NCYTE CENTER
National Cybersecurity Training & Education Center

BRIDGING THE IT/OT CYBERSECURITY SKILLS GAP:

LEVERAGING COMMUNITY COLLEGES, INDUSTRY PARTNERSHIPS, AND GOVERNMENT RESOURCES TO DEVELOP A FUTURE-READY WORKFORCE

Closing the IT/OT Cybersecurity Divide:
Building a Skilled Workforce Through Education, Industry, and Government Collaboration

FEBRUARY 2025

AUTHOR

Kyle Jones

Department of Information Technology,
Sinclair Community College

Table of Contents

ABOUT THIS REPORT

This report examines the growing cybersecurity challenges arising from the convergence of Information Technology (IT) and Operational Technology (OT). It highlights the increasing need for a skilled workforce capable of securing integrated IT/OT environments and explores the critical role of community colleges, industry partnerships, and government initiatives in closing the cybersecurity skills gap. By outlining key threats, workforce competencies, and strategies for education and training, this report provides a roadmap for developing a future-ready workforce to protect critical infrastructure and industries from evolving cyber threats.

Executive Summary

The convergence of Information Technology (IT) and Operational Technology (OT) is reshaping industries. The efficiency and innovation produced by the convergence also introduce significant cybersecurity challenges across the nation. As a member of the National Cybersecurity Training & Education Center (NCYTE), I will investigate the skills gap created by the integration of IT and OT across sectors such as manufacturing, healthcare, automotive, and critical infrastructure. I will also address current and future cybersecurity threats from IT/OT integration urgently requires a prepared workforce. This report is based on my 24 years in the industry as well as insights and research that addresses the growing role of OT and IT in the workforce.

The Expansion of OT Into IT Systems

The rising integration of OT and IT systems, connecting more devices and industrial systems to IT networks, increases efficiency but also expands cybersecurity vulnerabilities across internal and external environments. The rapid digitization of manufacturing and supply chain operations has led to the widespread adoption of network-connected OT devices, many of which are managed by individuals without cybersecurity or networking expertise. This growing reliance on interconnected systems has created a significant security gap by increasing the risk of cybersecurity threats by all the new devices connected to the network.

Future Threats Facing OT Integration

Experts predict cybersecurity threats against integrated OT and IT systems will become both more frequent and sophisticated. One of the primary concerns is the increasing attack surface with millions of new devices added to the IT systems. Initially, OT systems operated in isolated environments, which limited exposure to external and internal cyber threats. With the expanding network connectivity of industrial control systems, manufacturing equipment, and critical infrastructure, they become exposed to both existing physical threats and emerging cyber threats.

These environments are prime targets for cybercriminals and nation-state actors because of the significant damage they can cause to critical infrastructure, operations, and public safety. Once connected to external networks, these systems are vulnerable to ransomware attacks, unauthorized remote access, and data breaches. The incidents are often the results of unpatched vulnerabilities in legacy OT systems that were not originally designed with cybersecurity in mind. Operational disruptions, financial losses, time, and compromised safety to internal and external users unfortunately result from these attacks.

The rise of artificial intelligence (AI) will further complicate securing integrated environments. Malicious actors are leveraging AI to automate attacks, making them more adaptive and challenging to detect. AI-enhanced malware can identify weaknesses in OT networks and exploit them at a speed and scale that traditional cybersecurity measures struggle to counter. To combat these threats and vulnerabilities, organizations must prioritize security strategies, including continuous monitoring, segmentation of IT and OT networks, and ongoing workforce training and education.

Workforce Skills and Competencies for the Future

As IT and OT systems continue to converge, a unique blend of cybersecurity, networking, and industrial technology skills is necessary to address emerging threats. Key competencies include expertise in risk assessment, threat detection, incident response, and a secure system design for industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA), and other critical technologies. Professionals must also understand cloud architecture, AI-driven threat analysis and automated security response strategies. In addition to technical skills, IT and OT security experts need to be adaptive and possess strong problem-solving and communication skills to handle rapidly changing cyber threats.

Community colleges play a vital role in equipping students with the skills necessary for integrated environments. To address the skills gap, community colleges should partner with industry and other entities to offer hands-on, immersive educational experiences, such as apprenticeships, internships, externships, and real-world simulations.

Developing Strong Industry and Academic Partnerships

Partnerships between academia, government, and business are required to support the development of the IT/OT workforce. To effectively prepare students, academic institutions must collaborate with businesses, government agencies, and technology organizations that specialize in cybersecurity and industrial operations. Existing partnerships between community colleges and entities such as the National Science Foundation (NSF), National Security Agency (NSA), Department of Homeland Security (DHS), Idaho National Labs (INL), National Institute of Standards and Technology (NIST), Siemens, Rockwell Automation, Cisco, CompTIA, and SANS can provide access to advanced tools, resources, and real-world learning opportunities. These collaborations ensure that IT/OT programs align with industry standards and respond to growing cybersecurity threats in critical infrastructure sectors.

