The OT Security imperative — What is your strategy?

01 OT in a connected world

As industrial environments are digitally transformed, they become more connected—and more vulnerable.

Industrial systems have been evolving since steam-powered machines spurred the first Industrial Revolution in the 1800s. At every step along the way, industrial device innovations have improved the ability for workers to get their jobs done faster, more efficiently, safer, and at a lower cost.

As automation became more prevalent, so did the need for Operational Technology (OT)—the use of computer hardware and software to monitor and control physical devices. Industrial Control Systems (ICS) became a necessity for OT environments. They monitor and regulate process values like temperature, pressure and flow, and monitor machines to detect and prevent hazardous conditions and breakdowns. Because ICS is an element of the OT environment, we will refer to OT throughout this paper unless there is a specific point that only relates to ICS.

As these environments continue to evolve, OT environments are leveraging more digital information technology (IT) solutions that connect to the network to become even more efficient and productive. Organizations are incorporating more Industrial Internet of Things (IIoT)—smart sensors that enable machines and systems to automatically share and analyze information. One of the visions of digital transformation is to leverage IIoT devices to connect and integrate industrial control systems with enterprise IT systems, business processes, and analytics. This provides a number of key advantages:

- **Better management and visibility**
  Connecting industrial systems to an IT network gives industrial environments a more comprehensive view of individual equipment and entire industrial ecosystems and makes managing and operating those systems easier and more effective.

- **Improved uptime**
  By constantly monitoring the condition and performance of systems and equipment, IIoT sensors allow organizations to implement predictive maintenance schedules that help to eliminate costly repairs and downtime. This improves performance, quality, and productivity, which leads to increased profitability.

The benefits of this convergence of IT and OT are undeniable. However, this merger introduces its own unique risks and challenges; primary among them is ICS security. Greater complexity, expanded risks, and new threats have led to an increased trend of integrating cybersecurity intelligence and analytics across increasingly digitized OT environments.

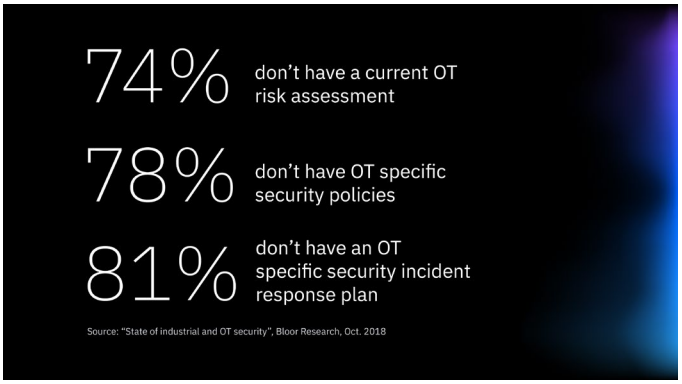
As a result, securing ICS in OT environments is now a top priority.

02 Cybersecurity and the OT/IT convergence

Cybersecurity in industrial OT environments lies at the bottom of the security learning curve.

Decades ago, when corporations first started leveraging client/server networks and the Internet, they didn't initially think about security. Security didn't become a priority until criminals realized they could hack into IT systems to manipulate them and steal money and data. Companies suffered significant impacts as they learned to deal with this new challenge.

OT environments today face similar challenges when connecting ICS technologies to the network. Until recently, operational technology was interconnected with proprietary, vendor-based closed connections and protocols that could not be accessed remotely. Now that ICS technologies are moving toward standard IT communications protocols, IT security challenges have become part of OT environments. But many organizations simply aren't prepared to take on these new security challenges.



Cybersecurity implementation in converged OT/IT environments today is the equivalent of IT cybersecurity twenty years ago. But the impacts of a security breach in an OT environment can be so severe that there is no time for an extended learning process.

