What Every Operator Needs to Know About Operational Technology Cybersecurity

Steve Mustard and Jim Schultz

Knowledge	Principles	Practical Considerations
What is operational technology?	Operational technology (OT) is used to monitor and control processes in industrial environments, such as water and wastewater treatment facilities, factory floors, refineries, and oil and gas platforms. Examples of OT equipment include ■ distributed control systems (DCSs), ■ supervisory control and data acquisition (SCADA) systems, ■ historian databases, and ■ protocol and media converters.	System availability is the primary concern, followed by integrity of the data, and finally data confidentiality. In OT, data integrity and confidentiality are particularly important for device logic or configuration files used in control applications. It can be difficult to take equipment out of service to update. Equipment and communications protocols tend to be proprietary, and it can be difficult to implement typical cybersecurity controls. Underlying technology can be very old and lacking much-needed security features and updates, making it more vulnerable to basic cybersecurity incidents. The equipment environment is almost always heterogeneous, with devices of various ages and sources.
What is the "system unavailability" risk?	Computer viruses can be downloaded onto information technology (IT) workstations, laptops, and servers remotely (using unauthorized access or through the use of social engineering) or using removable media, such as USB drives, CDs, and DVDs. Viruses can propagate across a network to infect other machines. Viruses may be used to ■ obtain confidential information (such as usernames and passwords), ■ cause excessive network traffic that disrupts normal operation, ■ wipe an entire hard disk clean, or ■ lock a disk until a ransom is paid.	In 2017, malware was deployed to a safety instrumented system controller in a refinery in the Middle East. The malware caused the system to trip and shut down the facility. The malware would not have been deployed had the operators kept the controller key switch in the correct position, a basic operational procedure. This attack illustrates why availability (safety in this case and many others) is the top cybersecurity objective in OT.
What is the "operations or production shutdown" risk?	Because operations or production are heavily dependent on the OT systems that monitor and control them, a failure of these systems can result in a shutdown of the facility or process. Typical cybersecurity causes are ■ viruses; ■ unauthorized access; and ■ lack of backup of system data, programs, or settings.	In 2021, the Colonial Pipeline was shut down for longer than a week after ransomware was deployed on its billing system. This caused major disruption to fuel supply in the Eastern U.S. The attack occurred through an insecure remote-access connection. The attack was aimed at IT infrastructure, but OT was shut down out of an abundance of caution.

Knowledge	Principles	Practical Considerations
What is the "service outage" risk?	In a specific instance of operations or production shutdown, the result can have serious ramifications for others, for example, the loss of water or wastewater services, the loss of communications, etc. Typical cybersecurity causes are ■ viruses; ■ unauthorized access; and ■ lack of backup of system data, program, or settings.	In 2015, hackers infiltrated the control system of a Ukrainian power company and took control of the electricity distribution network. Approximately 80,000 homes were left without electricity for up to 6 hours. Similar outcomes are possible in water and wastewater systems in the form of insufficient fire flow, boil water alerts, overdosing chemicals, treatment bypass, etc.
What is the "equipment damage" risk?	Production or operational facility is connected to the monitoring and control systems that can be affected by a cybersecurity incident. Without adequate mechanical or independent shutdown systems, physical damage is possible. Typical cybersecurity causes are ■ viruses and ■ unauthorized access.	In 2014, hackers gained access to a steel mill in Germany and disrupted the operation of the safety system, causing massive damage to the blast furnace. This is just one of many possible examples that illustrates how IT and OT risks (*e.g.*, consequences at the process level) are different and how those risks need to be treated differently.
What is the "environmental damage" risk?	Many OT control systems monitor or control processes that, in the event of failure or incorrect operation, can cause harm to the environment. Examples include oil and gas production and wastewater treatment. Typical cybersecurity causes are ■ viruses and ■ unauthorized access.	In 2000, a disgruntled former contractor used stolen equipment to manipulate a wastewater control system deliberately, causing a release of 2,800 m^3 (750,000 gal) of untreated wastewater into the environment in Queensland, Australia.
What is the "injury or death" risk?	Many OT control systems monitor or control processes that, in the event of failure or incorrect operation, can cause harm to personnel or members of the public. Examples include oil and gas production, transportation, and wastewater treatment. Typical cybersecurity causes are ■ viruses and ■ unauthorized access.	In 2008, a 14-year-old modified a televison remote control to change the points on a train network in Lodz, Poland. Twelve people were injured, and four trains were derailed.
What is the goal of cybersecurity?	The overall goal of cybersecurity is to reduce cybersecurity risk to a level acceptable to the organization. Cybersecurity is risk management.	Risk cannot be completely eliminated; it only can be reduced. There are also practical constraints that affect how much a utility can do (and how quickly) such as budget, resources, expertise, etc. Often, cybersecurity controls — called countermeasures — need to be prioritized with a phased implementation that involves risk-management methods.