National center projects play a vital role in identifying and developing tools to help educate faculty members about the educational gaps in the IT/OT workforce. NCyTE, an NSF ATE National Center for Cybersecurity, is ideally situated to tackle the shortage of OT cybersecurity curriculum by supporting faculty training and curriculum development. To align education with workforce needs nationwide, NCyTE can act as a liaison between community colleges, businesses, and government agencies. By engaging IT/OT experts, the center can offer targeted faculty development programs that equip instructors with the knowledge to integrate IT/OT security concepts into their teaching. Recommendations include the creation of instructional materials, hands-on lab activities, case studies, and student projects focused on IT/OT security risks and solutions.

Introduction

Most people are familiar with Information Technology (IT), as it's become integral to both our personal and professional lives. We commonly interact with cell phones, PC's, tablets, and wireless systems in our homes and work environments. However, Operational Technology (OT), which is integral to managing and controlling industrial systems, remains unfamiliar to the public. This lack of awareness creates a significant challenge in understanding the cybersecurity implications that arise from integrating IT and OT. As key industries such as manufacturing, healthcare, automotive, and energy continue to adopt interconnected digital technologies to increase operational efficiency, new cybersecurity vulnerabilities that demand specialized skills and knowledge arise.

Despite the increasing reliance on integrated IT and OT systems, the current workforce often lacks the cross-disciplinary expertise needed to address cybersecurity threats effectively. Most professionals specialize in either IT or OT, making it difficult for organizations to hire workers who can navigate the security risks of both domains. Complex industrial environments are vulnerable to a wide range of threats without integrated knowledge. As the United States continues to face an aging workforce, and with education struggling to keep pace with dynamic technologies due to various constraints, many employees are trained only in either OT or IT. Community colleges must provide this new workforce with education and training to bridge this skills gap.

This report begins with a foundational overview of IT and OT, their convergence, and the unique risks that arise from their integration. It then examines the cybersecurity skills gap at the intersection of IT and OT and explores the pivotal role that community colleges should play in addressing this challenge. Finally, the report will discuss how community colleges, in collaboration with other entities, can bridge this gap by developing targeted curricula, enhancing faculty capabilities, and preparing students for comprehensive IT and OT integrated cybersecurity roles.

Overview of Information Technology, Operational Technology, and their Convergence

Information Technology

While it is assumed most people have a basic understanding of IT, it is essential to define it for proper differentiation from OT. The National Institute of Standards and Technology (NIST, n.d.-a, para. 1) identifies IT as: “any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.” IT encompasses the movement, storage, and processing of data and information pivotal in modern digital infrastructure.

IT systems, including physical components such as servers, networking hardware, and storage devices, facilitate the seamless transmission and management of information across various platforms. This also encompasses cloud tech technologies that are now integrated into most systems. While these systems operate within the physical realm, their core functions primarily occur in the digital space.

Operational Technology

The technologies used within the field of OT consist of physical devices that enact change in the physical world. More formally, OT is: “programmable systems or devices that interact with the physical environment or manage devices that do so. These systems/devices detect or induce direct changes through the monitoring and/or control of devices, processes, and events” (NIST, n.d.-b, para. 1). Their purpose is to: “connect, monitor, manage, and secure an organization’s industrial operations” (Cisco, 2025, para.2).

Examples of technology found within the field of OT include hardware components like sensors and robotic actuators and more complex systems like programmable logic controllers (PLCs) and locally controlled SCADA. Integrating IT with these OT physical devices has expanded throughout our manufacturing, healthcare, automotive, and energy sectors has broadened the exposure to cybersecurity risks.

IT and OT: From Initial Separation to Modern Convergence

Understanding the historical separation of IT and OT creates a foundation for comprehending the more recent convergence. Initially, both IT and OT emerged separately for their own purposes. Military and business purposes drove the creation of the network of information and data technologies that are now refer to as IT, helping to aid research and human communication (Leiner et al., 1997). The technologies that fall under the umbrella of OT developed from the goal to further mechanize the gains made in the industrial revolution (Bong, 2022). These mechanizations were used for manufacturing, transportation, and utilities. The IT and OT technologies had different objectives, and as a result, they mostly operated independently from one another for decades.

Since the widespread adoption of the Internet in the 1990s, interconnectedness and the availability of information and data have skyrocketed. Since then, governments, businesses, and other industries have developed ways to use these advances to increase the safety, efficiency, and reliability of various processes and activities. The convergence of IT and OT in recent years has played a prominent role in these improvements across multiple domains.

An example of integrating IT and OT is in healthcare, where it has transformed patient care and improved operational efficiency. Innovative medical devices like infusion pumps and ventilators are now linked to hospital IT network systems, enabling healthcare providers to monitor patient vitals in real-time and receive alerts about any abnormalities. Similarly, remote patient monitoring devices enable doctors to track chronic conditions like diabetes and heart disease from anywhere worldwide, decreasing hospital readmissions and improving patient outcomes. Robotic-assisted surgical tools and automated medication dispensing units enhance precision and reduce human error, saving countless lives. Using predictive analytics in hospital operations has also improved resource management, allowing facilities to optimize staff schedules and equipment usage based on real-time patient data.

