2018

Critical Infrastructure Risk Assessment

Industrial Control Systems Cybersecurity:

Survey of Engineering and Operational Technology Professionals

PARSONS

Overview

Parsons began this effort to explore the state of cybersecurity risk in critical infrastructure facilities with a simple question. The cyber threat has undoubtedly converged – both information technology (IT) and operational technology (OT) environments are being attacked. But, to what degree have solutions to this two-pronged threat actually converged?

Parsons is committed to shedding light on the stark differences between IT and OT cyber threats and implications. IT cyber-attacks are fundamentally tied to data, and the theft and nefarious use of stolen information. These risks are now well understood, following countless high-profile attacks on the likes of Sony, Equifax, Target and many other household names.

OT cyber threats and risks involve the machine environment in critical infrastructure facilities, and the now-proven potential to disrupt essential needs such as electricity, water, commercial aviation and even countries' national security apparatuses. It is no longer hyperbole or exaggeration to assert that cybersecurity is a matter of life and death.

This reality would likely be better understood if, for example, the crippling 2015 attack on the Ukraine electric grid's OT environment had taken place in Los Angeles, Riyad, or London. The March 2018 Russian cyber-attack on America's infrastructure, while stopped short of full-scale disruption of services, is the latest wake-up call.

> The IIoT reality inherently necessitates that OT machine engineers play a **vital role** in assuring critical infrastructure resilience from the **cyber threat**.

With over 90 percent of critical infrastructure assets in America owned by private sector interests, understanding the degree to which OT and IT cyber solutions have converged is not a matter of simply asking federal government officials for a report. The answer lies with employees, management and boards of directors of the companies and cooperatives that operate critical infrastructure assets. Countless studies and surveys have posed the IT/OT convergence question to the traditional source – the C-suite, where CEOs, CIOs, CISOs, CTOs and others in leadership positions manage organizations' operations.

This survey endeavors to explore the convergence question more deeply as it relates to critical infrastructure organizations' OT environments, where the Industrial Internet of Things (IIoT), wired, wireless and network-connected devices are being added at staggering rates. These devices – while dramatically improving efficiency, safety and operating capacity – are also at the center of the OT cyber defense imperative.

> Relying on a **purely IT-centric**, bolt-on software-model for protecting the OT environment is the equivalent of having a **mechanical engineer** in charge of cybersecurity for an organization's email servers.

The millions of connected industrial control systems (ICS), whether an older computer managing a smart HVAC system, or a state-of-the-art wireless meter helping control water flow in a nuclear plant, are the new target for cyber hackers. These ICS devices are typically sourced, procured, installed and managed by physical system engineers in the OT environment, not software engineers from the IT or information system (IS) departments.

The IIoT reality inherently necessitates that OT machine engineers play a vital role in assuring critical infrastructure resilience from the cyber threat. Relying on a purely IT-centric, bolt-on software-model for protecting the OT environment is the equivalent of having a mechanical engineer in charge of cybersecurity for an organization's email servers.

Understanding the degree to which organizations have truly converged IT and OT cybersecurity planning and implementation is best understood with the voice of the OT engineer included, along with IT, in the dialogue. Parsons is proud to release the first comprehensive exploration of this vitally important issue, from the perspective of professional engineers who share in the responsibility of keeping our communities and nations safe.

With the backdrop of exponential growth in IIoT device integration and increasingly sophisticated IT and OT cyber-attacks, to what degree are critical infrastructure organizations meeting the converged IT/OT cyber threat with effectively converged solutions? Is the IT-centric, software-based model still the predominant solution today?

Carey Smith
President, Parsons Federal

Key Findings

Parsons 3 Key Takeaways

The survey findings point to an alarming lack of collaboration between engineers, the OT environment experts, and IT experts who typically lead the cybersecurity function. Coupled with dramatic increases in the number of connected devices being added to the OT environment, cybersecurity resilience in critical infrastructure facilities is weakened by both process and technology hurdles.

Designing-in cybersecurity, as opposed to bolt-on software-centric approaches, requires the full integration of OT engineers responsible for the connected devices. Fully converged IT/OT cybersecurity solutions remain the goal, but is not the predominant scenario in today's critical infrastructure facilities.

