Operational technology security in the Energy and Utilities industry

Points of view and takeaways from industry CIOs

October 2022

Casey Werth, Global Industry Leader | Energy Industry | IBM

Rob Dyson, Security Services Consulting & Systems Integration Competency Leader | IBM

Steve Dougherty, Associate Partner, Energy, Environment & Utilities | IBM

Jessica French, Field Marketing Professional | Energy & Utilities | IBM

Context

Five chief information officers (CIOs) from energy and utility companies, and two security leaders in their organizations, met at The IBM CIO Roundtable to discuss how CIOs in the industry are responding to the increased focus on operational technology (OT) as a part of a broader cybersecurity strategy, and its relationship to IT.

Topics from the discussion included OT security and governance, a cultural shift, OT threats and security, and both external and internal threats.

The IBM CIO Roundtables provide an opportunity to share leading practices and discuss topics of mutual interest based on an agenda created through advance interviews.

Contact your IBM representative if you are interested in participating in the next IBM CIO Roundtable.

Quotes from the E&U IBM CIO Roundtable

Governing OT security

“The new regulations really are only about managing risk, and then in looking at the governance. We’ve been responding by modifying our infrastructure and operations since 2015 onwards. So, we were a little bit ahead of our peers in the industry, insofar as we’d already thought about governing OT security before it was a legal requirement, to really start managing the risks.”

IT and OT governance

“The first thing is there will be tension between IT and OT around governance. I think it has to do with control. I think that for whatever reason there’s a view, especially from engineers, that if I don’t control it myself, it’s not going to work the way it should.”

Accountability

“We follow the RACI, but it’s about people. And our next piece is about execution on not just ownership and governance, but accountability. So, we’re bringing that craft team together, and our operating engineers together, and the network operations center, all with equal accountability. And it’s not going well, because they’re learning to work together in ways that they never had to before.”

Cross-train IT and OT professionals

“One of the key things we've done is taken some of our best trained security resources and staffed them in what is more of the OT space. The RACI responsibilities just look different, and that's actually proven a lot of mileage for us in regard to changing the way we think about things. Identifying just what is a digital asset in our industry is going to be a continued challenge for all of us. People may not see the keypads into the substation as a digital asset, and they may not see drones as a digital asset, but all those items are digital assets that we have to secure and protect.”

Critical infrastructure attacks

“You can look at almost every intelligence survey that comes out. And the nice thing to see is that they all agree. And the leading attacks today are on critical infrastructure. So, it’s in those industrial environments. It’s not as much in the corporate space anymore.”

Market context

OT security programs in energy and utilities

Companies that operate within the energy and utilities sector provide product and services that are classified as critical infrastructure. Operational technology environments include all technologies within an industrial environment, traditional IT technologies, and specific operational technology products (see examples on the right).

Because E&U companies are modernizing these environments to become more efficient, effective, and competitive while providing new products and services to their customers, these environments have become vulnerable to cyberattacks.

In addition, due to the global geo-political situation, nation states are increasingly leveraging cyber-attack techniques to conduct cyber warfare with a goal of crippling their target's critical infrastructure. In 2021, the IBM® Threat Intelligence team found that most attacks were focused on the OT environments.

Operational technology environments include

Industrial technologies	• Industrial Control Systems (ICS) • Process Control Systems (PCS) • Supervisory Control and Data Acquisition (SCADA)
Traditional IT technologies	• Servers, firewalls, databases, network switches, routers, and others
Specific OT products	• Distributed Control System (DCS) • Programmable Logic Controllers (PLC)

OT security programs are highly complex for E&U

The eight domains below demonstrate what a comprehensive security program covers—those in blue highlight the NERC CIP requirements to prioritize for E&U compliance.