While these advancements offer significant benefits, they also present new and ever-changing cybersecurity challenges. The increased connectivity of medical devices and hospital networks renders them vulnerable to cyberattacks, potentially compromising patient safety and data privacy. Safeguarding integrated environments requires a skilled workforce with cybersecurity and operational technology expertise to mitigate risks and ensure compliance with healthcare regulations. This is just one example—other industries, each with its own set of challenges, are facing similar cybersecurity concerns.

Threats Facing OT Integration

The integration of OT and IT systems will cause cybersecurity threats to grow in complexity, sophistication, and frequency because of the large number of devices being added daily to the IT network systems (Sinha, 2024). Adaptable security strategies are needed, given the scale of this change. The vulnerabilities introduced by IT/OT convergence extend far beyond traditional IT security concerns and require a nuanced understanding of industrial environments. Vulnerabilities to be discussed include expanded attack surface, ransomware and extortion attacks, targeting legacy OT systems, insider threats, nation-state actors, and AI-driven attacks.

Expanded Attack Surface

The convergence of IT and OT considerably increases the attack surface (Edwards, n.d.). As discussed in the overview, OT systems were initially isolated, proprietary, and air-gapped (not connected to a network), which limited their exposure to external cyber threats. Now, their increasing network connectivity exposes them to the same longstanding cyber threats that IT systems have faced. OT system failures, however, don't just affect information and data; they can cause catastrophes in the physical world.

Envision a factory where the robotic arms assembling car parts are controlled by PLCs connected to the corporate network. If a vulnerability in the PLC software is exploited, an attacker could gain control of the robotic arms, disrupting production, incorrectly assembling parts, or even endangering workers. The software's weaknesses create a point of entry into the physical world and thus accesses to the OT components.

Ransomware and Extortion Attacks

Ransomware attacks are becoming increasingly prevalent and sophisticated. Cybercriminals are now targeting industrial environments with ransomware, encrypting critical OT systems and demanding a ransom to restore operations. System recovery is not guaranteed even with ransom payment; substantial downtime and financial losses remain a risk. Another rising trend involves attackers exfiltrating sensitive data, encrypting systems, and demanding ransom to prevent data release to the public (Fortinet, n.d.).

The Colonial Pipeline attack in 2021 demonstrated the devastating impact of ransomware on critical infrastructure (Government Accountability Office [GAO], 2021, para. 4). This type of attack clearly outlines how attackers use operational equipment connected to network infrastructure to take advantage of onsite systems. The attack disrupted fuel supplies to the East Coast of the United States and required a substantial ransom to be paid by the company.

Targeting of Legacy OT Systems

Some OT systems still in use today are decades old and were designed without cybersecurity in mind. These legacy systems often have unpatched vulnerabilities and lack modern security controls, making them easy targets for attackers. Organizations are often hesitant to update or replace legacy OT systems due to compatibility concerns, cost, and the risk of disrupting operations.

Another 2021 attack allowed malicious actors to gain control of a water treatment system in Florida (Cybersecurity & Infrastructure Security Agency [CISA], 2021). The attackers changed the plant settings, attempting to add a high concentration of sodium hydroxide to contaminate the water supply. Although multiple factors of negligence contributed to this incident, the unpatched, outdated Windows 7 software was a contributing problem.

Insider Threats

Insider threats, whether malicious or unintentional, pose a significant risk to IT/OT environments. Employees with access to critical systems can inadvertently introduce malware, mis-configure security controls, or intentionally sabotage operations. The lack of security awareness, network security, and vulnerability assessment training among OT personnel exacerbates this risk.
In 2017, an employee of a Middle East petrochemical plant unintentionally downloaded malware through a phishing attack (U.S. Department of the Treasury, 2020). Failsafe mechanisms prevented a catastrophe because of a cyber-informed engineering plan. Despite a positive outcome, this example shows how an employee could unintentionally contribute to a devastating result for an organization's infrastructure.

Nation-State Actors and Advanced Persistent Threats (APTs)