Knowledge	Principles	Practical Considerations
Are there federal or state regulations regarding cybersecurity?	At the U.S. federal level, the America's Water Infrastructure Act of 2018 requires water utilities meeting certain size requirements to evaluate the cybersecurity of IT and OT systems as part of a risk and resilience assessment every 5 years. The Cyber Incident Reporting for Critical Infrastructure Act contains specific incident reporting requirements for IT and OT for all sectors. Most recently, the U.S. Environmental Protection Agency (EPA) amended the public water system sanitary survey requirements to include cybersecurity with implementation details to be determined by each state individually. At the state levels, New Jersey, Florida, Tennessee, Maryland, and North Carolina have varying requirements for IT and/or OT cybersecurity. A variety of states have made or have pending legislation that make paying ransomware illegal.	EPA has been tasked with oversight of cybersecurity in the water and wastewater sector. Subscribing to the cybersecurity alert service offered by EPA can help with awareness regarding federal regulations that affect a specific utility. Contact the state's environmental regulatory office to inquire about state regulations that affect your utility. To avoid rework, be sure to understand all pertinent cybersecurity requirements upfront. If paying ransomware is illegal in the state, ensure the facility is taking enough extra measures to reasonably prevent it from occurring in the first place. Ask the question: "Are you prepared to respond without paying the ransom?"
How should cybersecurity be managed?	Training and awareness are key to improving cybersecurity posture. Operators should learn about IT and OT system concepts, standards, technology, operations, safety and physical security, risk management, and emergency response preparedness. Physical, cybersecurity, and operational risk assessments should be conducted that evaluate that controls are in place to reduce the likelihood and consequence of a cybersecurity incident. These assessments should include clear, detailed recommendations to close all identified gaps.	There are many examples of cyber events in water systems where basic disciplines such as password integrity, unsecured remote access, phishing victims on company computers, etc., are responsible for providing a means for intrusion. With better awareness and knowledge, water systems can prepare their people, update their processes, and manage their technology.
Who should manage IT cybersecurity?	One size does not fit all, but typically, IT staff should manage IT cybersecurity. However, if OT depends upon IT, then IT becomes a component of managing OT cybersecurity. OT needs to be aware of relevant risks, remediation (reduction), and accept whatever risk remains; or seek a better solution.	When sufficiently separated, OT systems can operate without a dependency on IT. In such cases, there may not be a compelling need for OT to participate actively in IT cybersecurity decisions.
Who should manage OT cybersecurity?	Again, one size does not fit all. However, a general approach that can work well for most utilities is an OT Cybersecurity Committee comprised of a cross-functional representation of IT and OT subject matter experts.	Our technical problems have increased in complexity to a point where there is not any one person or group that knows everything there is to know. Therefore, collaboration is key to being effective at reducing OT cybersecurity risk to a level acceptable to the organization.
What is the best way to leverage the strengths of IT and OT resources?	An OT cybersecurity policy is a good way for a utility to communicate expectations to utility staff. A responsible-accountable-consulted-informed (RACI) chart can establish demarcation points where IT and OT staff can hand off responsibility to one another. The whole lifecycle of systems and equipment should be considered — plan, procure, install, configure, maintain, and dispose.	A generic starting point for demarcation consideration and customization includes the following steps. ■ IT manages the lifecycle of IT applications, IT hardware, and operating systems, such as office applications, anti-malware, network intrusion detection, servers, workstations, laptops, Windows, firewalls, routers, switches, large UPSs, etc.

