MAYER | BROWN

DRAGOS

Responding to Cyber Incidents Affecting Operational Technology

Jason Christopher
Principal Cyber Risk Advisor, Dragos
(470) 222-5478
jdchristopher@dragos.com

Stephen Lilley
Partner, Mayer Brown LLP
(202) 263-3865
slilley@mayerbrown.com

Veronica Glick
Senior Associate, Mayer Brown LLP
(202) 263-3389
vglick@mayerbrown.com

May 20, 2020

Today's Speakers

Jason Christopher. serves as Dragos' Principal Cyber Risk Advisor and blends innovative approaches for risk management with state-of-the-art products across the company's product catalogue. Prior to Dragos, Jason was the CTO for Axio, where he developed their multimillion dollar critical infrastructure business strategy & created cyber risk products for executives, engineers, and security specialists. Before joining Axio, Mr. Christopher led the research for cybersecurity metrics at the Electric Power Research Institute. He was previously the technical lead for Cybersecurity for Energy Delivery Systems (CEDS) Operations program at the US Department of Energy, where he managed the nation's risk management & incident response capabilities. He also served as the energy sector lead for the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

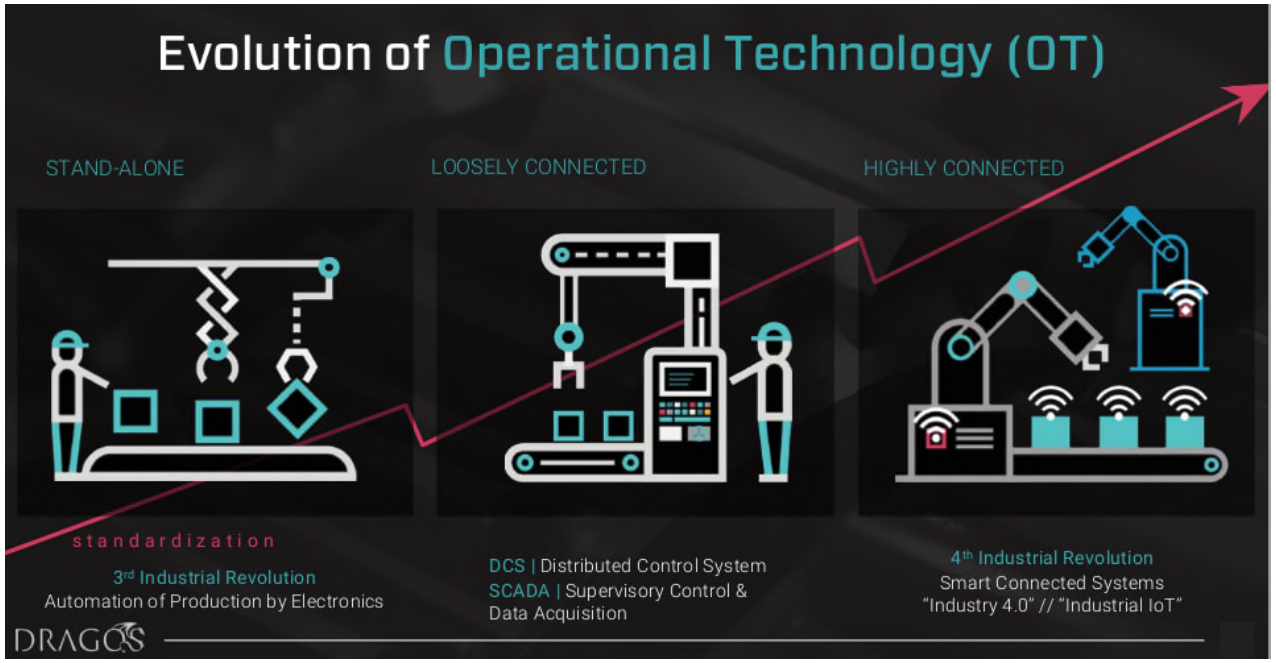
Stephen Lilley is a partner in Mayer Brown's Washington DC office, and a member of the Cybersecurity and Data Privacy and Litigation practices. He advises clients on a broad range of cybersecurity issues, including managing litigation and regulatory risk, internal governance, incident response, and addressing risks posed by the Internet of Things and Operational Technology. Before joining Mayer Brown, Stephen worked for the US Senate Judiciary Committee as Chief Counsel to the Subcommittee on Crime and Terrorism, where he had a particular focus on cybersecurity.

