WHITEPAPER

AUTOMATION.COM

A subsidiary of the International Society of Automation

By Renee Bassett, Automation.com

OT Cybersecurity Actions and Perceptions in the Energy Sector

Survey highlights areas of progress and concern around creating more secure systems for petrochemical and oil & gas operations.

FORTINET®

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity is more crucial than ever to the safety and security of industrial operations. With the increasing interconnectedness of information technology (IT) and operational technology (OT) systems comes the urgent need to better secure SCADA, industrial control systems, remote access and more. This is especially true in the petrochemical and oil & gas industries, as the energy sector has been by far the most frequent target of OT cyberattacks[1]. Such attacks have not only caused unauthorized access and data exposure but also disrupted operations, threatened safety, and prompted significant regulatory changes for oil & gas and petrochemical companies.

The May 2021 cyberattack on Colonial Pipeline—a ransomware attack on the company's IT system—resulted in the company shutting down operations of its pipeline for several days. The incident disrupted gasoline delivery in the southeast United States and led to an immediate directive from the Transportation Security Administration (TSA) requiring new cybersecurity measures[2]. This first TSA directive and other federal regulations for cybersecurity of pipelines and critical infrastructure that followed[3,4,5] launched some companies into a journey toward OT cybersecurity. For others, the directives validated steps already being taken to become more cyber secure.

Fortinet wanted to find out more about oil & gas and petrochemical companies' cybersecurity efforts, priorities, and preparedness so the company commissioned the OT Cybersecurity Preparedness 2023 Survey in cooperation with Automation.com[6]. Conducted in May 2023, the survey asked process control engineers, IT/OT security architects and other OT security or operations professionals about their companies' cybersecurity activities: what OT-specific systems need to be protected, their perception of cybersecurity best practices, and how well oil & gas companies are doing with implementing those best practices.

The survey filtered out respondents who did not have knowledge of their companies' cybersecurity activities, resulting in a pool of highly qualified respondents: 78% in upstream, midstream, and downstream oil & gas operations and 22% in chemicals and allied products. The broader community of oil & gas and petrochemical professionals can benefit from evaluating how their companies compare to their peers and gaining insight into what their companies may need to address next.

Of all the business risks faced by oil & gas companies, 60% of survey respondents placed OT cybersecurity in the top five.

SECURING OT SYSTEMS

Oil & gas industry professionals are aware of the risk of cyberattacks, and many consider cybersecurity a priority. In fact, of all the business risks faced by oil & gas companies, 60% of survey respondents placed OT cybersecurity in the top five. Survey respondents cited the prevalence of recent cyberattacks as the top reason motivating pursuit of cybersecurity, followed by regulatory changes. The expectations of customers, and of their own top management, were also motivators for some.

Respondents acknowledged that a wide range of activities are crucial for securing the OT environment. Activities ranked as very or extremely important by 85% or more included:

- Vulnerability assessment, management scanning, and early detection of attacks
- Incident response planning
- Use of security analysis, monitoring, and assessment tool
- Review of cybersecurity standards and best practices
- Asset discovery and visibility of operating environment

Other activities considered very or extremely important by between 72% and 82% of respondents include management of security compliance, threat intelligence, visibility of security status, visualization of security events, and central management of security policies. Many of these activities relate to cybersecurity governance, including who "owns" OT cybersecurity efforts and activities—IT, OT or some new cross-functional team. This indicates that integrating cybersecurity activities with the organization is important.

When asked how effective they thought their companies were compared to peers in OT-securing activities, most respondents perceived their companies as on par or above average, as shown in Figure 1. More than a quarter of respondents, however, thought their companies were below average in threat intelligence, visualization of security events, and incidence response planning.