Knowledge	Principles	Practical Considerations
What is the best way to leverage the strengths of IT and OT resources? *(continued)*		■ OT manages the lifecycle of OT applications and OT hardware, such as human-machine interface, integrated development environment, historian databases, programmable logic controller (PLC) programming software, PLCs, operator interface terminals, remote terminal units, meters, radios, cell modems, small UPSs, etc. ■ Changes are reviewed and approved by the OT Cybersecurity Committee functioning as a Change Advisory Board. ■ Changes are tested in a testbed for adverse effects before deployment to a production environment.
Why might OT Cybersecurity Committee members disagree on the technical approach to cybersecurity?	A disagreement sometimes can be the result of two people or parties operating on a different set of rules or priorities. For example, the root cause may be a difference in prioritization of IT cybersecurity objectives (prioritized as confidentiality-integrity-availability) and OT cybersecurity objectives (prioritized as availability-integrity-confidentiality). Similarly, there could be a difference in what IT and OT guidance and standards recommend.	Understanding the point of view of all concerned parties can be the key to achieving consensus regarding the best solution that reduces risk to meet the facility's needs. Employee safety and public welfare should be top priorities for the OT Cybersecurity Committee.
What are some resources that can be used to help manage cybersecurity risks?	Guidance on the recommended controls is provided in numerous guides and standards. Popular standards that generally focus on cybersecurity include ■ National Institute of Standards and Technology (NIST; Gaithersburg, Maryland) SP800-53r5, ■ International Organization for Standardization (ISO; Geneva) 27001, and ■ Center for Internet Security (CIS; East Greenbush, New York) 18. Popular standards that generally focus on OT cybersecurity include ■ International Society of Automation (ISA; Research Triangle Park, North Carolina)/ International Electrotechnical Commission (IEC; Geneva) 62443, ■ NIST SP800-82, and ■ U.S. Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Performance Goals.	Guidance on basic concepts can be found in Water Environment Federation (WEF; Alexandria, Virginia) and ISA publications. Guidance on cybersecurity risk can be found in Section 4.15 of the *Design of Water Resource Recovery Facilities, MOP 8,* published by WEF as well as in the ISA/IEC 62443 series of standards that define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems published by ISA.
Is there a recommended way to use the available guidance and standards?	A good starting point is for utilities to decide which guidance and standard documents will be used to define the target state of cybersecurity. Next, if a prospective standard includes a baseline (low, moderate, high), then decide which will be used and customize the controls selection to your industry and your utility based on your specific constraints. Next, develop cybersecurity policies and assess your current posture against these new policies.	The main objectives of this exercise are to create a target state that is achievable, sustainable, meets regulations, and reduces cyber risk to within your organization's tolerance. It is important for all stakeholders to have a clear vision of the cybersecurity target state. A target state network architecture drawing is a good way to illustrate all IT networks, OT networks, external connections, the internet, how these various "zones" connect, and how traffic will be controlled tightly to comply with your cybersecurity policy.

Steve Mustard, *P.E., CEng, Eur Ing, CAP, GICSP, CMCP, is President of National Automation Inc. (Spring, Texas) and an independent automation consultant and a subject matter expert of the International Society of Automation (ISA).*

Jim Schultz, *P.E., CISSP, CISA, CCNA, GICSP, CIEH, is a Senior Operational Technology Cybersecurity Consultant with Black & Veatch (Overland Park, Kansas).*