Security program domains	NERC CIP regulation areas	Complementary areas for security programs		
Security monitoring and intelligence	• Emergency response • Incident response • SOC operations • Threat response • Vulnerability management	CSIRT Data analysis and forensics Intelligence sources Platform administration Predictive analysis	Reporting Threat monitoring Threat research Threat triage Use case management	
Security governance, risk, and compliance management	• Awareness • Continuity and disaster recovery • Risk assessment • Risk objectives • Supplier management	Audit Compliance Policy Privacy	Program management Recruit and training Strategy planning	
Systems and infrastructure security	• Patch management • Physical • Secure disposal	Cloud (CASB) DDoS Embedded and industrial Endpoint (EDR)	Endpoint (HIPS) Endpoint (NGAV) IPS / IDS Messaging	Network access (NAC) Storage Web application Web gateway and proxy
Service management, planning, reporting and operations	• Asset management • Configuration management	Change management Continuous improvement Measure & report Platform administration Problem management	Service catalog Service design Service management Service operation	Service transition Software asset management Software management Strategy and planning
Identity and access management	• Access administration • Privileged access management	Access control Cloud identity and access management	Identity administration Reporting	
Data security	• Critical data protection	Big data security Cloud data security Cryptography	Data access management Data governance Data leak prevention	Database security Discovery and classification
Application security	• Secure engineering	Business app security CTS (spell out CTS) and SaaS security Mobile app security	SDLC security Secure design review	Static and dynamic testing Threat modeling
Security architecture		Asset creation and reuse Assurance Business and IT alignment Components and subsystems	Integration Methods Modeling Policy enforcement	Solution design and testing Standards Transition roadmap Vendor selection

OT security assessments

Many companies are re-adjusting their OT journey or strategy through various maturity assessments. Re-assessments are driven by new risks and scenarios such as increased digitalization, global events and threats, climate change pressures, evolving transportation electrification, and exponential technologies and enablers such as 5G and IoT. See a sample of OT assessments that are commonly being re-visited by E&U below.

OT security assessments include:

Compliance	• Framework: ISO/IEC 62443 or NIST CSF • Regulatory: NERC CIP • OT hardware and device penetration and vulnerability analysis
OT security program	• IBM 10 Essential Practices (EP) security framework • OT security user access review • DoE's C2M2v2 maturity model • Framework and architecture assessments
Technical OT infrastructure	• Leverage OT-IDS products • MITRE ATT&CK for OT (can it detect attacks) • Framework and architecture assessments
OT security risk	• Quantitative (automated risk scoring software for OT networks) • Qualitative (no special tools required) • OT risk quantification on a NERC CIP infrastructure • Smart meter security assessments

Assessments are needed at the start and end of the OT security journey for E&U companies. They help to gather insights on governance and assess risk, compliance, threats, and vulnerabilities. Assessments also support continuous improvement to help identify needed enhancements or changes.

OT security program governance

E&U companies are missing the necessary OT security program governance to be prepared for security-related incidents. Governance is challenging for E&U—NERC CIP applies to multiple different divisions, such as IT, OT, HR, physical security, network security, and legal and there is a gap in connecting them all together.

OT security program governance areas include:

Organization	• OT security roles and responsibilities • OT security skills for OT security functions • OT security incident response
Process	• Documented OT security processes • OT security framework alignment • OT security process training
Technology	• Tools and tech aligned to OT security objectives
Metrics and reporting	• Defined metrics (key risk indicators and KPIs) to measure OT security program success • Defined reporting and stakeholder updates

To help support governance, many E&U organizations use a RACI model, which indicates the parties that are responsible, accountable, consulted, and informed on decisions. The most successful RACIs will be co-developed with cross-department teams, representing security, industry operations and technology professionals. They join forces to anticipate security-related events such as a breach, break-in or hacker and ensure that the RACI is equipped to take it on. The RACI should align to the security program domains and be reviewed consistently.

To hear directly from E&U CIOs that participated in the roundtable, continue to the next section.

RACI for OT security governance in E&U (illustrative example)

RACI charts are a useful exercise to structure a program, but the RACI must be operationalized to ensure effectiveness.