Glossary of Relevant Terms

Industrial control systems: A general term that encompasses several types of control systems and associated instrumentation used for industrial process control.

SCADA: Supervisory control and data acquisition a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level supervisory management of industrial control systems.

Operational Technology (OT): Equipment found in many industrial and critical infrastructure settings that include devices such as valves, switches, actuators and other physical controls.

IIoT: Industrial Internet of Things. Devices in industrial settings that are connected to the Internet and/or internal networks.

66% of respondents indicate their organizations are adding more connected IIoT devices to industrial control systems in the OT environment, in addition to connected devices already in place.

80% indicate their OT environments are utilizing a mix of either old technologies, new ones, or both. Many of today's new network-connected IIoT devices bring added cybersecurity protections. **Old technologies either do not have cyber protections or rely on outdated methods such as software patches that are no longer resistant to attack.**

78% of respondents indicate that they are not "highly involved" in industrial control system cybersecurity. **Fully converged IT/OT processes, people and solutions to critical infrastructure resilience are rarely in place today.**

Detailed Survey Results

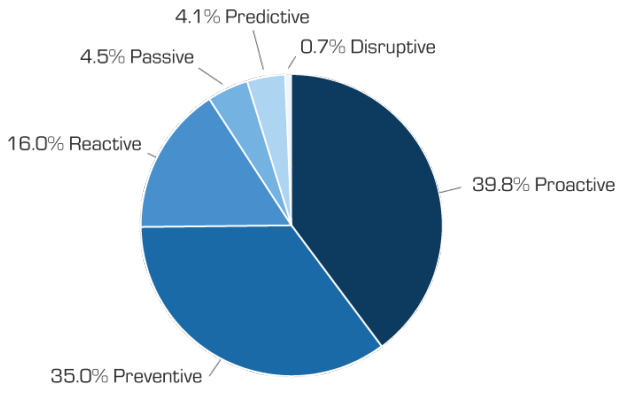
In a survey of engineers working in critical infrastructure environments, Parsons found that a majority of OT professionals credit their organizations with making cybersecurity a high priority for day-to-day operations. Further exploration of survey responses provides valuable insight into a sector-wide lack of preparation, coordination and education regarding OT vulnerability to hackers and other Digital Age threats.

Preparedness & Maturity

Nearly two-thirds of professionals say their organization has a cybersecurity posture that is preventive or proactive. Despite this level of preparedness, it does not reflect the defense posture of the respondents' OT against the same cyber threats.

> "Do a detailed audit of all current assets and systems. Know what you have and **challenge your organization** to know what is being done to **protect those assets**."
> – *Survey Respondent*

How would you gauge your organization's state of cybersecurity maturity?

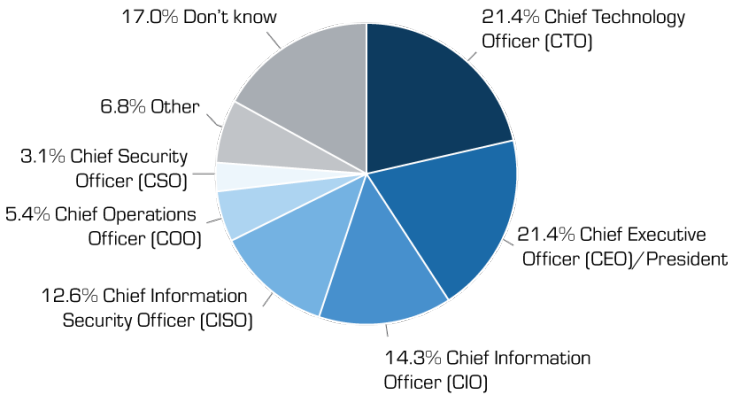


Fractured Oversight

Respondents identified a variety of C-suite roles with responsibility for ICS, including those traditionally associated with IT. Nearly 20 percent claim ICS accountability lies with the CEO – a position too broadly defined in most businesses to include a specialty-level focus on OT cyber threats.

> "Senior management must recognize the importance of **securing industrial systems** and **allocate resources** accordingly."
> – *Survey Respondent*

At the senior management level of your organization, which of the following has primary responsibility for industrial control systems (ICS) cybersecurity?