Veronica Glick is a senior associate in Mayer Brown's Washington DC office, and a member of the firm's Cybersecurity and Data Privacy practice. She counsels clients on a variety of complex legal issues regarding incident response, investigations, and regulatory compliance. Veronica serves on a pro bono basis as Deputy Chief Counsel for Cybersecurity and National Security to the US Cyberspace Solarium Commission and as a member of the United Nations experts committee regarding the prevention of terrorist exploitation of the Internet.

Operational Technology Supports Our Way of Life

- **Operational Technology** (OT) consists of "hardware and software that **detects or causes a change** through the direct monitoring and/or control of **physical devices, processes and events in the enterprise**." (NIST IR 8183)
- OT is often found in industries that manage **critical infrastructure**, such as **energy, agriculture, water systems, transportation systems**, **chemicals, telecommunications,** but also in **automated manufacturing, pharmaceutical processing**, and other industries.

OT Connectivity Presents Significant Opportunities for Businesses



- Over time the number of inter-connected computers and devices have grown in the OT environment
- Leveraging data produced by these and other machines can allow companies to run their OT environments more effectively and efficiently.

OT Presents Distinct Issues From Traditional IT

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (Reliability) Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	Manage data Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Control physical world Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3 to 5 years	Lifetime on the order of 10 to 15 years
Components Location	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

- NIST has described important differences between OT and IT.
- These include:
  - Increased safety risk from incidents;
  - Increased use of proprietary protocols, out of support products, and other factors that increase complexity;
  - Heightened availability requirements;
  - Potential physical inaccessibility of affected devices;
  - Memory or other constraints may limit ability to update affected devices;
  - Standard tools for securing information technology, including intrusion detection systems and tools for providing system availability, may not be in place.

24 x 7 operations
10-30 year lifecycle
16 critical infrastructure sectors

NIST Special Publication 800-82, Guide to Industrial Control Systems Security.

Agenda

- Cyber Threats to OT
- Legal Risks Presented by Cyber Incidents Affecting OT
- Responding Effectively to Cyber Incidents Affecting OT
- Preparing to Respond Effectively


Cyber Threats to OT
MAYER | BROWN
DRAGOS

Cyber Threats To OT Continue to Grow

Nation state actors have the ability "to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours."

Hon. Daniel Coats,
Director of National Intelligence
Statement before Senate Intelligence Committee
2019

Dragos' 2019 Threat Assessment:

- Three new activity groups targeting ICS entities globally, bringing total to 11;
- Increased threat focused on ICS organizations, particularly in critical infrastructure across U.S. and APAC;
- Ransomware and commodity malware threaten industrial operations and can potentially bridge the IT/OT gap;
- Adversaries increasingly targeting remote connectivity.

Cyber Attacks Present Significant Risks to Companies That Rely Upon Operational Technology

High-Stakes Attacks:

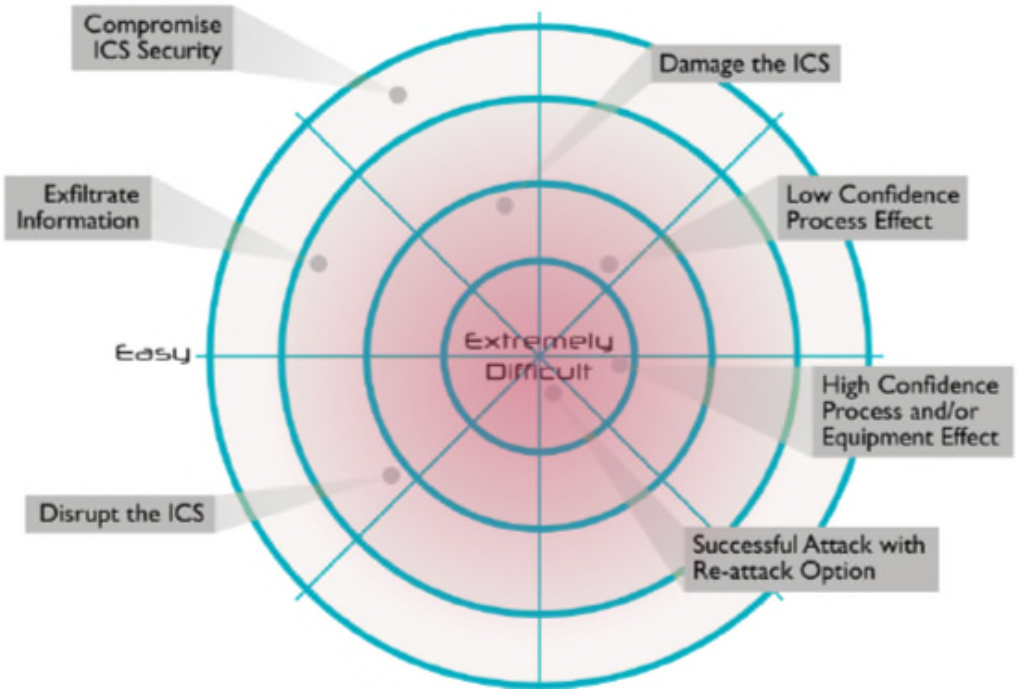
A 2017 attack compromised a petrochemical facility's safety instrumented systems. It reportedly was discovered because of a flaw in the malicious code.