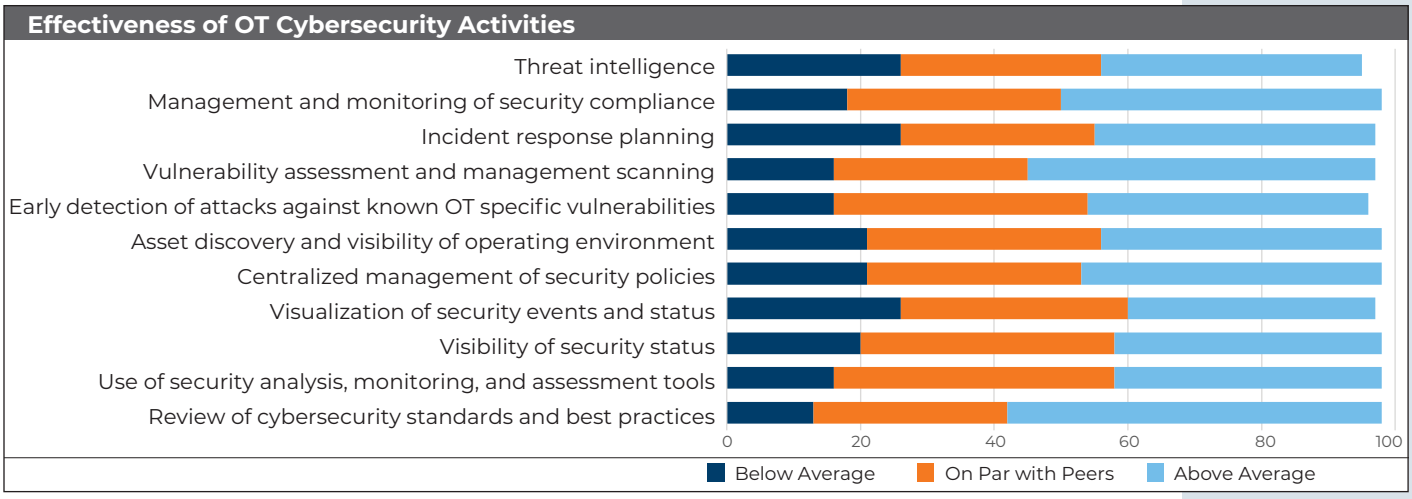


Figure 1. Most respondents say their companies are on par or above average compared to peers regarding OT-securing activities.

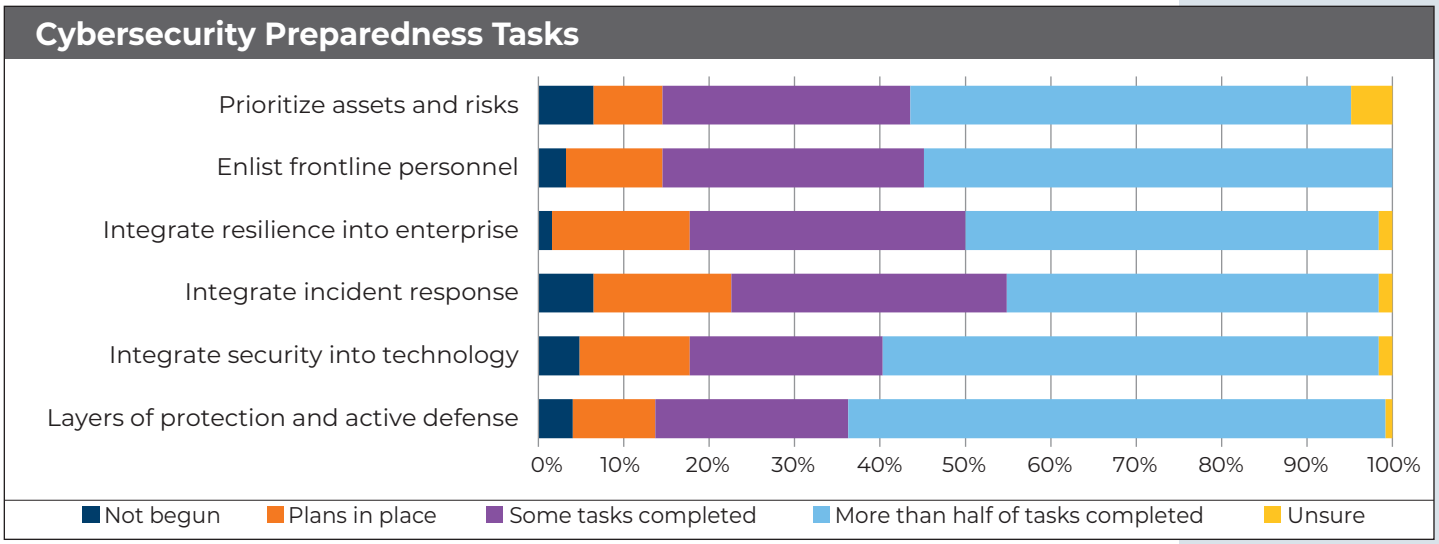


Figure 2. Survey respondents were asked to assess their companies' accomplishment in each area of applying cybersecurity protections to specific operational technology (OT) environments.