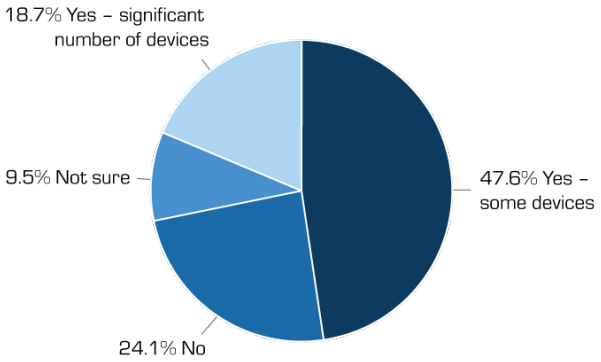


Integration of OT Devices & Technologies

Not surprisingly, most professionals say their OT is connected to the Internet or networked in some fashion. But 24 percent also claim that none of their tech is connected, which is unlikely to be true. In today's internet-of-everything environment, operators must presume their OT devices are Wi-Fi and/or Internet enabled.

"The playing field is **not level**. We have to guard all areas; hackers only have to hit the **weakest link**."
– *Survey respondent*

Is your department or other operational (non-IT) areas of your organization integrating new Industrial Internet of Things (IIoT) devices or automation technologies that connect to IT or operational technology (OT) networks?

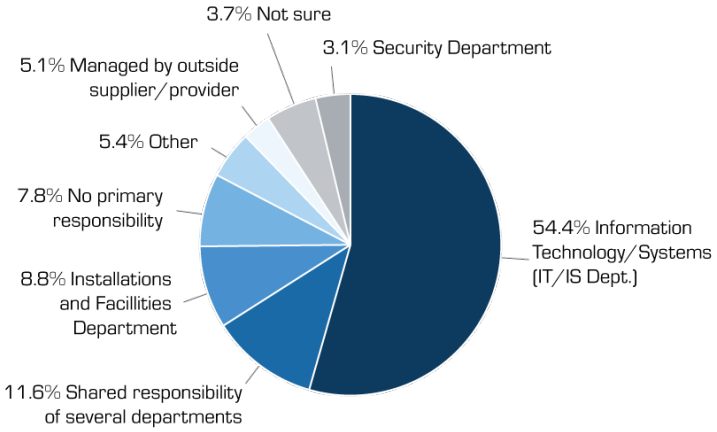


IT Departments in the Lead

A great deal of cybersecurity expertise resides with IT professionals, but most are new to OT or unfamiliar with common types of OT equipment and systems. The key to effective OT defense is a full convergence of IT and OT capabilities in defense of systems vulnerable to threats from cyberspace.

"Don't assume that your **IT department** security function will **protect your OT**."
– *Survey respondent*

For day-to-day ICS cybersecurity management and processes, which area/department in your organization has primary responsibility?

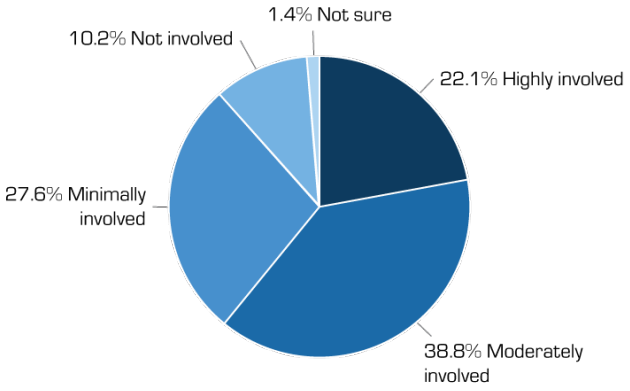


OT Professionals on the Sidelines

An alarming 78 percent of respondents are not "highly involved" in ICS cybersecurity planning and implementation. Effective IT /OT convergence requires collaboration among engineering, information technology, operations, and business functions.

