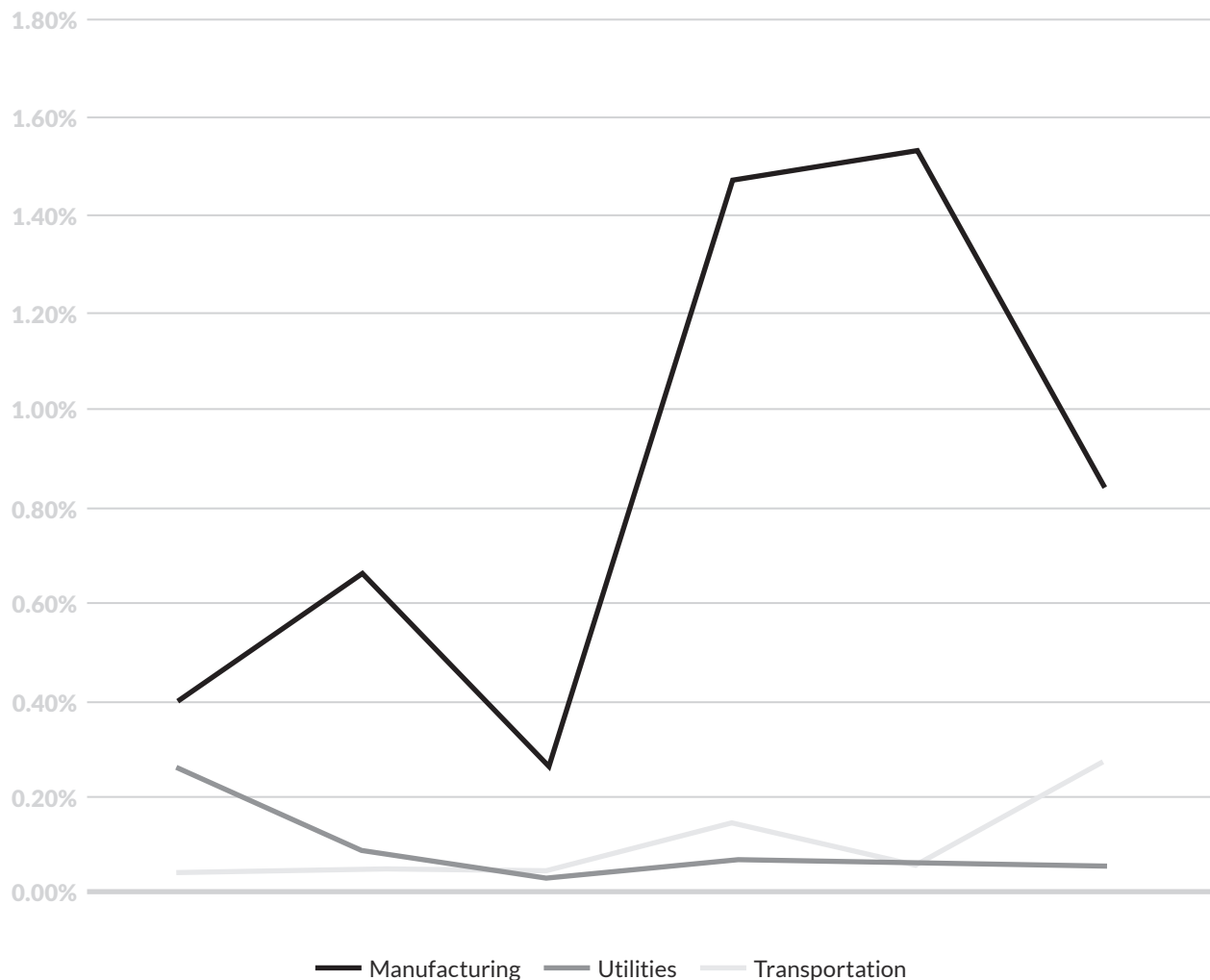
Notably, breach data varies in the total reported each year, necessitating a percentage review for overall shifts across industries. Contrasting utilities and transportation, the manufacturing industry is targeted often and reporting more breaches. A cyber event in any part of that chain can prevent the business from functioning.