As companies pursue better methods of securing their OT systems, the goal is a proactive approach that incorporates the entire enterprise and its supply chain, embedding security into all processes[7]. Reaching that level of cybersecurity maturity involves accomplishing six fundamental actions:

- Prioritizing assets
- Enlisting frontline personnel
- Integrating cyber-resilience into enterprise processes
- Developing an integrated incident response
- Integrating security into technology environments
- Providing layers of protection and active defenses

The survey asked oil & gas / petrochemical respondents to assess their companies' progress toward completing those important cybersecurity preparedness tasks. The results revealed a split in cybersecurity maturity. Fifty-two percent of respondents reported their companies are well on their way, completing more than half or most of the tasks in these important action areas. The other half of respondents seem to be just getting started, with 8% saying their companies had plans in place but had not completed any tasks and 6% saying their companies had not begun cybersecurity activities at all.

Details of cybersecurity preparedness are shown in Figure 2. Individual comments supported this picture of an industry with companies on different parts of the path to maturity. Some described well-designed, 360-degree views of cybersecurity and having dedicated cybersecurity teams in place. Others said they were in the beginning phase of programs to close gaps. Still others pointed to budget delays and lack of management support.

When it comes to enlisting frontline personnel in cybersecurity efforts, 55% had completed more than half of tasks, which can include cybersecurity awareness and training for OT and non-OT employees and contractors, identifying the risk culture of the organization, and recruiting and developing cybersecurity talent. Another 31% had started and 11% had plans in place. Only 3% had not begun activities in this area.

Closing the skills gap for frontline workers through training is an important activity not only because these workers are on the frontline when it comes to security defense. Frontline workers could also distinguish themselves by demonstrating OT cybersecurity leadership. Fortinet's 2023 State of Operational Technology and Cybersecurity Report revealed that more OT cybersecurity professionals now come from IT security leadership rather than the operations team[8]. That is a trend that could be reversed.

Some described well-designed, 360-degree views of cybersecurity and having dedicated cybersecurity teams in place. Others said they were in the beginning phase of programs to close gaps.

SECURING MORE THAN IT SYSTEMS

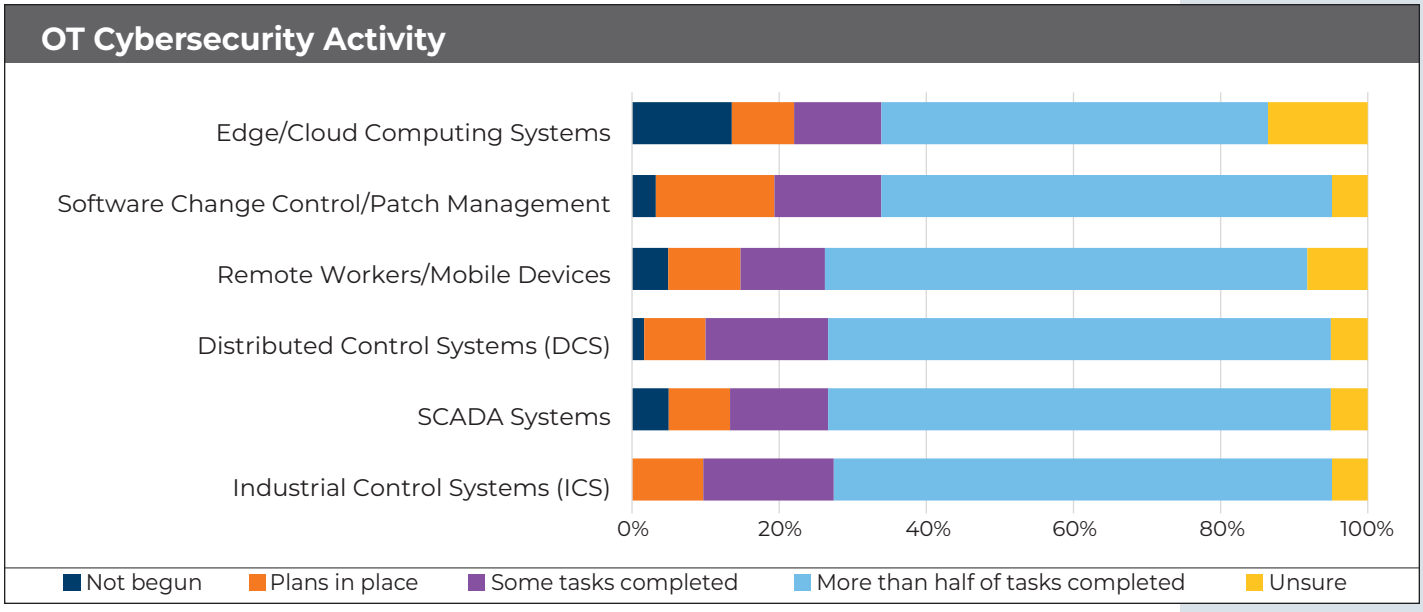
The six fundamental cybersecurity actions are sometimes seen as the responsibility of a company's IT department. As such, the perception can be that those protections are only being applied to the business systems. So, the survey asked what actions were being taken for OT-specific systems (Figure 3).