- **Most *likely* incidents include:**
  - Data theft / espionage, including attackers seeking to understand key systems and develop foothold for future attacks
  - Collection of trade secrets or economically valuable information
  - Extortion or ransom
- **Most *damaging* incidents include:**
  - Deny, degrade or destroy operations
  - Cause process disruption or physical destruction

The Most Complex Attacks on OT Require Significant Technical Knowledge

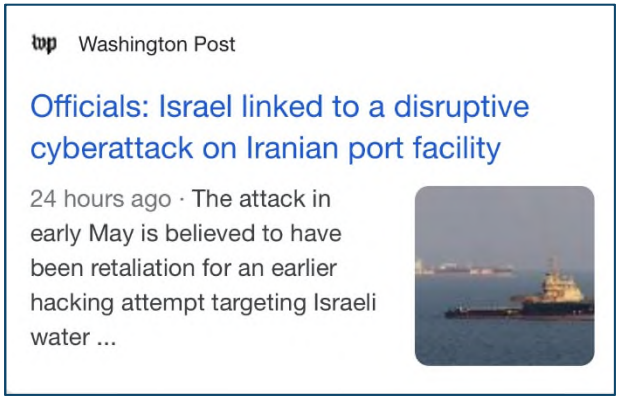
The knowledge involved in ICS attacks, with physical impact, includes:

- IT security
- OT security
- OT-specific protocols
- Engineering processes
- Incident response
- Disaster recovery



A Wide Range of Sectors Have Been Affected by OT Cyber Attacks

- March 2019 – A metals and mining company reportedly suffered **~$70-80M** in losses due to a ransomware attack that forced the company to switch to manual operations and reduced overall output by 50%.
- March 2019 – NERC reportedly issued a warning that a hacking group was conducting reconnaissance into the networks of **electrical utilities**.



- Aug. 2019 – A hacking group responsible for attacks against three U.S. **utility companies** in July 2019 was subsequently reported to have targeted seventeen U.S. utilities companies.
- March 2018 – US-CERT issued an alert alleging that the Russian government had targeted "U.S. Government entities as well as organizations in the **energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors**" with sophisticated cyber attacks.

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION SIGN IN SUBSCRIBE

MIKE MCQUADE

ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

Most Popular

FedEx

MAERSK

MERCK

Mondelēz International

SAINT-GOBAIN

Reckitt Benckiser

One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs

Fedex says its expenses tied to malware attack was $400 million over past year, Merck put costs at $670 million in 2017

By Kim S. Nash, Sara Castellanos and Adam Janofsky

Updated June 27, 2018 12:03 pm ET

NotPetya... Not Ransomware

"Wiper disguised as ransomware," with increased collateral damage beyond any initial targets.