IT and OT perspectives do not differ solely in comprehension or leadership vision. From an educational perspective, IT and OT practitioners commonly originate from very different backgrounds. IT practitioners typically obtain an information technology or cybersecurity-based degree for entry into the field. Outside of formal education, some practitioners leverage certifications or a combination of both certifications and degrees for entry into field. OT practitioners typically originate from a computer science or engineering background, often leveraging cybersecurity certifications to augment their educational background. Each educational and skill development path provides a focus for approach and deliverables in defending and maintaining operations.

As concerns have grown for cybersecurity adoption in the manufacturing space, a number of approaches have been considered, including legislation. New legislation, research and training will have little impact



Fig. 1: Percent of Breaches in Manufacturing, Utilities and Transportation (Verizon Breach Reports, 2014-2019)



without understanding the underlying issues in adoption: comprehension of cybersecurity and cyber resiliency risk strategies. If traditional approaches are leveraged for convergence of IT and OT, organizations will struggle. Current comprehension is fundamentally born of segregated workforces with segregated educational paths. IT

and OT cultures differ significantly, including funding, approach and expertise. Risk approaches in IT and OT differ significantly based on operational approaches with OT being extremely risk adverse. Realistically, leadership needs to drive a merger of approaches, staff, budgets and integration, leveraging non-conventional and organizational views. Based on

very different risk approaches, risk strategies, management and policies need to consider both arenas in a fundamentally new way. Manufacturers looking to leverage the innovation and opportunity envisioned with Industry 4.0 have to significantly reconsider many different approaches for a pathway to success.



## Future

IT and OT convergence will drive innovation opportunity and success for supply chains. As outlined in the World Economic Forum's (2018) future of jobs, innovative new skills and hybridization of disparate skills will be required by people to usher in convergence of IT and OT. Convergence will require supply chains to identify new approaches in training, education, leadership and risk management (WEF, 2018). "Crossing the Chasm" (Moore, 1991) provides great insights for predicting the future.

### Supply Chain Fragmentation

Innovators and early adopters will enable leadership and cross functional teams integrating IT and OT staff. Leaders who bridge people, skills, budgets and people integration gaps will thrive. Bridging these gaps will require significant effort to redirect overall vision and strategy across disparate groups, employing teams unconstrained by organizational norms (Zenko, 2015). Manufacturers integrating a unified vision of convergence from executive leadership to tactical players in their organizations will lead in Industry 4.0 advancements and benefits. Innovators and early adopters will also drive and accumulate the most talented group of IT and OT staff. Accumulation will originate from a combined effort of comprehension of convergence,

cybersecurity, cyber resilience and data driven acquisition throughout the supply chain. Human capital will be generated through retraining and obtaining fresh talent from educational institutions, internal efforts and industry groups. Risk averse supply chain players will cling to their market shares, while innovators will expand and overtake market rivals.

### Education Pipeline

In addition to manufacturer challenges with IT and OT convergence, education will face

**IT and OT convergence will be driven by many people factors. People factors will not solely drive critical change.**

significant challenges. The education pipeline will grapple with massive innovation requirements, while simultaneously being shackled by education's risk adverse approach (Horn & Dunagan, 2018). Horn and Dunagan (2018) indicated innovation requires separate teams outside of the organizational structure to drive meaningful impact, unchained from organizational road blocks. Just as the supply chain will fragment, education will be faced with merging historically disparate disciplines into hybrid education programs or cling to risk averse models. Depending on the size and role of an institution, education will approach Industry

4.0 from different perspectives. The Department of Education and accreditation bodies have focused on seat time and input drivers for quality assessments, impeding institutions hoping to embrace innovation and deliver graduates with impactful skills (Horn & Dunagan, 2018).

Small and medium-sized manufacturers with limited resources requiring retraining and innovative education for workers will gain a competitive edge by partnering with leading higher education institutions. Larger colleges and universities will see little value in customizing education for small and medium-sized business, clinging to established practices and research methodologies. Small and medium-sized colleges interested in innovation and relevancy will be more receptive to Industry 4.0 workforce requirements. Innovative institutions will create programs from holistically new approaches to subject matter, meeting hybridization instead of a conglomeration of existing courses. Pockets of institutions partnered with businesses/manufacturers will emerge, ushering in new careers, skillsets and hybrid education paths.