Sixty-eight percent of respondents report that their company had completed most tasks related to protecting their industrial control system (ICS). Eighteen percent had some tasks completed, and 10% had plans in place. Distributed control system (DCS) cybersecurity is similarly robust; 68% report half or more of their planned cybersecurity tasks had been completed. Another 17% had some tasks completed and 8% had plans in place but had not implemented specific measures.

As for SCADA systems, a similar 68% report that half or more of the fundamental cybersecurity tasks had been completed. Another 10% had some tasks completed and 8% had plans to protect their SCADA systems but had not implemented specific measures.

Awareness is growing around the importance of software change control and patch management as another layer of protection against cyberattacks. Sixty-one percent of respondents report that these protective measures are being implemented for OT systems software most of the time, and another 15% say they're being applied some of the time. Sixteen percent had plans in place to implement software change control and patch management.

Figure 3. While some think cybersecurity actions are only being applied to oil & gas / petrochemical business systems, the survey revealed that the OT systems listed are increasingly well protected.



ACCOMPLISHING THE FUNDAMENTALS

The Fortinet report mentioned earlier indicates[8] that OT professionals in general are developing a more realistic sense of their organizations' OT cybersecurity capabilities and this survey of companies in the energy sector bears that out. Survey respondents recognize the following fundamental tasks and activities need to be accomplished and, as said earlier, about half are well on their way.

Integrating cyber-resilience into enterprise processes includes vendor management, risk reporting and metrics, product security, and organizational structure and roles. The research showed that 48% of oil & gas / petrochemical companies had completed more than half of their tasks in this area; an equal 48% are on their way (32% with some activities completed and 16% with plans in place). Only 2% had not begun.

Similarly, 44% of companies are well on their way to having **integrated incident response**, which could include response plans, simulations, continuity planning, disaster recovery, and system resilience plans; 32% had started and 16% had plans in place, but 6% had not yet begun.

Integrating security into technology environments encompasses asset management, software patch management, cloud and edge security, secure architecture, endpoint or mobile security, physical security, and secure system development. Approximately 58% of respondents had completed more than half of these tasks, 23% had completed some tasks, 13% had plans in place, and 5% had not begun.

Oil & gas / petrochemical companies seem to have taken the most action **deploying active defenses and providing layers of protection** to secure OT systems. Active defense can include cyber-intelligence, vulnerability awareness, asset monitoring and analytics. Actions related to layers of protection include setting policies, use of standards (such as the ISA/IEC 62443 standard[9]), auditing and compliance activities, assessment and diagnostic activities, and program and project management. As shown earlier in Figure 2, 63% of respondents say that more than half of these tasks had been completed, 23% indicate some had been completed, and 10% say plans are in place.

Internal network segmentation is the most common security control employed. Other common security activities include internal security training and education, hardening the network by disabling unnecessary services, role-based access control, and having a dedicated SCADA/ICS security team.

Edge and cloud computing cybersecurity, which are often considered the responsibility of IT, is increasingly being applied to OT systems. A relatively large percentage of respondents (14%) were unsure of their companies' status in this area, and another 14% said it had not been addressed. This uncertainty could be partly due to this area being the responsibility of the IT department. However, 52% of respondents said more than half of tasks had been completed in this area.

The survey also asked specifically about **security for remote access** (remote workers or mobile devices); 66% of respondents said more than half of tasks had been completed in this area, while 5% had not begun and 8% were unsure. Many systems in industrial OT and ICS environments allow secure remote access for connecting to third-party technicians or contractors, as well as for increased productivity and other reasons. While such access does bring increased risk, a range of solutions are used to mitigate risk in the oil & gas sector, such defense in depth, network segmentation, and air gapping[10].

Edge and cloud cybersecurity, which are often considered the responsibility of IT, are increasingly being applied to OT systems.