"Offer **comprehensive and ongoing** cyber-security training covering an overview of company Industrial Control Systems, Risk Management & Assessment, Security Program Development & Deployment. Include discussions regarding the **security architecture** used and how security controls have been applied."
– *Survey Respondent*

Which best describes your role and the role of other operational engineers (non-IT professionals) relative to ICS cybersecurity planning and implementation?

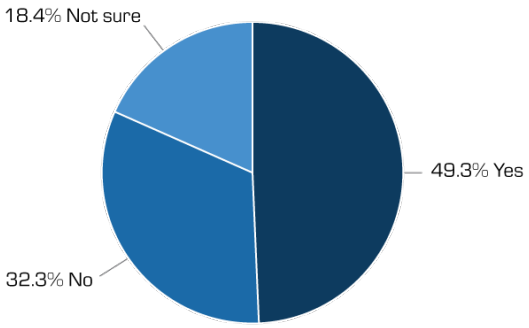


Outdated Hardware and Software

Survey respondents acknowledge the risk posed by legacy hardware, software and systems. Mitigating the risk in the OT environment from legacy IT can be complex and expensive. By the time a downstream risk to OT is exposed, organizations may be faced with adopting bolt-on security solutions or costly replacement of vital OT components.

"Make sure new equipment is the **latest technology**, get rid of old hardware, train and require outside vendors to **understand and properly configure** new equipment to be safe."
– *Survey Respondent*

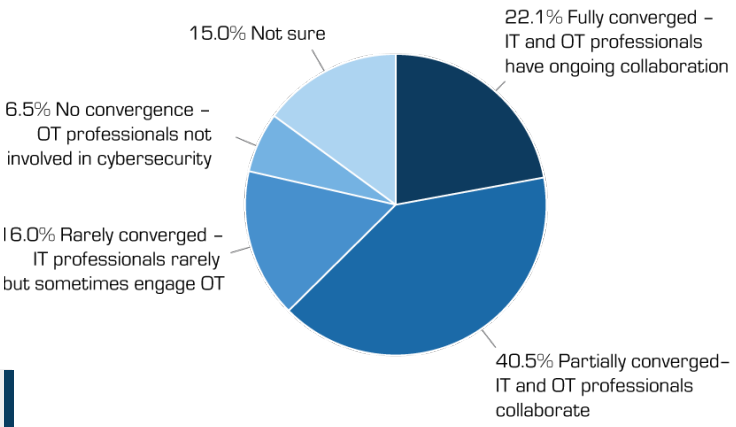
Do you believe that industrial control systems, such as SCADA computers, local operator stations, PLCs, RTUs, etc., in the operational arenas of your organization are at risk for cyber-attack because outdated hardware or software is being used?



Lack of OT/IT Convergence

Only 22 percent describe their organization's IT/OT cybersecurity model as "fully converged." Even a "partially converged" approach poses risk – a response indicated by 40 percent of those surveyed – and indicates that many OT professionals are still not collaborating on a regular basis with their IT counterparts.

Which of the following options best describes your organization's cybersecurity model relative to protecting operational areas?

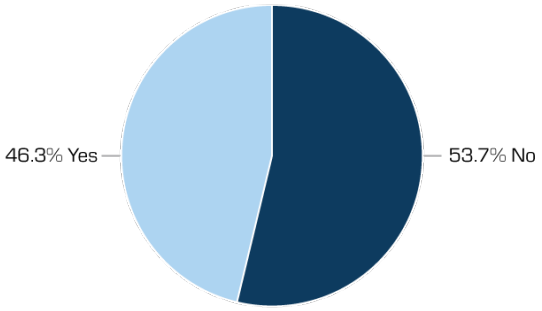


> "Cybersecurity should be conceptualized at the project predesign stage, NOT after project completion (as an afterthought). From personal experience, project predesign stage cybersecurity design **costs '1X'**, while post-project completion cybersecurity design costs **'5X' to over '10X'** (and even more)."
> – *Survey Respondent*

Need for Trained OT Professionals

A majority of OT professionals say they have received no cybersecurity training. While IT cybersecurity training is prevalent across industry sectors, it is imperative that investments be made in OT cybersecurity training for engineers and other stakeholders working in ICS ecosystems.

Have you ever received cybersecurity training specific to operational technology or industrial control systems (as opposed to email and other IT functions)?



