Deloitte.

Future forward readiness

Securing Operational Technology (OT)

Cybersecurity is not just an IT issue. These days, manufacturers, power and utility operators, energy companies, logistics providers, and many others are increasingly becoming targets of cyberattacks targeting OT.

Current trends and potential challenges

- Protecting mission-critical operations from cyber criminals and nation states is urgent
- Many organizations realize they are targets and are seeking to deploy cybersecurity and risk management systems that address the evolving threat landscape
- There is an increase in regulatory oversight, especially following recent high-profile cyberattacks
- Cyber talent is scarce and in high demand, especially for OT
- Many organizations have increasingly complex IT/OT ecosystems with distributed operations, including remote workforces, and third-party connectivity
- Companies face cyber threats to the Operational Technology (OT) systems that control their operations. These threats could disrupt the supply of essential goods and services resulting in regional or national economic and geopolitical impacts.

Desired outcomes

Address today's OT cybersecurity risks while helping prepare for the future with a suite of end-to-end services rooted in a consequence-based, risk-centric methodology and aligned with industry accepted standards. Benefits include:

- **Improved security & compliance:** Assessments so you may carefully gauge security gaps/maturity, vulnerabilities, and regulatory compliance
- **Safety first:** Proactively analyze and quantify cybersecurity risks that threaten the safety and reliability of your operations through our cyber-safety assessments (i.e., Cyber Process Hazards Analysis - Cyber PHA)
- **Enhanced security profile:** Take your Cyber program to the next level through our advanced OT security studies, such as vulnerability rationalization, attack path modeling, cyber factory, and site acceptance testing, as well as penetration testing.
- **Right-sized security program:** Deloitte provides a tailored OT program development based on your different risk tolerance and readiness capacity, including OT cybersecurity frameworks, policies, standards, procedures, job aids, and training.
- **Improved technology investments:** Get more from your technology investments through our services to help you evaluate, select, design, deploy, improve, and document a variety of OT cybersecurity technologies.
- **24/7 monitoring and response**: Operational assistance for monitoring, incident response, threat hunting, asset, and vulnerability management.

Future Forward Readiness

Deloitte can help you achieve an enhanced security posture as threats and disruptions grow. With services across the advise, implement, and operate spectrum, Deloitte can help forge a better balance between safety, security, quality, and usability to maintain the security of the products you manufacture and the environments you operate.

Cyber OT in action

OT Cybersecurity Programs

Deloitte has helped organizations, large and small, develop and implement their OT cybersecurity programs. Our approach typically starts with a high-level risk assessment to help the organization understand their operational cybersecurity risks, risk tolerance, and target profile(s). We then work closely with the stakeholders to establish roadmaps and governance materials (e.g., policies, standards, procedures, job aids, and employee/supplier training).

OT and IoT Technology Selection and Deployment

Deloitte helps our clients evaluate, select, design, deploy and maintain a wide variety of OT and IoT cybersecurity technology. Examples include IoT detection systems, endpoint security, vulnerability identification and more. Our technology-enabled services coupled with our extensive network of alliances enable us to provide leading approaches.

Vulnerability Rationalization

In response to our clients' challenges in managing the ever-growing number of vulnerabilities in their OT systems, Deloitte developed a risk-based approach to rationalize cybersecurity vulnerabilities we call Vulnerability Rationalization. The methodology extends the established framework of Common Vulnerability Scoring System (CVSS) to consider safety, environmental, and business consequences, helping clients prioritize what vulnerabilities to treat, terminate, transfer, or tolerate within their OT systems

OT Security Acceptance Testing

It is critical that new or recently updated OT systems be tested to determine if the implementation addresses security requirements and follows industry standards and leading practices. Deloitte offers cybersecurity acceptance testing before the system is shipped. Acceptance testing incorporates numerous test steps to analyze items such as passwords, user accounts, port security, device hardening, network management, switch/firewall security, controller write protection, and network segmentation.

Consequence-based Risk Assessments for Operational Technology (OT) in Critical Infrastructure Sectors

Deloitte employees pioneered the development of the Cyber Process Hazards Analysis (PHA) methodology of performing industrial control and automation system (IACS) cybersecurity risk assessments as specified in international standards. The Cyber PHA methodology uniquely evaluates multiple combinations of threats, vulnerabilities, and consequences to provide leadership with a broad view and ranking of the operational risks (e.g., health, safety, environment, business interruption, equipment damage, off-spec product) associated with a cyber incident.

Turn complex challenges into opportunities

Our industry-tailored approach enables us to apply the applicable recommendations to your precise business challenges.

When you're looking for global leadership
Deloitte is recognized as a global leader in the OT and IoT cybersecurity market. With our strong experience we provide guidance to the world's largest companies.