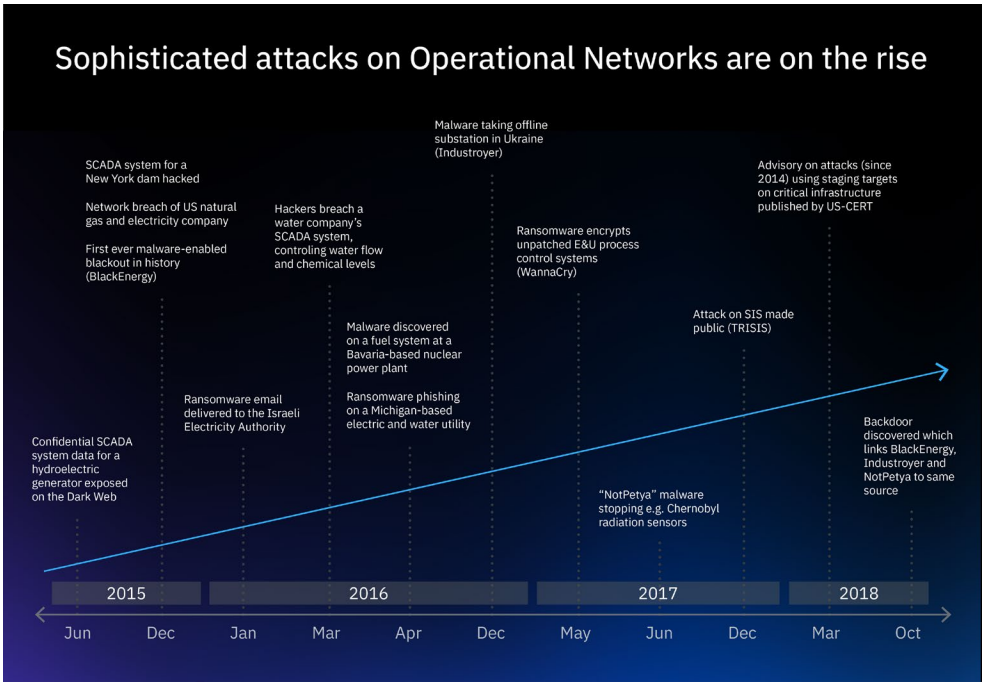
Industrial OT security challenges

OT environments face a number of challenges around security.

- **Risks**
  - **Lack of risk mitigation and remediation**
    Due to a strong focus on operational risks and costs, in operations there's a general lack of understanding of cybersecurity threats; the probability of their occurrence; and their potential impact. And there's often no strategy in place for mitigation.
  - **Hard to test production environments**
    Although penetration (pen) testing is an important tool in IT security, it can pose a significant risk to ICS systems. As a result, pen testing must be used with caution, or replaced with alternative testing methods, in an OT environment.
  - **Limited security awareness**
    Employees in industrial environments like Operators and Engineers don't understand cyber security, and IT security specialists don't know the OT environment. As a result, few risk mitigating techniques and tools exist in OT environments. For example, weak authentication practices are also commonplace.
  - **Limited patching**
    Software updates and patching are critical to security. But, because OT patches often require vendor approval or extensive testing before they're applied, the patching process is slow. Patching also creates downtime.

- **Visibility**
  - **Limited asset visibility**
    OT environments typically have limited or no visibility of potential ICS vulnerabilities, network traffic, and security management functions. In fact, most industrial environments do not have a good accountability of their ICS devices or what processes they support. This alone provides a malicious actor with plenty of opportunities to create problems.
  - **Seeing all devices across OT proprietary protocols is critical**
  - **Sensitive and regulated data is not secure**
    OT environments, like their Corporate IT counterparts, contain sensitive IP and, in many cases regulated data that must be secured. Because data discovery and classification has not been performed this data is vulnerable to a wide variety of impacts if not secured appropriately.Operators and Engineers don't understand cyber security, and IT security specialists don't know the OT environment. As a result, few risk mitigating techniques and tools exist in OT environments. For example, weak authentication practices are also commonplace.
- **Impact**
  - **Security incident impact can be catastrophic**
    When an IT network gets hacked, data gets compromised, stolen, or lost. However, when industrial control systems are hacked, the impacts are even greater—degradation of production quality; downtime leading to decreased productivity and revenue; environmental contamination; and there can be safety issues that can result in injury or death.
  - **Lack of an OT security response plan and playbook**
    Most OT organizations have no response plan for cybersecurity threats and are, therefore, unprepared to respond in the event of a serious incident.