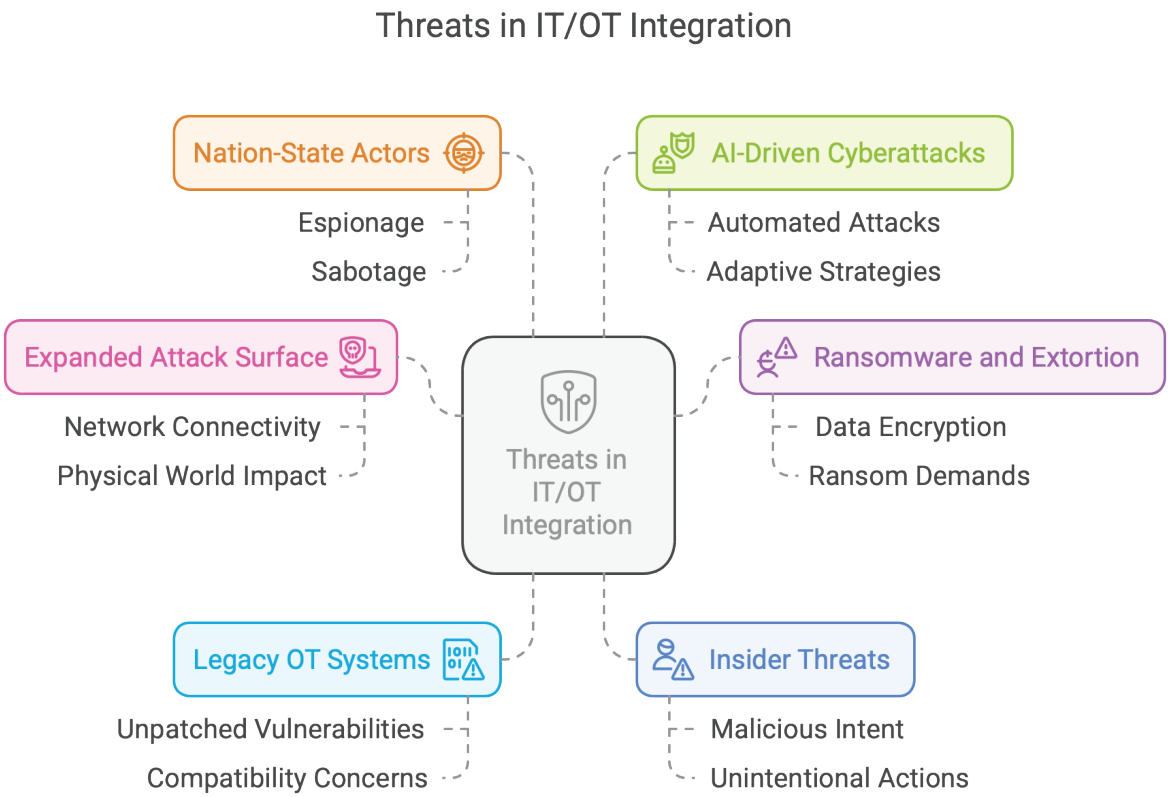
Nation-state actors and APTs are increasingly targeting industrial environments for espionage, sabotage, and disruption. These actors have the resources and expertise to develop sophisticated cyber weapons that bypass traditional security controls. When accessed, nation-state actors can access operational technology in integrated systems and stay on the networks monitoring operations indefinitely until otherwise discovered.

The Stuxnet worm, which targeted Iranian nuclear facilities in 2010, demonstrated the potential impact of nation-state attacks on critical infrastructure (Council on Foreign Relations, 2010). This worm gained access to mechanical centrifuges and reported incorrect data to the monitoring systems. These centrifuges were spinning faster than intended, causing catastrophic failure while reporting normal behavior to the IT systems.

AI Driven Cyberattacks

The rise of AI-driven cyberattacks poses a significant threat to IT/OT integrated environments. Malicious actors are leveraging AI to automate attacks, making them more adaptive and challenging to detect. AI-enhanced malware can identify weaknesses in OT networks and exploit them at a speed and scale that traditional cybersecurity measures struggle to counter.

There are many ways AI can aid cyberattacks, including, “identifying vulnerabilities, deploying campaigns along identified attack vectors, advancing attack paths, establishing backdoors within systems, exfiltrating or tampering with data, and interfering with system operations” (Stanham, 2025). For example, when identifying vulnerabilities, cybercriminals can use AI to analyze network traffic, identify detection patterns, and adapt their tactics to evade security measures in real time. By leveraging AI, attackers can outmaneuver traditional defense strategies.



Proactive Security Strategies

To mitigate these emerging threats, organizations must prioritize security strategies, including:

- **Continuous Monitoring:** Implementing continuous monitoring systems to detect and respond to cyber threats in real-time.
- **Segmentation of IT and OT Networks:** Segmenting IT and OT networks to limit the impact of cyberattacks.
- **Vulnerability Management:** Implementing a robust vulnerability management program to identify and patch vulnerabilities in IT and OT systems.
- **Security Awareness Training:** Providing security awareness training to all employees, including OT personnel and individuals responsible for critical infrastructure.
- **Incident Response Planning:** Developing and testing incident response plans to ensure that organizations are prepared to respond to cyberattacks.
- **Supply Chain Security:** Addressing supply chain risks by ensuring that third-party vendors and suppliers have adequate security controls in place and are meeting regulations and standards.
- **Zero Trust Architecture:** Implementing a Zero Trust architecture that requires all users and devices to be authenticated and authorized before accessing network resources.

To effectively counteract these increasingly sophisticated and pervasive cyber threats, a highly skilled and competent workforce is essential. Professionals need the expertise to understand the growing threat landscape and proactively implement and manage robust security measures. Community colleges' established workforce development programs and industry partnerships uniquely position them to provide the essential training and education needed to develop this critical talent pool.