+$10B in estimated damages

2M computers impacted in 2HRs

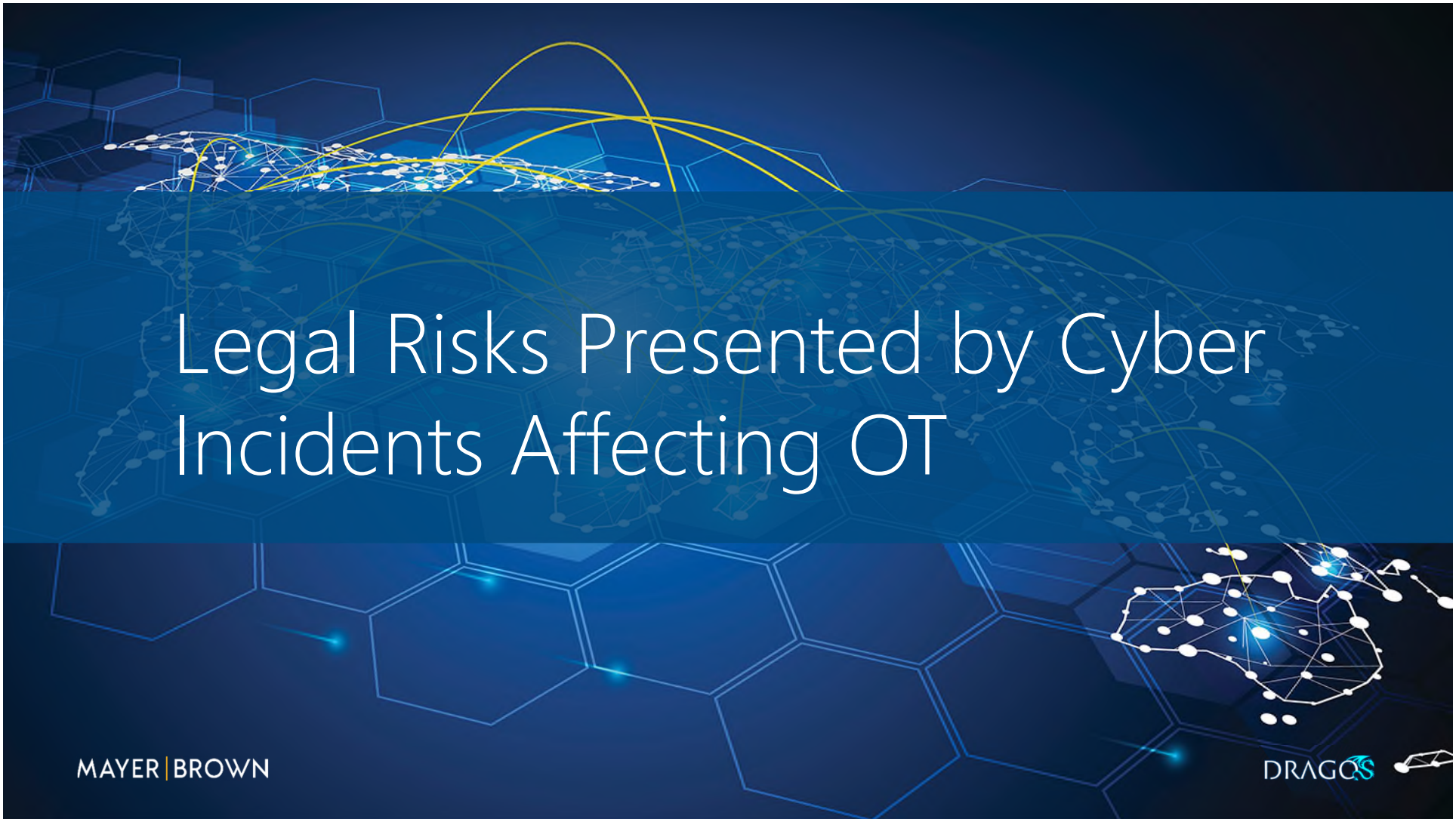
+65 countries involved in response

Opportunities to Strengthen OT Security Remain

Dragos 2019 Year in Review:

- **71%** of organizations assessed had **poor security perimeters**, allowing the Dragos Red Team to traverse and gain access into the ICS networks
- **76%** of organizations could **not detect Dragos' Red Team** activities
- **66%** of incident response cases involved adversaries **directly accessing the ICS network from the internet**

A 2019 CISA alert describes a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility. The entity's emergency response plan did not address cyber incident response specifically.