Attacks on OT environments are on the rise



Over the last few years, the publicized impact and sophistication of security breaches in operational networks have increased, which raises the demand for a risk based security approach. Unfortunately, because many companies do not have security controls in place, they are often unaware of security vulnerabilities in their OT environments. There is evidence, that intruders exploiting these vulnerabilities gather information and prepare an attack without being detected for many months or years. In several cases, the exploit became visible when the attack was launched and damage was inflicted. Implementing an OT security program is a fundamental step, companies should perform now.

03 A good OT security program starts with a strategy that includes the establishment of OT security priorities: how prepared are you?

You have to understand the challenges you face before you can properly secure your OT environment.

Start by assessing the state of your OT security awareness and readiness by considering these eight basic questions.

Question 1

Does your company know what ICS devices are installed in the field?

Asset identification is one of the most basic elements of an OT security program. You cannot secure what you don't know you have. Therefore, you must identify and document every device and the processes they support; which systems are interconnected and how; and what security controls you already have in place. You also have to know which systems don't support modern security controls so compensating controls can be installed to mitigate risk.

Question 2

Has your company identified and trained people to manage and sustain OT security?

Technology alone isn't enough to address ongoing OT cybersecurity issues. Additionally, plant engineers and operators responsible for keeping systems running don't have the time or knowledge to address security. Therefore, it is highly recommended that OT security specialists be added to the OT team to establish and maintain the OT security program, in the same way security specialists are part of the corporate IT environment. Because of the lack of skills in this new specialized area, most companies are turning to third parties for support.

Question 3

Does your company have specific OT cybersecurity strategies and policies that address your highest risks?

Plant operations and IT environments are fundamentally different. They require different strategies and policies. It's important to set security priorities. In an OT environment, safety, process integrity and availability are always the highest priorities. Threats that impact these factors present the highest risk, so the security strategy must address them first.

Question 4

Can you trust the output from your devices?

OT process integrity relies on the ability to trust the devices on your network. In order to achieve that trust, your security strategy must include mechanisms that alert you to or prevent unauthorized changes. It is imperative that sensitive, critical, or regulated data be identified, classified, and protected. Protection should include an access control solution that limits access to authorized users only and monitors those users' activities when using the data.

Question 5

Are you using IT security techniques within the OT environment?

Many IT security techniques are counterproductive for OT environments. For example, a password authentication policy that locks a user out after five failed attempts could be disastrous in terms of time (and, potentially safety) in an industrial environment where an engineer has to resolve a problem with a critical system within seconds. Worse, it could serve as an easy way for attackers to lock legitimate users out of the system. OT security controls must be architected specifically for OT environments.

Question 6

Does your OT Security team understand your OT environment?

It's difficult to understand the inherent risks and mitigation measures required to isolate vulnerabilities that impact OT systems without complete system documentation and understanding. This is why it is imperative to have OT security professionals supporting the OT environment rather than relying on an IT security professional.

Question 7

Do you fully understand your company's OT Security Risks?

The advantages of industrial environment digital transformation certainly outweigh the risks—but only if those risks are fully understood and proactively managed. This evolution will increasingly take advantage of more IIoT and cloud computing solutions that will continue to impact the risk posture of the OT environment. Don't let a poor security program be the reason that your company can't accelerate its ability to grow and compete.

Question 8

Are you prepared to respond to a cyberattack in the OT environment?