IT and OT convergence will be driven by many people factors. People factors will not solely drive critical change. Convergence will be heavily impacted by the processes people integrate into their organizations.

# Processes

## Now

Decades of separate evolution in both IT and OT created unrelated processes and technologies managed by isolated teams. Convergence challenges exist in many smart manufacturing firms across the globe. Conflicts between IT and OT arise from different priorities, inherently part of each group. Successful integration of IT and OT promises significant advantages, such as in performance, flexibility, and cost and risk reductions.

Reorganizing human capital into unified IT/OT teams enables new visions of cybersecurity and cyber resiliency through cross training and holistic defensive strategies. Strategic alignment at executive levels is another step towards successful unification. Joint IT and OT teams can share a variety of domain knowledge and expertise, achieving unification. Comprehension of similarities and differences between IT and OT will promote a more cohesive and risk aware culture for convergence.

Successful IT/OT convergence will require proactively planning and promoting security during each stage of system and software development life cycles to ensure each of the technology enhancements brought by Industry 4.0 negate any security risk the company is not willing to

accept. Organizations investing resources in overcoming the differences between disparate OT and IT groups will gain a significant competitive edge over their peers. IT and OT will explore new opportunities, facing challenges and difficulties. Despite short term issues, the long-term benefits of IT and OT convergence is an investment that will pay off for organizations navigating uncharted waters.

As we witness rapid adoption of automation, most companies have failed to take appropriate steps to safeguard information critical to their and their customers' businesses. There are a multitude of applications, dependencies and connection points required to fulfill business needs today and

tomorrow—all of which add complexity.

According to Ron Ross (Aitoro, 2019), Computer Scientist and Fellow at the National Institute of Standards and Technology, “complexity is the hackers’ best friend. We literally are hemorrhaging critical information about our key programs. They’re coming after you every day. They’re either going to bring down your capability or they’re going to steal stuff from you...” Supporting Ross’s statements, the FBI reported the negative financial impact of cyberattacks to the U.S. in 2017 was \$60 billion USD. By mid-2019, that amount topped \$1 trillion USD and continues to grow at unprecedented levels.





Being prepared when an attack occurs is the best way to mitigate potential damage and operational impact. The hard cybersecurity problems are buried below the water line in the hardware, software and firmware.

As IT and OT converge within the business, they must consider the implications of cybersecurity vulnerabilities. There are a number of standards being deployed from government and industry sectors to include: NIST 800-171, AIAG Auto 3rd Party Information Security, PCI, PII, ITAR, State legislative requirements, etc. For the small to medium-sized businesses, this creates a morass of acronyms. Luckily, there are cybersecurity solutions available to help manufacturers of all sizes protect themselves from cyber threats and prepare for the brave new world of Industry 4.0.

### **The NIST Cybersecurity Framework**

The National Institute of Standards and Technology (NIST) has developed a solid cybersecurity framework that includes a series of guidelines and best practices for dealing with potential cybersecurity threats. More importantly, it is accessible to all organizations, not the least of which includes small to medium-sized businesses. It can be applied to organizations whose cybersecurity is focused on IT, industrial control systems, cyber-physical systems or connected devices more generally including the IoT.

According to Ron Ross (Aitoro, 2019), “the Cybersecurity Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties” and that its “outcomes serve as targets for workforce development and evolution activities.”

The Framework provides for on-going cybersecurity resiliency providing that leadership embraces it as a portion of its on-going Risk Management process.

The framework lays out five basic activities, or core principles, that can be used to achieve a more

secure operation. The functions aid organizations in expressing management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats and improving by learning from previous activities, the framework notes.

Additionally, they align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, if an agency makes investments in planning and exercises, it can support timely response and recovery actions, resulting in reduced impact to the delivery of services.