Skills Gap and Curriculum Development

As IT and OT systems continue to converge, the workforce must develop a unique blend of cybersecurity, networking, and industrial technology skills to address emerging threats (Kumpf, 2023, para.10). The growing reliance on connected OT devices and industrial control systems requires professionals who understand IT security principles and the operational environments where these systems are incorporated. This convergence requires a workforce capable of bridging the traditional gaps between IT and OT, ensuring the security and reliability of the critical infrastructure we rely on daily.

Skills and Competencies

Key competencies include expertise in risk assessment, threat detection, incident response, and a secure system design for ICS, SCADA, and other critical technologies. Professionals must also understand AI-driven threat analysis and automated security response strategies. In addition to technical skills, IT and OT security experts need to be adaptive and possess strong problem-solving and communication skills to handle rapidly changing cyber threats and communicate them effectively and efficiently to other parts of the operations. Following is a more detailed look into these competencies.

Risk Assessment and Management

Professionals must be able to conduct thorough risk assessments that consider the unique vulnerabilities introduced by IT/OT convergence. This includes understanding the potential impact of cyberattacks on both IT and OT systems, as well as the interdependencies between them.

Application: Implementing risk management frameworks and becoming familiar with industry standards such as NIST's Cybersecurity Framework or ISO 27001 to identify, assess, and mitigate risks specific to IT/OT environments.

Threat Detection and Incident Response

Professionals must be proficient in detecting and responding to cyber threats targeting IT and OT systems. This involves the use of advanced security tools and techniques, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) systems, next-generation firewalls, threat intelligence platforms, and alerting tools.

Application: Developing and implementing incident response plans that address the specific challenges of IT/OT environments, including procedures for isolating affected systems, containing the spread of malware, and restoring operations.

Secure System Design

Professionals need to understand the principles of cyber-informed engineering and be able to apply them to IT and OT systems. This includes implementing security controls such as network segmentation, access controls, and encryption to protect sensitive data and critical infrastructure.

Application: Designing and implementing secure architectures that incorporate defense-in-depth principles, such as layered security controls and redundancy, to minimize the impact of cyberattacks.

Knowledge of ICS, SCADA, and Other Critical Systems

A comprehensive understanding of the technologies and protocols used in ICS, SCADA, and Industrial Internet of Things (IIoT) environments is essential. This includes knowledge of common ICS protocols, such as Modbus, DNP3, and OPC UA, as well as the specific security challenges associated with these protocols.

Application: Implementing security measures to protect ICS, SCADA, and IIoT devices from cyberattacks, such as vulnerability patching, network segmentation, and access controls.

AI-Driven Threat Analysis and Automated Security Response Strategies

As AI and automation become more prevalent in cybersecurity, professionals must develop skills in these areas. This includes understanding how to use AI-powered tools to detect and respond to cyber threats, as well as how to automate security tasks to improve efficiency.

Application: Using AI-powered tools to analyze network traffic for anomalous behavior and automatically respond to potential cyberattacks.

Problem-Solving Skills and Adaptability

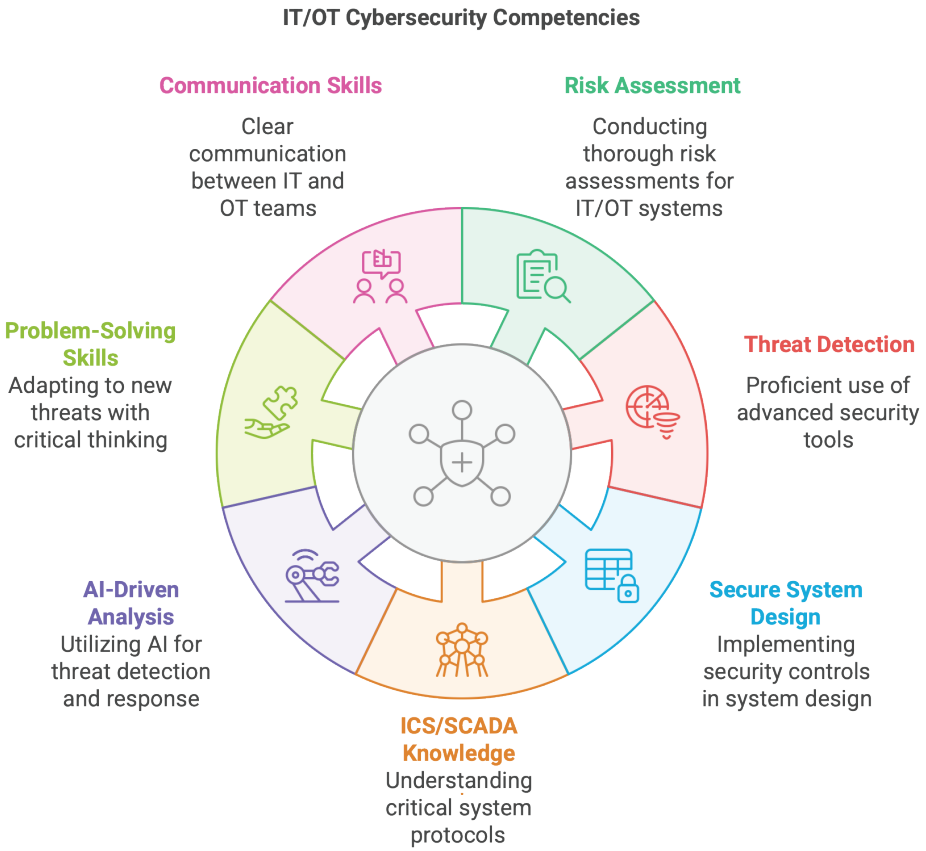
The cybersecurity landscape is constantly evolving, and professionals must be able to adapt to new threats and challenges. This requires strong problem-solving skills, critical thinking, and the ability to learn quickly and relay information effectively.