NEXT STEPS

When asked to write in "the area in which your company has done particularly well or has been most successful with regard to protecting OT systems," respondents responded with the following, which provides a useful checklist of protective activities:

- Adoption of Purdue Reference Model and ISA/IEC 62443 ZCRs
- Aggressive and regular external attack & penetration testing as well as software supply chain analysis (SBOMs).
- Asset inventory, security controls tagging and auditing
- Controlled access to OT area using network media access control
- End points hardening
- Engagement of CS, IT, OT, operations to architect and deploy the most secure network and systems
- Governance, monitoring, awareness
- Hiring competent people and forming a proper cybersecurity organization
- Integration of clients' systems
- Isolated and segmented OT network with MFA access only, for all users
- Preparation of proper design basis, specification, and risk analysis
- Risk and vulnerability assessment
- Standards and audits
- System hardening and security patching
- Vulnerability assessment, Pentest of products and system and mitigation actions
- We have implemented a network monitoring / anomaly detection, OT change management and Least Privilege solution

All those accomplishments are important elements of what oil & gas / petrochemical companies need to be doing to secure their OT systems. Reflecting the split nature of the energy sector's overall cyber maturity, however, respondents provided a similar list of what their companies, in their opinion, were not doing well. Asking respondents to write in "What important OT cybersecurity task(s) has your company ignored, not done well, or not gotten to fast enough?" revealed a surprisingly similar—and similarly useful— list:

- Application whitelisting and intrusion detection
- Asset inventory, lifecycle management, visibility into the OT networks, event logging
- Awareness, training
- Disaster recovery

- Earning buy-in from shop floor
- Hardening systems and incident response planning
- Leveraging / integrating OT SMEs into OT cyber security
- Moving process data users to a DMZ outside of the process control network
- OT security organization development
- Physical security, patching, documentation (e.g., policies)
- Provide structural organization for cybersecurity operations
- Removing obsolescence from the OT environment
- Segmentation of the OT network and not allowing access from corporate.
- Specific advanced training to staff for cyber security
- System surveillance and automatic anomaly notification
- Visibility, incident response

Partner for OT Cybersecurity Success

For more than a decade, Fortinet has protected OT environments in critical infrastructure sectors such as energy, defense, oil & gas, manufacturing, food, and transportation. By designing security into complex infrastructure via the Fortinet Security Fabric, organizations have an efficient, non-disruptive way to ensure that the OT environment is protected and compliant. Fortinet's commitment to protect IT / OT infrastructure is reflected in its corporate activities and active partnerships with leading cybersecurity organizations:

- **The Fortinet Training Institute**, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone.
- **FortiGuard Labs** uses machine learning and AI technologies to gather and share timely and consistently top-rated threat intelligence and related research.
- **ISA Global Cybersecurity Alliance** (ISAGCA) is a forum for advancing cybersecurity awareness, education, readiness, and knowledge sharing related to the ISA/IEC 62443 series of standards.
- **The Cyber Threat Alliance**, is a global digital ecosystem enabling near-real-time sharing of cyber threat intelligence among companies and organizations.