The five functions of the NIST Cybersecurity Framework are:

1. **Identify** - This function expressly deals with understanding potential cybersecurity risks to an organization, including its systems, people, assets, data, capabilities and networks. The primary question is: what must be done to manage existing risks and mitigate the potential for damage?
2. **Protect** - Naturally, understanding leads to taking action—which is the protection aspect of the framework. This is where a manufacturer must develop and implement safeguards for its operations or services.
3. **Detect** - A proper monitoring system must be put in place to identify either a recent or ongoing cybersecurity event. The timely discovery of these attacks are crucial to a successful security strategy.
4. **Respond** - Upon discovery, every manufacturer must have controls available to respond accordingly to an attack. This includes functionality to block attacks or users with capabilities of regaining access to a system(s). This functionality is a bit different for manufacturers, as most providers use only limited networks or wireless connectivity. Industrial-quality access controls are necessary to monitor not just internal processes and systems, but also that of vendors and involved partners. Dynamic, real-time policy enforcement is essential across the entire network, and not just for local operations.
5. **Recover** – Essentially, the same as data or systems recovery, this function deals with the restoration of impaired or damaged services and content. Another aspect of this is opening up communications with clients or customers to reveal the impact of an event. Ideally, it would also include follow-up measures to prevent future attacks.



Of course, the NIST cybersecurity framework is nuanced and will have to be adapted to each company. There are also several implementation tiers, starting with partial at the lowest and ending with adaptive at the highest, that signal the preparedness of a manufacturer or organization when it comes to cybersecurity.

The convergence of IT and OT requires organizations to be cybersecure. The best course of action to get your company cybersecure—or to find out just how vulnerable it is—is to work with experts in manufacturing cybersecurity and the NIST framework.

## Future

Manufacturing processes, cycle time reductions, inventory levels, product mix, staffing and innovation transformations will

accelerate over the next five years as new technologies and trends transform the manufacturing industry in a profound way. Automation is and will continue to improve supply chain flexibility and ease labor constraints. According to the 2019 Sikich Manufacturing Report, deemed by CEOs, top practices in the next five years being deployed in the supply chain are:

- Collaborative design with customers
- Sharing forecasts with suppliers
- Technological certification of major suppliers – particularly related to information protection of intellectual property and personal property

Successful innovation will incorporate transformations bound with cybersecurity and cyber resilience measures, as defined by NIST standards outlined above.

Innovators will engage with experts to ensure cybersecurity and cyber resilience issues are addressed early and treated as a critical risk, prioritizing cyber risk management from executive leadership to edge.

Cybersecurity policy, procedure and preventative controls must be clearly articulated and implemented for new technologies, while providing a defense in depth strategy. Identity and access management in conjunction with encrypted data will contribute to maintaining the confidentiality, integrity and availability of manufacturing information and operational technologies. Incorporating cybersecurity through each phase of the system development lifecycle will help reduce security flaws, gaps and reduce risk to an acceptable level with the manufacturer's risk appetite.





# Technology

## Now

Technology, innovation and synergy are all contributing factors to the evolution of both IT and OT. IIoT technology transitions and the movement to Industry 4.0 can reap benefits, but also lead to gaps in cybersecurity (Barrios, et. al., 2019). Improper security can lead to additional risks and costs. Understanding the similarities and differences between IT and OT is imperative to address these gaps. Industry 4.0 will evolve current IIoT solutions, fostering new capabilities and security risks in manufacturing operations.

According to the Industrial Internet Reference Architecture (IIRA), the industrial Internet is various personnel and systems such as computing devices and machines which empower industrial operations (IIC, 2018). IT can range from storage systems, computing technology, business applications to even data analysis. A few examples of OT specifically correlate to machinery, equipment, assets, monitoring and control systems, programmable logic controllers (PLCs), Remote Terminal Units (RTUs), Supervisory Control & Data Acquisition (SCADA) systems and more. The primary differences are the functions each IT or OT device performs.

Converging IT and OT together brings forth several benefits to

include but not limited to the reduction of mechanical errors, operational costs and project completion time. Additionally, convergence leads to heightened benefits of Big Data, optimization of business process and enhanced insight for decision makers (Writer, 2017). IT and OT benefits articulate clear advantages and advancement, but what about the security flaws imminent between each digital ecosystem?


Past and current manufacturing technologies present various vulnerabilities, including software, hardware and configuration issues (DHS, 2011). Proprietary protocols initially established to operate on isolated enterprises are now connecting to the Internet (SANS, 2019). According to the SANS 2019 State of OT/ICS Cybersecurity Survey, 34.5% of control networks have internet connectivity and 64% utilized third party infrastructure or business's intranet, expanding the threat landscape significantly. The SANS (2019) survey also indicated control systems security incidents have risen from over 35% in the year 2017 to nearly 38% in 2019 (Filkins & Wylie, 2019). Incidents were not only linked to transition to internet connected solutions, but also due to the increase in destruction and disruption-oriented attacks performed by both organized crime and foreign nation states. Despite

IT and OT union attempts, the lack of convergence from OT and IT technicians (regarding people and processes) is underwhelming, resulting in gaps of communication, understanding and security (SANS, 2019).