Activities of a security program	Dedicated security team				Industry operations team				Technology org team			
(roles)	Role 1	Role 2	Role 3	Role 4	Role 1	Role 2	Role 3	Role 4	Role 1	Role 2	Role 3	Role 4
Monitoring	R	R	A	I					R	R		I
Investigations	C	R		I			I		C	C	A	I
Response		R		I			I		C	C	A	I
Computer security incident response team (CSIRT)			R	I			I				A	I
Cyberthreat intelligence		R	A	I								I
Security control administration and engineering			A	I		I			R	R	I	
SIEM administration and engineering		C	A	I		I			C	C	I	
Service delivery and operations development					C	R	A	I				I
Security analytics and incident reporting		C	C	I	C	R	I				A	I
Security integration		R	A	I	C	C	I		C	R	R	I

R (Responsible)	A (Accountable)	C (Consulted)	I (Informed)
Has the obligation to do the work and duty to exercise independent judgment to raise appropriate issues.	Has the authority to decide and is the recipient of any consequences. There can only be one "A" per process step.	Must be given the opportunity to influence plans and decisions prior to finalization by the "Responsible" party.	Is informed of progress, key decisions and deliverables by the "Responsible" party.

CIO Roundtable takeaways

OT security and governance

Technology is increasingly becoming a key component of every industry. CIOs in the energy and utilities sphere are tasked with taking more responsibility and providing more security for operational technology as threats to operations would impact critical infrastructure. Utilities are changing the way they approach governance of IT and OT from a cybersecurity perspective, with many OT functions moving under IT. This folding in of OT is a very challenging process for CIOs, and one that involves time and patience.

Several CIOs mentioned that their companies are using a RACI model to help inform and implement governance around OT. RACI stands for responsible, accountable, consulted, and informed to indicate the level of ownership and different roles that various personnel have in the governance of OT. As one executive explained, from a decision-making perspective, there's buy-in and everyone is on board, but in the execution is where the resistance lies—"that's where the rubber meets the road." Most companies have IT and cybersecurity governance functions oversight at the Board of Directors level, and the CIOs report to those special committees.

Achieving buy-in

A key challenge in enhancing security in the OT area comes in generating interest and buy-in from the board. The anxiety around increasing security risks is driven top-down from the senior level. One CIO had success creating a board security philosophy that incorporates a convergence of both IT and OT, and subsequently incorporating an enterprise security group of directors responsible for both.

It can be helpful to approach risk quantification to message the risk element of cybersecurity to drive the business case to achieve buy-in. The OT security expert reinforced that identifying the relevant threats, which are constantly evolving, is the best way to approach a quantitative risk approach and develop a road map that will represent the business case when seeking budget to support a broader cybersecurity strategy.

There is some responsibility for security leaders to educate the regulators to help them understand how technology is evolving, and where technology will help cover risk. Regulators understand and think about cybersecurity in the personal lives but are more focused on physical security as they view their professional domain. Cybersecurity must be conveyed to regulators as being of equal importance to physical security.

Industry trends of the North American grid

E&U leaders are faced with new roles and responsibilities, burnout, tool sprawl, continuous expansion, outdated and new regulations, and blockers to their transformation.

New dedicated leaders	• Chief security and privacy officers (former FBI and DoD managing agents) • Physical security, cybersecurity, investigations – may have operations OT and IoT
Increasing responsibility	• CIO or chief technology officer assuming more control over operations infrastructure such as cloud, IoT adopt IP, budget and tooling • Creation of the Grid Security VP, peer of CSO specifically dealing with operations and grid compliance
Facing burnout	• 3-year chief security officer and chief information security officer life span • Lack of resources to manage rapid transformation across IT and OT • Loss of confidence to adapt and maintain security capabilities by C-levels
Tool sprawl concerns	• Too many redundant tools and shelf-ware add complexity • Desire ongoing support and financial investments and DoD / Financial Services grade security • Silos exist even in OT – metering, distribution, transmission, control and generation
Continuous expansion	• New electric vehicle infrastructure, Distributed Generation Resources (DERs), more intelligence in low voltage distribution network (ADMS) • Multiple resources integrating with energy markets – AMI, commercial EMS
Regulation pressures	• NERC CIP regulations are dated and not manageable with technology advancements paired with advanced Tactics, Techniques, and Procedures (TTPs) • FERC posing new requirements for internal network monitoring to supplement monitoring at the edge gateways of ESPs
Transformation blockers	• Knowledge that CapEx is a priority of transformation and change and key to lower OpEx and cost recovery through rate base • The pace of transformation is making security architecture, documentation and SecDevOps lost arts