Legal Risks Presented by Cyber Incidents Affecting OT
MAYER | BROWN
DRAGOS

Litigation Risks After OT Cyber Incidents Are Significant

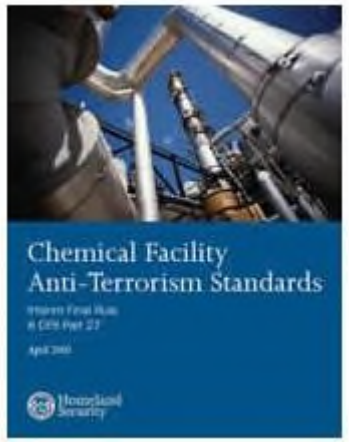
- **Civil Lawsuits**: litigation with business partners, contractual counterparties, mass tort actions.
- **Derivative actions**: for publicly-traded companies, actions brought by shareholders against officers and directors alleging failure to oversee an effective cybersecurity program.
- **Securities class actions**: brought by shareholders alleging that public disclosures after an incident were misleading or prevented them from protecting themselves from further injury.

Companies Also Face Regulatory Risk, For Example in the Bulk Power System . . .

- The Federal Energy Regulatory Commission (FERC) certified the North American Electric Reliability Corporation (NERC) to set out security reliability standards – Critical Infrastructure Protection ("CIP").
  - **NERC has exacted high penalties –** up to $500,000 in 2017, $2.7M in 2018, $10M in 2019, and $450,000 in 2020 to date – after a trend of declining violations in the prior 5-year period.
    - For the **$10M fine** assessed in 2019, NERC concluded that "many of the [CIP] violations involved long durations, multiple instances of noncompliance, and **repeated failures to implement physical and cyber security protections**."
  - June 2019 – FERC approved CIP-008-6, which includes **incident reporting** and response planning requirements.
- May 1, 2020, **Executive Order 13920** signaled continued scrutiny prohibits certain transactions that pose risks to the electric energy transmission supply chain.

. . . As Well As The Chemicals Industry

- The Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Facility Anti-Terrorism Standards (**CFATS**) program regulates high-risk facilities to ensure cyber and physical security measures are in place.
  - The CFATS regulatory program applies to approximately 3,300 facilities.
  - **Violations are subject to a civil penalty**, up to $10,000 per day for major deficiencies.
- Last week, the Government Accountability Office issued a report stating that **action is needed to enhance DHS's oversight of cybersecurity at high-risk chemical facilities**.
  - The report found that the guidance has not been updated in more than 10 years.