Cyberattacks can be disastrous for an OT environment. This requires a well-rehearsed plan in place to quickly respond to and mitigate the damage in the event of a successful attack. At a minimum, this response plan must include:

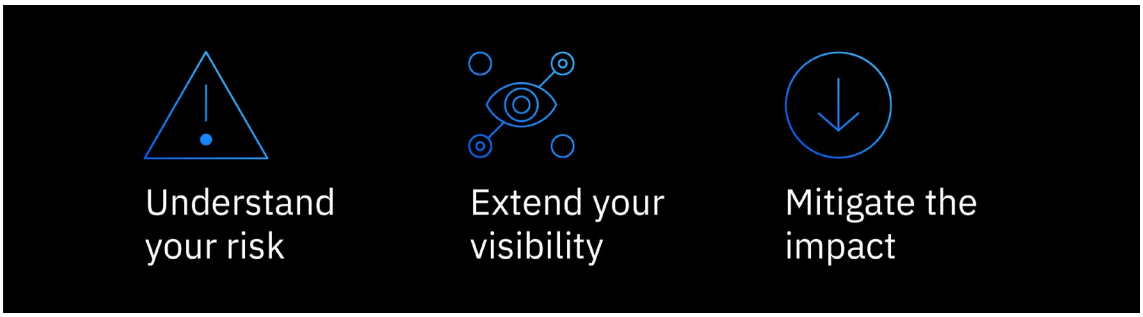
- Clearly-documented and understood roles, responsibilities and playbooks.
- The ability to pinpoint the industrial processes being attacked and the devices involved.
- Log files that can be forensically examined.
- User profiles and log files of users that have access to OT devices.
- Documentation of the data that could have been impacted
- Disaster recovery plans and redundancies to restore critical assets and data.

04 Creating a sound OT security strategy

Solid OT security isn't just about technology. It's a Program.

Technology is only one piece of the OT security solution. A comprehensive security strategy also includes defined roles and responsibilities for the people involved, clear security processes, and supported policies in addition to enabling technologies.

Your OT security strategy starts by focusing on the fundamentals.



Understand your risks

What are your risks, gaps, and vulnerabilities and what is your overall strategy to mitigate them? For those companies just starting their OT security journey, we provide offerings around understanding risk.

IBM can help organizations understand what's required in order to identify risks. Achieving the proper level of risk understanding requires a phased approach:

- **Develop OT security strategy and plan**
  Our process helps identify your risks and assess your risk tolerance. We identify what projects and processes need to be implemented to achieve the maturity level you desire, and we set out with a plan aligned to a calendar that can be executed.
  - OT Security Strategy and Planning Services
- **Conduct OT security risk and compliance assessment**
  We conduct a risk and compliance assessment to determine your level of compliance with regulations and frameworks that apply to your industry.
  - OT Security Risk and Compliance Services
- **Conduct OT vulnerability assessment**
  We have a unique approach around vulnerability assessment. This precise process identifies vulnerabilities and helps you to develop a mitigation plan to protect your environment.
  - IBM X- FORCE Red ICS Testing
- **Establish OT governance and RACI (Responsible, Accountable, Consulted, Informed) requirements**
  We help you develop policies, procedures, roles, and responsibilities to enhance governance.
  - OT Security Policy, Procedure, and RACI Design Services

If your organization does not have the capabilities and skills to perform these initial assessment and planning stages in-house , or you perform these already but need an independent 3rd party report, IBM's OT security experts and solutions can help you through every phase of the risk discovery process.

Extend your visibility

A critical component in a good security program is having visibility into your entire OT operation. You need to know exactly what your OT devices are and have a good accountability of them. You have to look at your network design and infrastructure with an eye toward security. Identify critical data that must be classified for security treatment. And look at the people who are using your systems and develop secure access control policies.