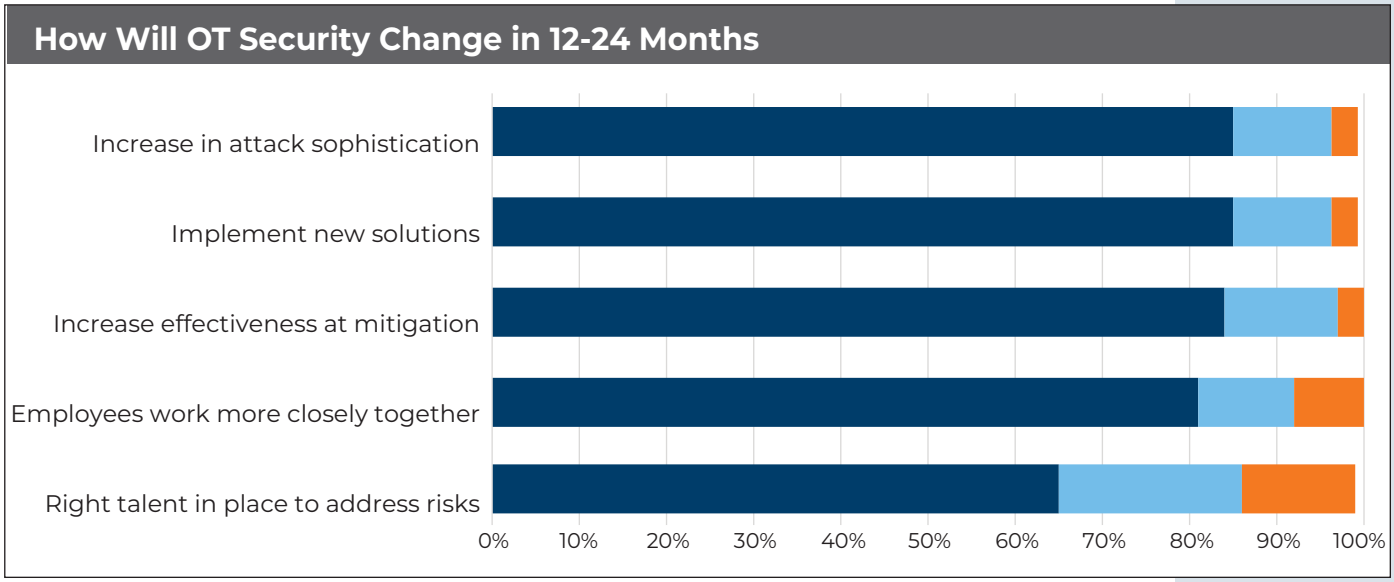
OUTLOOK

OT cyber threats and responses are fast-moving and volatile areas of activity, which means professionals in the oil & gas / petrochemical arena need to be both vigilant and ready to acquire new knowledge or skills.

As shown in Figure 4, survey respondents were generally positive about the outlook for OT cybersecurity in the next 12-24 months; more than 80% agreed that companies will implement new solutions and be increasingly effective at mitigating OT risks—even though they also agreed that cyberattacks will likely increase in sophistication.

Most respondents (85%) also predict that IT and OT employees would work more closely together going forward. Fewer (60%) agreed that their company would have the right talent in place to address risks, however, implying that staffing and OT-specific expertise will likely remain a challenge.

Figure 4. Respondents were asked whether they agreed or disagreed with statements describing how OT cybersecurity might change in the coming one to two years.



CONCLUSION

The results of this survey show an industry roughly split. About half of oil & gas / petrochemical companies are well on their way to what might be called a mature cybersecurity posture. They have completed most of the many steps and subtasks associated with OT systems protection, have systems in place to detect anomalies and monitor progress, and they have people and plans in place to adapt, improve and course correct. The other half of respondents seem to be just getting started. They have a range of plans and good intentions but not enough concrete implementations of protective tools, reliable procedures or knowledgeable partners. Most remain concerned about finding and training the right talent.

It is important for all members of an organization to do their part to create a secure OT environment. From management creating a supportive culture and implementing effective governance to trained frontline personnel recognizing and acting to fix vulnerabilities, each person must proactively seek to be part of the OT security solution.

References

1. Rockwell Automation and Cyentia Institute, **Anatomy of 100+ Cybersecurity Incidents in Industrial Operations** (August 2023)
2. DHS, **DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators** (May 27, 2021)
3. DHS, **Ratification of Security Directive** (September 24, 2021)
4. CISA, **Cyber Incident Reporting for Critical Infrastructure Act of 2022**
5. DHS, **DHS Issues Recommendations to Harmonize Cyber Incident Reporting for Critical Infrastructure Entities** (September 19, 2023)
6. Automation.com, **Cybersecurity in the Oil & Gas Sector: Securing the OT Environment. Spring 2023 Survey Results Report** (August 2023)
7. McKinsey & Company, **Organizational cyber maturity: A survey of industries** (August 2021)
8. Fortinet, **2023 State of Operational Technology and Cybersecurity Report** (May 2023)
9. International Society of Automation, **ISA/IEC 62443 series of standards**, resources and training
10. Takepoint Research, **TPR Survey Report: The State of Industrial Secure Remote Access** (2023)

About the Author

Renee Bassett is Chief Editor of Automation.com, a subsidiary of the International Society of Automation (ISA). Renee is a technology journalist with 20+ years' experience producing and managing content creation related to industrial automation, manufacturing, engineering and IT systems.

About Automation.com and ISA

Automation.com is the digital media subsidiary of the International Society of Automation (ISA). Automation.com publications include websites, digital magazines, newsletters and webinars for industrial, infrastructure and business professionals interested in automation, cybersecurity, digital transformation, Industry 4.0, IIoT, smart manufacturing, sustainability, and related topics. The International Society of Automation (isa.org) is the trusted provider of standards-based foundational technical resources. ISA created the ISA Global Cybersecurity Alliance (isa.org/ISAGCA) to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (isasecure.org) and the ISA Wireless Compliance Institute (isa100wci.org).

About Fortinet

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.