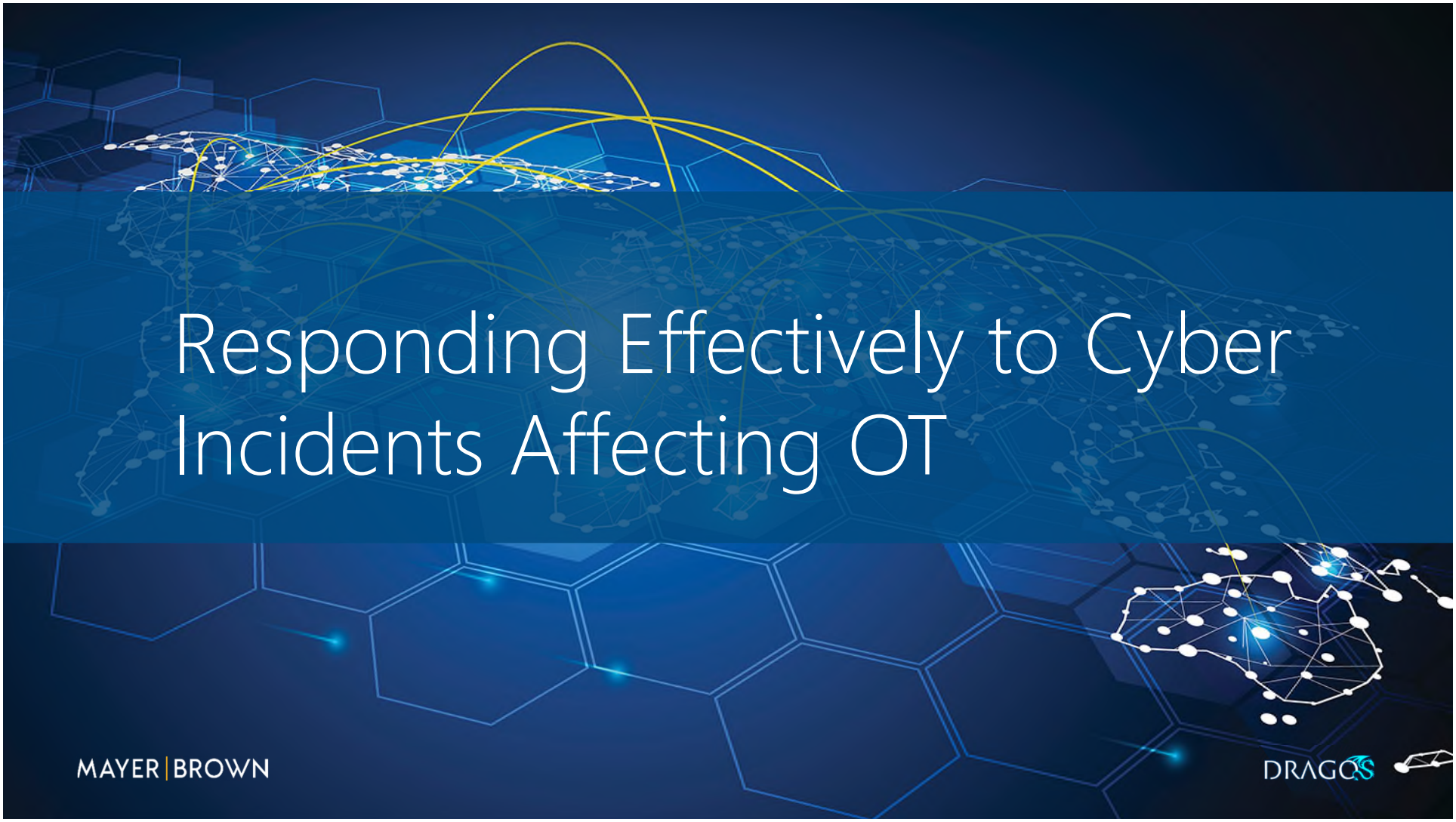


Water Systems Will Soon Need to Certify Completion of an Assessment and ERP

- **America's Water Infrastructure Act** of 2018 requires each community water system serving a population of greater than 3,300 persons to conduct a **risk and resilience assessment** and:
  - prepare or revise, where necessary, an **emergency response plan** (ERP) that incorporates the findings of its assessment – the plan must include physical security and cybersecurity; and
  - certify to the EPA Administrator that the assessment and ERP have been completed. For entities serving populations over 100,000, the ERP certification must be complete by **Sept. 30, 2020**.
- The EPA can initiate an enforcement action and assess a penalty of up to **$25,000 per day for non-compliance**.

Incidents Also May Put Pressure on Vendors' Vulnerability Management Programs

- While operators of Operational Technology are likely to have the primary responsibility for responding to incidents, they are also likely to look to the suppliers of affected equipment, particularly if an incident exploited a vulnerability in an OT system.
- An incident may raise questions, for example, as to whether and when a vendor knew about an exploited vulnerability, and provided and adequately disclosed a timely patch—and conversely, whether an operator timely installed a patch.
- OT vulnerability management is likely to remain a priority issue in the coming years. For example, the **proposed Cybersecurity Vulnerability Identification and Notification Act** would give CISA subpoena power to identify operators of unpatched critical infrastructure.


Responding Effectively to Cyber Incidents Affecting OT
MAYER | BROWN
DRAGOS

Companies Can Mitigate Legal Risks by Responding Effectively to Incidents

- The diverse **range of cyber incidents** that companies face can require them to navigate an equally **broad range of risks** and considerations during the response to an incident.
- Generally, however, key elements of an effective response to cyber incidents include:
  - Understanding of **roles and responsibilities** in a response;
  - Timely **coordination** among stakeholders within an organization;
  - **Sound judgments** by appropriate stakeholders, including through **escalation** within company;
  - Use of **third-party resources** (e.g. OT expert forensics firm, outside counsel, communications consultant);
  - **Coordinated approach** to the diverse technical, legal, business, and practical challenges presented by an OT incident.

A Diverse Group of Stakeholders Contributes to Effective OT Incident Response

Legal counsel has a critical role to play in helping the business respond throughout the phases of incident response, from detection to lessons learned.