Through IBM and our extensive ecosystem of third-party partners, we can provide assistance and guidance:

- **Conduct OT and ICS device discovery**
  We identify exactly what your assets are, with an eye toward possibly importing them into an asset management solution.
  - OT Security Asset Management Services

- **Conduct network discovery and security architecture review**
  Now that your devices are interconnected through your network, the network architecture must be designed to manage risk. We assess both the network architecture and all of your endpoints and design a strategy around them.
  - OT Infrastructure and Endpoint Security Services
- **Conduct data discovery, classification, and analysis**
  Data is important in OT, just as it is in an IT environment, and a lot of that data is sensitive. Using our services and technology, we perform a complete data discovery analysis.
  - OT Data Security Services
  - IBM Guardium
- **Perform OT/ICS user access review**
  User access management is critical in OT environments. There are lots of third-party contractors in OT—often, more than there are employees. We help you track who's doing what with your OT and ICS systems by putting good access and privileged access management practices in place.
  - OT Identity and Access Management Solutions

Mitigate your impact

Once your risks have been identified and you have good visibility into your OT environment, it's time to implement security solutions. We work with you to design, develop, and implement a comprehensive security solution, and help you manage that solution if you don't have the expertise to do it yourself.

IBM is there every step of the way as you get your OT security strategy up and running, and to provide all of the assistance and guidance you need to ensure that your organization remains secure.

- **Secure data and endpoints**
  Now that you know where your data is and what's sensitive and proprietary, our services, experts, and technologies help you to manage your data risk.
  - OT Data Security Services
  - IBM Guardium
  - IBM MaaS360
- **Plan and implement OT Identity and Access Management (IAM) solutions**
  Our specialists, solutions, and third-party partners help to ensure that you always know who has access to your systems; when they had access; and what activity and changes took place during that access.
  - Identity and Access Management Solutions
- **Design, build, and optimize an OT security operations center (SOC)**
  The OT SOC is very different from a corporate IT SOC in terms of use cases, policies, and incident response. We help you design and optimize your SOC for the special needs of the OT environment.
  - Security Intelligence and Operations Consulting
- **Manage OT network and SOC security services**
  We have the capability to manage your network and firewalls and make sure they're constantly aligned with your OT environment. We also support your OT Security through our global Managed Security Services that are tuned to the OT environment.
  - Managed Security Services
- **Develop OT security incident response**
  OT incident response is different from IT, and a lot more complex. You're working with OT engineers and operators, vendors, and contractors—often in a union environment. We help you to develop an incident response plan and different playbooks for these unique conditions, as well as providing access to forensic services and back-up and recovery solutions and services should an attack occur.
  - IBM X-Force IRIS
  - IBM Resilient
  - IBM Resiliency Services

05 IBM Security solutions bridge the IT/OT gap

IBM's OT security services approach helps clients at different maturity level to improve their OT Security posture and accelerate time to value from their OT security investment.

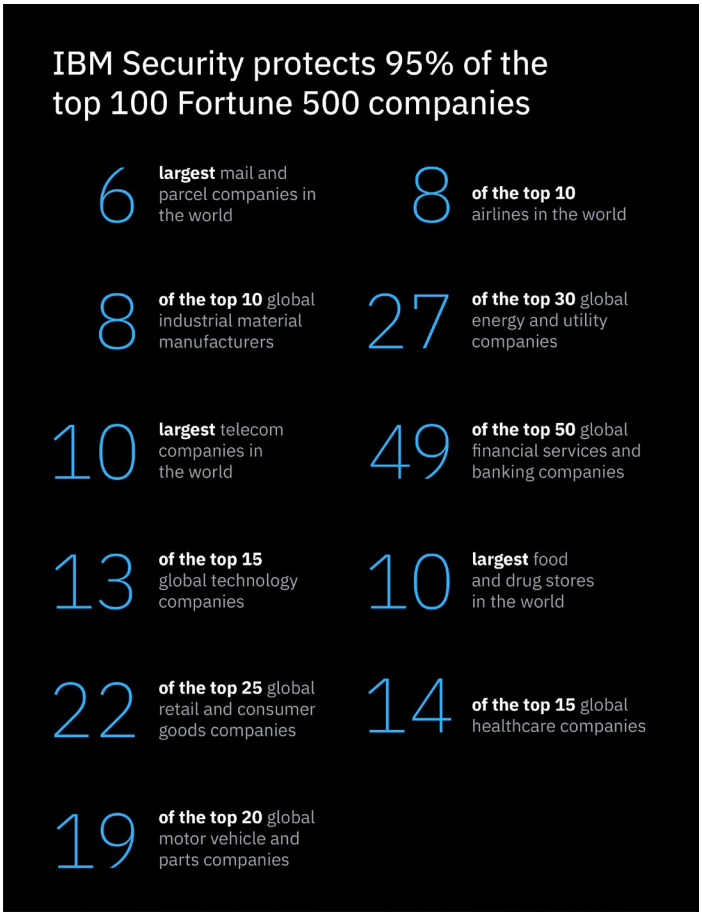
IT security solutions aren't designed to address OT security challenges. And OT solutions that rely on technology alone aren't effective. They need to be part of a well-designed OT security strategy.