OT threats and security

Where critical infrastructure is concerned, cyberthreats to OT are much more of a prevalent risk than most people understand. One CIO cited a survey by Gartner that had revealed that 25% of all cyberthreats are to OT, using ransomware. Many CIOs are in the process of educating their companies' teams so that they understand that the threats are real.

One leader shared the irony that most of the engineers and operations team members probably take cyberthreats seriously in their personal lives at home, because that seems more real and tangible; for example, if their phone gets hacked or their bank has a data breach. However, in the work setting, the same employees don't view security as their job.

Energy and utilities CIOs are also working to identify relative threats and quantify the risk, because, while risks can come out of the blue at any time, it is impossible to guard 100% against every threat imaginable. Instead, CIOs are looking to assess the threat levels, prioritize security, and quantify companies' digital assets.

External and internal threats—one of the roundtable subject matter experts pointed out that, although the situation in Ukraine puts Russia top of mind as a threat actor in the current geopolitical climate, China may actually pose a bigger threat. They warned that China systematically is helping cybercriminals obtain IT and OT positions with energy companies abroad in order to sabotage the infrastructure from within. This raises the risks around hiring, as companies need to look closely at who they're hiring.

A cultural shift

An executive described all the steps their company has been taking to implement the RACI model, but observed that, in the end, it's about people. In the utilities industry, engineers have been accustomed to working in operations, and they resist being moved into IT. In addition, engineers are used to being more hands on with operations and may not understand how their job relates to cybersecurity threats.

Because this kind of organizational change involves a shift in thinking and culture, it takes time. Several executives shared how their companies are getting very clear on roles and responsibilities, but also working to educate and integrate different IT and operational functions that haven't worked together in the past.

One CIO has had success treating the importance of OT security the same as they do safety in general. They bundle communications and messaging about the importance of safety and cybersecurity together and disseminate it to all employees. Similar to physical security, to be successful with OT security, any messaging must be accompanied by extensive training as well.

OT security program activities for E&U

Leading OT security programs are a continuum of integrated activities.

Insight	Prevention	Detection	Response	Recovery
Governance and continuous process improvement	Metrics and reporting	Issue management	Change management	Enhancements
• Device discovery • Data discovery and classification • User identification and classification • Process baseline analysis • Risk assessments • Compliance assessments • Threat assessments • Vulnerability assessments	• Network segmentation • Access controls –Privileged access –Remote access • Data protection • Application security • Endpoint hygiene –Patching –Configuration management. –Naming conventions • Security awareness training	• Identify vulnerabilities • Identify exploitation mechanism • 24x7 operations • Alert enrichment • Business context • Use cases • SIEM rule optimization • Reporting	• Incident response and management • IR playbooks • IR retainer • Simulations and training • Crisis communication • Remediate control gaps • Reporting	• Remediation plans • BC/DR program integration • Supplier activity management • After-action review Update security plans • Co-ordinate with third parties • Training

Conclusion

IBM CIO Roundtables provide a forum for E&U leaders to address various topics around the digital technologies that transform and power their businesses—such as automation, security and data.

Contact your IBM representative today if you would like to participate in the next IBM CIO Roundtable for E&U.

© Copyright IBM Corporation 2022

IBM Corporation
New Orchard Road, Armonk, NY, 10504 Produced in the United States of America

October 2022

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.