External forensic teams, frequently engaged through legal counsel, can be valuable for several reasons, including: (i) bringing to bear **particularized OT expertise** and experience with unique incidents; and (ii) providing a level of **third-party validation**.

MAYER | BROWN

DRAGOS

Priority Issue for Counsel: Assessing Key Legal Obligations

- Consider **notification requirements** for regulators, other government agencies, and contractual counterparties.
  - Certain incidents may trigger regulatory notification requirements e.g., NERC, SEC.
  - Contracts may put in place requirements to share large amounts of information on a compressed time frame.
- Review other applicable **contractual rights and obligations**.
- Tailor the analysis to the **specific compliance considerations** facing the company.
  - Ransom payments may raise sanctions compliance risk.
  - Incidents may raise questions under a broad range of legal regimes.

Priority Issue for Counsel: Gathering Facts, Preserving Evidence, and Maintain Privilege

- Accurate **development of the facts** of a cyber incident is critical to managing legal consequences. Legal counsel plays a central role in ensuring the appropriate development and documentation of key facts.
- Consider the possible competing prerogatives of **evidence preservation** and protecting business interests to restore operations quickly.
- The **attorney-client privilege** and **work product doctrine** can protect documents that inform legal advice from being produced in litigation or government investigations.
  - Establish clear and reasonable expectations within the incident response team.

Priority Issue for Counsel: Managing Internal Communications

- Regulators expect senior management and the board of directors to provide **appropriate leadership and oversight** of a cyber risk management program.
- Keeping senior management in the loop improves **prompt and effective decision-making** when key issues arise (e.g., proposed response to ransom demands).
- Ensuring that the Board of Directors are informed of an incident, to the extent appropriate, will help **mitigate litigation and regulatory risk.**
  - Understanding the Board of Directors' expectations and maintaining an appropriate level of detail can make these updates more effective.
- **Communications to employees** may be necessary or appropriate, and it can be helpful to include HR in such communication strategies.

Priority Issue for Counsel: Communicating with Third Parties / Media

- Communications with third parties – including regulators, the public, and the media can raise significant legal risks. Best practices include:
  - Communicate a **consistent and accurate message** regarding the business' response to the incident that satisfies legal obligations and client expectations.
  - Review messages prepared for the press for **consistency** with all other external communications.
  - Consider whether a public relations/crisis management firm should be engaged through counsel.
- Engagement with **law enforcement** also raises significant risks.
- Engagement with **insurers** can add complexity to third-party communications.

Priority Issue for Counsel: Information Sharing

- Information sharing can occur through **industry groups** and **government agencies**:
  - CISA manages **public-private cybersecurity engagement and information sharing**. CISA hosts the Industrial Control Systems Joint Working Group.
  - The Electricity Information Sharing and Analysis Center (**E-ISAC**) is situated within NERC.
- **Legal protections for shared information** will prevent that information from being used as the basis, in certain cases, for regulatory actions or civil litigation, and from being subject to FOIA and equivalent state-level statutes:
  - The Protected Critical Infrastructure Information Program, established in 2006
  - Cybersecurity Information Sharing Act of 2015


Preparing to Respond Effectively
MAYER | BROWN
DRAGOS

Availability of Appropriate Resources Can Enable a Prompt and Effective Response

A key part of preparation for OT incidents is ensuring that the response team has the logistical and external support to operate effectively in the wake of an incident.

Consider:

- Engaging key stakeholders in advance, in particular those that are involved early in an incident – outside counsel and cybersecurity firm(s) under privilege;
- Confirming preferred/backup methods of secure communications;
- Ensuring key policies and procedures (including the incident response plan and appropriate playbooks) are up to date and accessible; and
- Maintaining appropriate logging capabilities.

Training and Practice Improve Incident Response

- Training and practice ensure that the effort and resources expended to prepare for a cyber incidents are deployed efficiently and effectively when it counts.
- Regular tabletop exercises and incident "coaching" – often under privilege – allow a business to:
  - Build preparedness through practice;
  - Identify potential pitfalls and process gaps;
  - Meet regulatory expectations;
  - Build awareness within the company of roles and responsibilities;
  - Build relationships among key stakeholders;
  - Make sure the plan is up to date, and allow for capturing of lessons learned.

Questions?

MAYER | BROWN

DRAGOS

Americas | Asia | Europe | Middle East

mayerbrown.com