## Future

While many manufacturers have begun implementation of embedded computing and IIoT, not all sensors or technology has fully transitioned. As IT and OT progress, a standardized and centralized approach will be imminent. The lack of IT and OT integration may be addressed through horizontal and vertical integration. More specifically, bringing together several sections from the enterprise and manufacturing line will only enhance productivity.

Industry 4.0 horizontal and vertical integration brings more centralized and universal integrated networks, enabling automation and united departments, processes and operations. While manufacturers have used robotics technology for many years in production, more advanced and autonomous robots are being developed, requiring security integration. As technology matures over the next 15 years, robots will continue to become more



engaging, autonomous, adaptable and collaborative. Like any technology medium, robotic software and hardware solutions should be built with embedded preventative controls and cybersecurity implementation within planning and development stages.

Cyber resilience and the theory of through-life cyber resilience can help address emerging trends and associated security issues through implementation of a product's complete lifecycle, emphasizing cyber resilience governance, systems development processes and cyber resilience mechanisms (Theron, 2018). As security re-

quirements vary for different IT and OT devices, incorporation of cyber resilience from the system development phase to decommission will instill necessary security controls required for effectively managing risk. Cybersecurity and cyber resilience designed through strategic risk management merged with artificial intelligence and machine learning for threat/anomaly detection will have significant impacts in manufacturing.

Industry 4.0 will need to address rapidly changing technologies. Despite ongoing presence, robotics in manufacturing will be a major growth area for cybersecurity vendors (FMI, 2019). Similar to

other manufacturing technology, many different vulnerabilities exist, setting large growth projections for cybersecurity solutions. With open positions and a limited talent pipeline for cybersecurity, artificial intelligence and machine learning will propel forward in cyber resiliency. Companies specializing in integration of AI and ML for cyber resiliency will move into the Industry 4.0 ecosystem. Although all of Industry 4.0 will benefit from companies converging teams and approaches, such as AI and ML, the robotics security market will leverage threat prediction and anomaly detection, even in the physical realm (FMI, 2019), enabling significant convergence benefits.





## Action Items

- Reorganize human capital into unified IT/OT teams, enabling new visions of cybersecurity and cyber resiliency through cross training and holistic defensive strategies.
- Proactively plan and promote security during each stage of system and software development life cycles to ensure each of the technology enhancements brought by Industry 4.0 negate any security risk the company is not willing to accept.
- Educate executive decision makers on cybersecurity, cyber resiliency and risk management strategies, such as the NIST Cybersecurity Framework.



## About Automation Alley

**A**utomation Alley is the World Economic Forum's Advanced Manufacturing Hub (AMHUB) for North America and a nonprofit Industry 4.0 knowledge center with a global outlook and a regional focus. We facilitate public-private partnerships by connecting industry, education and government to fuel Michigan's economy and accelerate innovation. Our programs give businesses a competitive advantage by helping them along every step of their digital transformation journey. We obsess over disruptive technologies like AI, the Internet of Things and automation, and work hard to make these complex concepts easier for companies to understand and implement.

### *Download the Full Report*

Automation Alley members are able to download the 2020 Technology in Industry Report free of charge! Log into your member portal and find your copy under the resources tab.

**Not a member?** Join Automation Alley today and let us help you increase revenue, reduce costs and think strategically. Contact 800-427-5100 or [info@automationalley.com](mailto:info@automationalley.com) to learn more.

### *Copyright*

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form without the prior written permission of Automation Alley. "Fair use" excerpts may be included in news or research reports provided that a complete citation is given to Automation Alley.

### *Our Contact Info*

2675 Bellingham  
Troy, MI 48083-2044

Phone: 248-457-3200  
Toll Free: 800-427-5100  
Fax: 248-457-3210

Email: [info@automationalley.com](mailto:info@automationalley.com)

Website: [automationalley.com](http://automationalley.com)