Application: Being able to analyze complex security incidents, identify root causes, and develop effective solutions.

Communication and Collaboration

Effective communication and collaboration between IT and OT teams are crucial for incident response and overall security. Many advisory teams and business professionals consider these skills a top priority. Professionals must be able to communicate technical information clearly and concisely to both technical and non-technical audiences.

Application: Facilitating communication between IT and OT teams during incident response to ensure that all stakeholders are aware of the situation and can act.



Integrated IT and OT Curriculum Development at Community Colleges

Community colleges are essential in providing students with the skills necessary to succeed in the converging IT and OT landscape. By offering interdisciplinary and cross-discipline programs that combine IT, OT, and cybersecurity, they can effectively prepare students for the workforce. It is essential that students graduate and become well-informed technicians responsible for the running the infrastructure.

Curriculum Development

The curriculum should comprehensively address IT and OT systems, emphasizing cybersecurity principles. Key components should include:

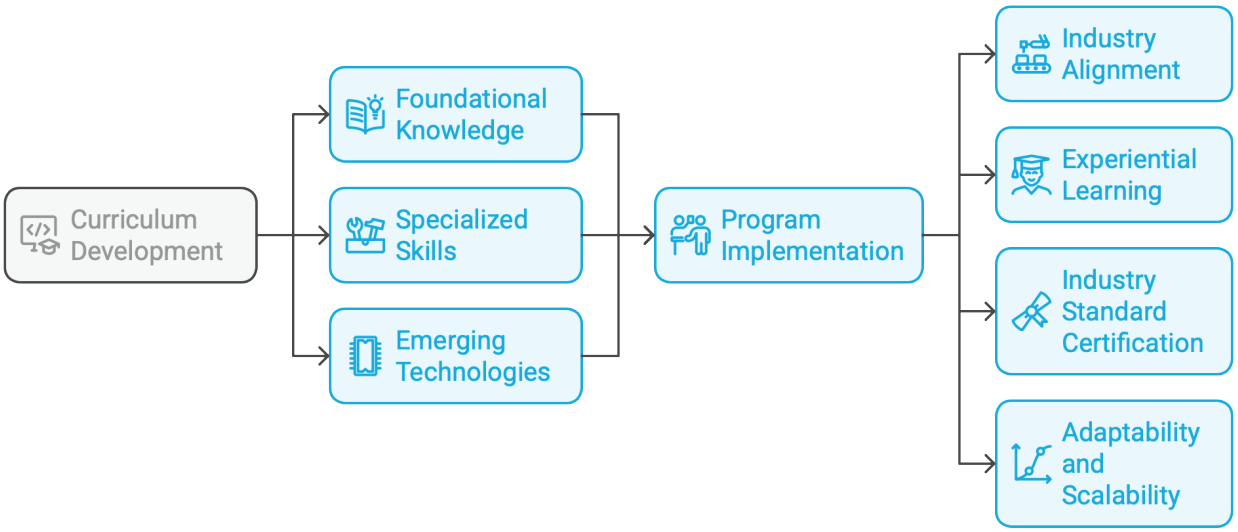
- **Foundational Knowledge:** Including the basics of IT systems (networking, cloud computing, data management), the fundamentals of OT systems (ICS, SCADA, IIoT), and an overview of cybersecurity principles (risk assessment, threat detection, incident response, secure system design).
- **Specialized Skills:** Covering understanding the vulnerabilities introduced by IT/OT convergence, case studies on ransomware attacks and other cyber threats targeting critical infrastructure, hands-on training in securing interconnected systems using tools like firewalls, intrusion detection systems, and network segmentation, and knowledge of compliance standards such as NIST frameworks and industry-specific regulations.
- **Emerging Technologies:** Encompassing AI-driven threat detection and automated security response strategies, ensuring students are prepared for the evolving threat landscape.