When you need a strong ecosystem of alliances
We have strong alliances with leading technology vendors.

When you need a one-stop shop
While navigating the uncertainties of OT security, the breadth of our services allows us to provide you with an expansive solution to help you achieve the outcomes critical to your organization.

We're well positioned to help you achieve your objectives

Wherever you are in your journey, we have the experience, knowledge, and tools to help move your organization forward.

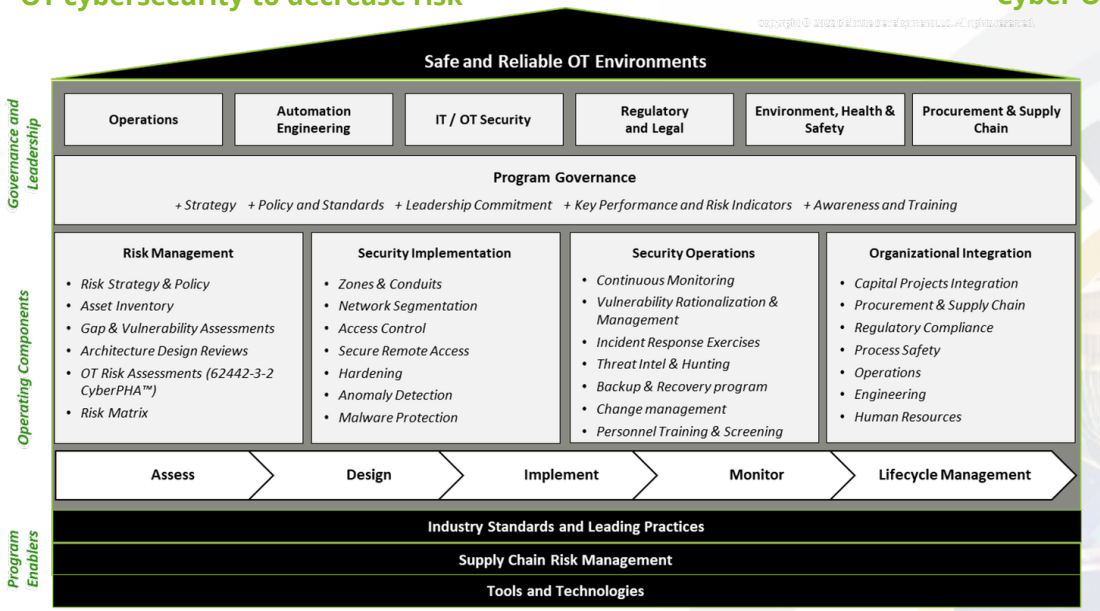
Outcomes-driven
In the face of growing complexity, we make finding an OT security provider easy. Our breadth and depth allow us to provide the outcomes (and value) you seek as a trusted advisor, a technology-savvy pioneer, a visionary integrator, and a dependable operator. We connect the dots, so you don't have to—helping you to improve security, trust, and resilience.

Quality-oriented
We bring together a powerful combination of proprietary technology, domain experience, leading alliances, and industry knowledge. Our obsession with quality means we consistently work to help you realize your vision, because preventing and mitigating OT security risks are mission critical.

Value-focused
We act as a leader in times of crisis, a teammate to help you navigate change, and a force to have your back when you are on the front lines. We create value for our clients beyond the deal, pioneering cutting edge resources and innovation, paving the way for forward leaning collaboration, and leading bold thinking on tomorrow's emerging technologies so you can turn risks into opportunities.

Future forward readiness

OT cybersecurity to decrease risk



Cyber OT in action

OT Security

- OT security program design, development, implementation
- OT security program maturity assessment
- OT security vulnerability rationalization and management
- OT security design and implementation
- OT Security regulatory compliance and readiness
- OT security tool evaluation
- OT security detection tool architecture, deployment, and configuration
- OT security training
- OT managed security services

Engineered for

- Organizations that design OT systems
- Organizations that manufacture, distribute and maintain OT systems
- Organizations that integrate OT into systems and ecosystems
- Organizations that use OT for safe and reliable operations
- Organizations deploying OT to transform and improve their business
- Organizations responsible for management of smart factories

Start the conversation

Wendy Frank
Principal, Cyber IoT Practice Leader
Deloitte and Touch LLP
wfrank@deloitte.com

Russell Jones
Partner, OT Security Leader
Deloitte and Touch LLP
rujones@deloitte.com

Ramsey Hajj
Principal, OT Security Leader
Deloitte and Touch LLP
rhajj@deloitte.com

John Cusimano
Managing Director, OT Security Leader
Deloitte and Touch LLP
jcusimano@deloitte.com