> "(IT personnel) should train on **OT industrial control system cybersecurity**, such as SCADA computers, local operator stations, PLCs and RTUs."
> – *Survey Respondent*

Conclusions & Recommendations

The Imperative for OT/IT Convergence

Among engineering professionals, awareness of OT vulnerabilities from cyberspace remains high, but standards and practices among their colleagues in IT departments and C-suites are not keeping pace with rapidly-evolving threats. With hackers and other nefarious players adapting their means of attack at nearly exponential rates, stakeholders charged with safeguarding critical infrastructure have no time to lose. Recommendations based on our findings include:

- **Define IT/OT convergence.** We asked survey respondents to characterize OT/IT cybersecurity convergence based on personal knowledge and experience, but a widely-accepted definition of convergence is lacking among critical infrastructure stakeholders. A set of definitions and standards must be developed for stakeholders from across critical infrastructure domains to advance the common cause of OT cybersecurity.

- **Invest in training.** Critical infrastructure organizations must invest in training and education to increase the cybersecurity capabilities of OT engineers and professionals. Training will increase the effectiveness of OT/IT collaboration and help guarantee that OT gets a seat at the table with regard to cybersecurity planning and resource allocation.

- **OT cybersecurity by design.** OT cybersecurity is too often seen as a challenge to be solved with bolt-on solutions to outdated or legacy equipment. Moving forward, organizations should instead incorporate OT cybersecurity into the design process for new and upgraded OT systems.

- **Organize for OT cybersecurity.** Leadership and management teams should be configured to address IT/OT vulnerabilities. This requires an end to the practice of stove-piping cybersecurity inside a single component such as IT or the CIO's office, and formulating standing practices for collaboration across relevant IT and OT divisions.

- **Encourage dialogue.** Critical infrastructure stakeholders must do their part to encourage additional study, information-sharing and industry-wide dialogue regarding cybersecurity and OT vulnerabilities.

As more OT devices and systems are connected by the Internet of Things and networked into digital environments every day, information management platforms, intrusions, attacks and disruptions will inevitably follow. **The time to act is now.**

For more information, please email us at: domain6@parsons.com

Parsons
100 West Walnut Street
Pasadena, California 91124
www.parsons.com

Methodology & Background

In April 2018, Parsons conducted an anonymous, on-line survey of more than fifteen types of engineers working in the operational technology areas of critical infrastructure organizations. Utilizing a database of engineers owned by CFE Media, publisher of several magazines designed specifically for engineers, a large sampling of 300 qualified respondents was achieved during the two weeks the survey was deployed.

Participation in the survey was purely voluntary, and no incentive or benefit of any kind was offered to survey respondents. All survey questions and possible responses in this report are identical to the survey itself. In addition to direct, quantifiable answers to the survey questions, several questions included the opportunity to provide qualitative answers as well. Some of the quotes from responding engineers are referenced in this report.

All text, images, charts and content, reproduced or quoted partially or in full, from this report must be attributed to: Parsons 2018 OT Cybersecurity Survey.

Respondent Disciplines

Electrical Engineers:	26.2%
Mechanical Engineers:	8.2%
Controls Engineer:	7.5%
Project Engineer:	5.4%
Engineering Manager:	5.4%
Design Engineer:	3.7%
HVAC Engineer:	3.7%
Automation Engineer:	3.7%
System Engineer:	3.4%
Civil Engineer:	3.4%
Facilities Engineer:	2.7%
Electronics Engineer:	2.4%
Manufacturing Engineer:	2.4%
Fire Protection Engineer:	2.4%
Other:	21.8%

Respondent Sectors

Commercial Facilities:	19.7%
Energy:	17.0%
Chemical:	10.5%
Government Facilities:	8.5%
Water & Wastewater Systems:	8.5%
Information Technology:	7.8%
Healthcare and Public Health:	3.7%
Defense Industrial Base:	4.8%
Critical Manufacturing:	4.4%
Transportation Systems:	4.4%
Communications:	3.1%
Food & Agriculture:	2.0%
Nuclear Reactors, Materials & Waste:	1.4%
Emergency Services:	1.0%
Dams:	0.3%