Program Implementation

With a robust curriculum established, the next crucial step involves the strategic implementation of these program to ensure its effectiveness and alignment with industry demands. Effective IT/OT cybersecurity programs require collaboration between multiple departments, including IT, engineering, manufacturing, supply chain, and computer science. Key considerations for effective implementation:

- **Industry Alignment**: Develop programs in close collaboration with industry partners to ensure alignment with current and future workforce needs.
- **Experiential Learning:** Integrating this study with opportunities for students to gain real-world experience through internships, apprenticeships, and other work-based learning experiences.
- **Industry Standard Certification:** Ensure student are knowledgeable for their industry with certifications, such as the Certified Information Systems Security Professional (CISSP) or the Certified Industrial Cybersecurity Professional (CICP).
- **Adaptability and Scalability:** Design programs to be adaptable and scalable to meet the changing needs of the IT/OT cybersecurity industry. This should be done in collaboration with strong partnerships.

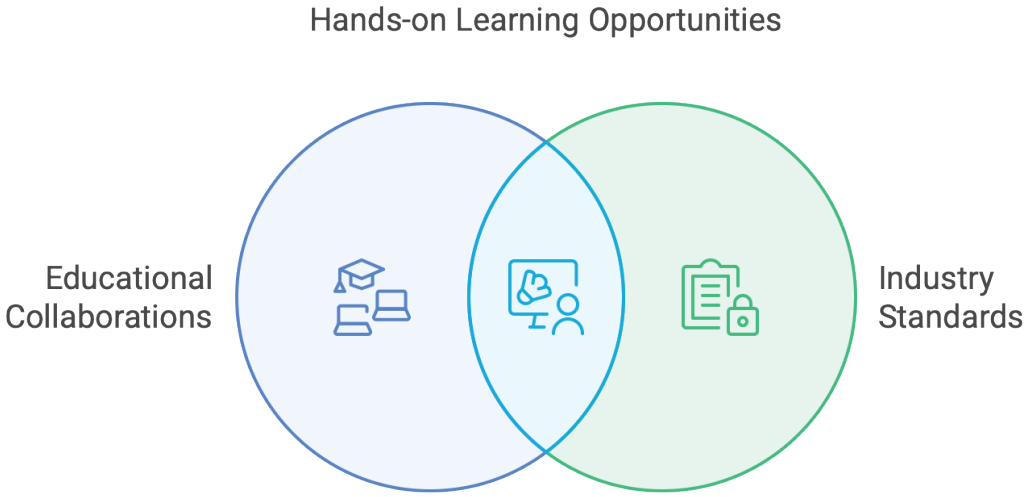
IT/OT Cybersecurity Curriculum Development and Implementation



Developing Strong Industry and Government Partnerships

To effectively prepare students, academic institutions must collaborate with businesses, government agencies, and technology organizations that specialize in cybersecurity and industrial operations. Partnerships with entities such as the National Science Foundation (NSF), National Security Agency (NSA), Department of Homeland Security (DHS), Idaho National Labs (INL), National Institute of Standards and Technology (NIST), Siemens, Rockwell Automation, Cisco, CompTIA, and SANS can provide access to advanced tools, resources, and real-world learning opportunities.

These collaborations ensure that IT/OT programs align with industry standards and respond to growing cybersecurity threats in critical infrastructure sectors. This also allows for students to have hands-on learning opportunities with cutting-edge equipment that they will use in the workforce.



Industry Partnerships

Community colleges can enhance student readiness for integrated roles by prioritizing workforce development initiatives. The following programs help students develop practical skills while building relationships with potential employers.

Internships

Internship programs provide students with invaluable real-world experience. Working with professionals in IT/OT environments, interns gain firsthand exposure to cybersecurity protocols, industrial control systems, and network security measures. These experiences not only enhance their technical skills but also help them develop problem-solving abilities and adaptability. Employers benefit by identifying and cultivating future talent, ensuring that graduates enter the workforce with relevant and applicable skills. This is especially important given that most community college students stay in the region where they went to school. (Center for Community College Student Engagement [CCCSE], 2024). This makes community colleges a valuable resource for the region of whom they serve.

Apprenticeships

Apprenticeships serve as a structured pathway for individuals to gain in-depth expertise while earning a wage. Unlike traditional academic programs, apprenticeships offer a blend of classroom instruction and on-the-job training, allowing participants to develop a strong foundation in cybersecurity, risk management, and operational technology. By engaging in long-term, hands-on learning, apprentices become well-versed in securing industrial networks, mitigating cyber threats, and implementing best practices for IT/OT integration. These programs provide a direct pipeline of skilled professionals to industries that are facing a workforce shortage in cybersecurity.

Externships

Externships can significantly enhance faculty expertise, allowing instructors to gain firsthand experience in real-world environments. By placing educators within industry settings, externships provide invaluable insights into current industry practices, emerging threats, and the specific skills sought by employers. This knowledge can then be channeled into more relevant and effective curriculum development.

The National Cybersecurity Training & Education Center (NCyTE) has offered externships to faculty members since 2023. The faculty members who have taken part in these experiences have provided valuable feedback, leading to the development of resources and curricula for the cybersecurity education community.