IBM is recognized as a worldwide leader in IT security and has years of experience in helping organizations to understand security risks, extend visibility, and prevent significant impacts as their IT environments. Companies worldwide have trusted IBM to help them on their OT security journey. We can bring that same experience to your organization.

Why IBM?

- **Expertise**
  Get the guidance you need to design, implement, train, and manage based on OT best practices. IBM is a leader in the security industry with expanding OT industry knowledge. We bring the best of both worlds to your unique environment.
- **Technology**
  Leverage best-in-class technologies to gain a single view across your entire OT infrastructure. Our market-leading security products for OT and have all necessary integrations in place.
- **Partner ecosystem**
  Engage with an open partner ecosystem to manage OT risks.

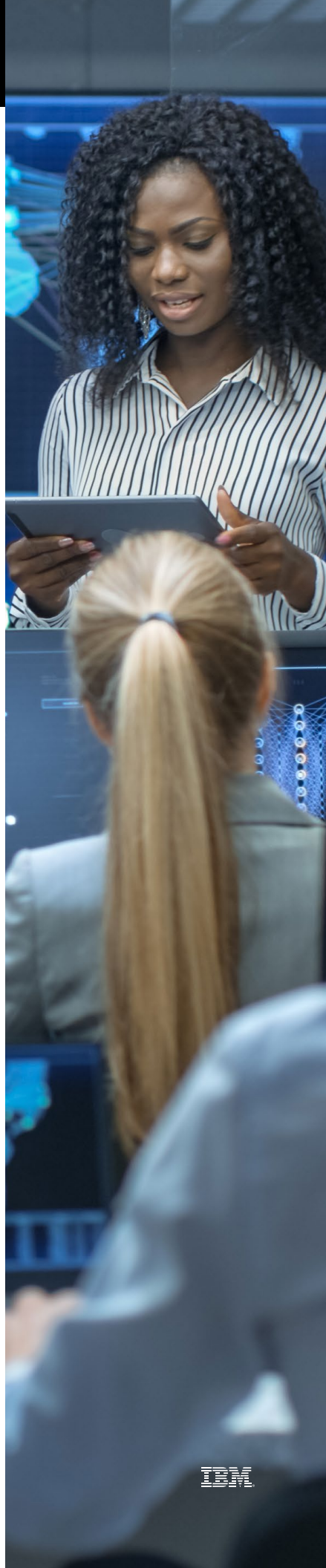
From assessment, to implementation, to monitoring and support, IBM's comprehensive approach to OT security keeps your assets, data, and people safe and secure. We have leveraged our knowledge and experience in cybersecurity to expand our capabilities into the OT environments by hiring and training OT security professionals around the world. And, to further enhance our capabilities, we have established business partnerships with some of the leading OT security solution providers in the industry.



06 Learn more

Find our how IBM can help you develop a complete strategy to conquer the challenges of securing your newly digitized OT environment.

Explore →



© Copyright IBM Corporation 2019. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp. NOTE: IBM web pages might contain other proprietary notices and copyright information that should be observed.

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.