Other Industry Partnership Opportunities

- **Advisory Boards:** Industry representatives can guide curriculum development to ensure it meets current demands.
- **Business and Industry Leadership Team (BILT):** Teams that vote on knowledge skills and abilities for the degree areas.
- **Equipment Donations:** Companies can provide colleges with the latest tools and technologies for hands-on training.
- **Guest Lectures and Workshops:** Industry experts can share insights into emerging trends and real-world challenges.
- **Joint Research Projects:** Collaborative projects can address specific cybersecurity issues in IT/OT integration.

Government Partnership

NSF Advanced Technological Education (ATE) Centers and other national center projects play a vital role in addressing educational gaps in the IT/OT workforce. NCyTE, an NSF ATE National Center for Cybersecurity, is ideally situated to tackle the shortage of OT cybersecurity curriculum by supporting faculty training and curriculum development. By engaging IT/OT experts, the center can offer targeted faculty development programs that equip instructors with the necessary skills to integrate IT/OT security concepts into their teaching.

By leveraging its experienced team, NCyTE can create instructional materials, hands-on lab activities, case studies, and student projects focused on IT/OT security risks and solutions.

Furthermore, the center can help community colleges establish connections with business partners and government agencies to align educational programs with current workforce needs. Nationwide, NCyTE's initiatives are a vital resource for improving IT/OT cybersecurity education.

As the author of this study and an academic leader in IT and cybersecurity workforce development, I emphasize the urgent need for collaboration between academia, industry, and government to close the IT/OT cybersecurity skills gap. As part of my role with NCyTE, I have assisted in managing a faculty externship program, gathering feedback from over 40 faculty members working across various OT positions. This feedback has provided valuable insights into gaps within the current education landscape, enabling NCyTE to strengthen its network of industry partnerships to help guide the center's strategic development.

Conclusion

The merging of OT and IT has introduced significant security threats to the manufacturing, healthcare, automotive, and critical infrastructure sectors. This presents both opportunities and challenges for industries worldwide. There is an opportunity to create targeted curricula that integrates the technician's job role with networking and cybersecurity concepts. This can be accomplished by promoting workforce development through internships and apprenticeships, collaborating with industry partners, and utilizing resources from NSF-funded centers.

Community colleges are ideally positioned to address the IT/OT skills gap. Strengthening these collaborations will ensure that students are well-prepared to protect critical infrastructure and navigate the evolving cybersecurity landscape. These initiatives will equip a new generation of skilled technicians capable of securing critical infrastructure against evolving cyber threats while fostering innovation in interconnected industrial environments

References

Bong, N. (2022, April 26). The evolution of automation. Progressive Automations. https://www.progressiveautomations.com/blogs/news/the-evolution-of-automation

Center for Community College Student Engagement (2024). How clear is their path? Guided career pathways and community college students. https://www.ccsse.org/guided-career-pathways/Guided-Career-Pathways.pdf

Cisco. (2025). How do OT and IT differ? Retrieved January 18, 2025, from https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

Council on Foreign Relations (2010, July). Stuxnet. Cyber Operation Tracker. https://www.cfr.org/cyber-operations/stuxnet

Cybersecurity & Infrastructure Security Agency (2021, February 12). Compromise of U.S. water treatment facility. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a#:~:text=Summary,U.S.%20drinking%20water%20treatment%20facility.

Edwards, M. (n.d.). Addressing and securing converged IT/OT environments. ISA Global Cybersecurity Alliance. Retrieved February 26. 2025, from https://gca.isa.org/blog/addressing-and-securing-converged-it-ot-environments

Fortinet (n.d.). What is data exfiltration? Retrieved February 26, 2025, from https://www.fortinet.com/resources/cyberglossary/data-exfiltration

Government Accountability Office (2021, May 18). Colonial pipeline cyberattack highlights need for better federal and private-sector preparedness (infographic). Watchblog: Following the Federal Dollar. https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic

Kumpf, K. (2023, December 21). Addressing the ongoing OT security skills gap. https://www.manufacturing.net/page/mnet-about-us

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (1997). A brief history of the internet. https://www.internetsociety.org/internet/history-internet/brief-history-internet/

National Institute of Standards and Technology. (n.d.-a). Information Technology. In NIST Computer Security Resource Center Glossary. Retrieved January 18, 2025, from https://csrc.nist.gov/glossary/term/information_technology

National Institute of Standards and Technology. (n.d.-b). Operational Technology. In NIST Computer Security Resource Center Glossary. Retrieved January 18, 2025, from https://csrc.nist.gov/glossary/term/operational_technology

Sinha, S. (2024, September 3). State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

U.S. Department of the Treasury (2020, October 23). Treasury sanctions Russian government research institution connected to the Triton malware. https://home.treasury.gov/news/press-releases/sm1162

NCyTE CENTER

National Cybersecurity Training & Education Center

The **National Cybersecurity Training and Education Center (NCyTE)** at Whatcom Community College, funded by the NSF, enhances U.S. cybersecurity education by supporting faculty, developing resources, and strengthening industry partnerships to build the cybersecurity workforce.

The National Cybersecurity Training and Education Center is funded by the National Science Foundation grant #2054724.