MAYER | BROWN

DRAGOS

Managing OT Cyber Risk: Lessons from the Front lines

Stephen Lilley

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

Veronica Glick

Partner, Mayer Brown LLP
(202) 263-3389
vglick@mayerbrown.com

Ben Miller

Vice President of Dragos Professional Services and R&D , Dragos
(443) 797-4449
bmiller@dragos.com

Kai Thomsen

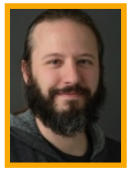
Director of Dragos Global Incident Response Services
kthomsen@dragos.com

January, 2021

Today's Speakers

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 partner 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.



Ben Miller serves as Dragos's Vice President of Dragos Professional Services and R&D. Ben leads a team of analysts in performing active defense inside of ICS/SCADA networks. In this capacity he is responsible for a range of services including threat hunting, incident response, penetration testing and assessments for industrial community as well as advanced research and innovation within ICS security.

Kai Thomsen serves as Dragos's Director of Dragos Global Incident Response Services. A certified SANS Instructor for the ICS curriculum he teaches "ICS Active Defense and Incident Response" (ICS515). Kai spent 7 years in the automotive industry and 14 years in the steel industry in various security roles, including Incident Response and Business Continuity.

Agenda

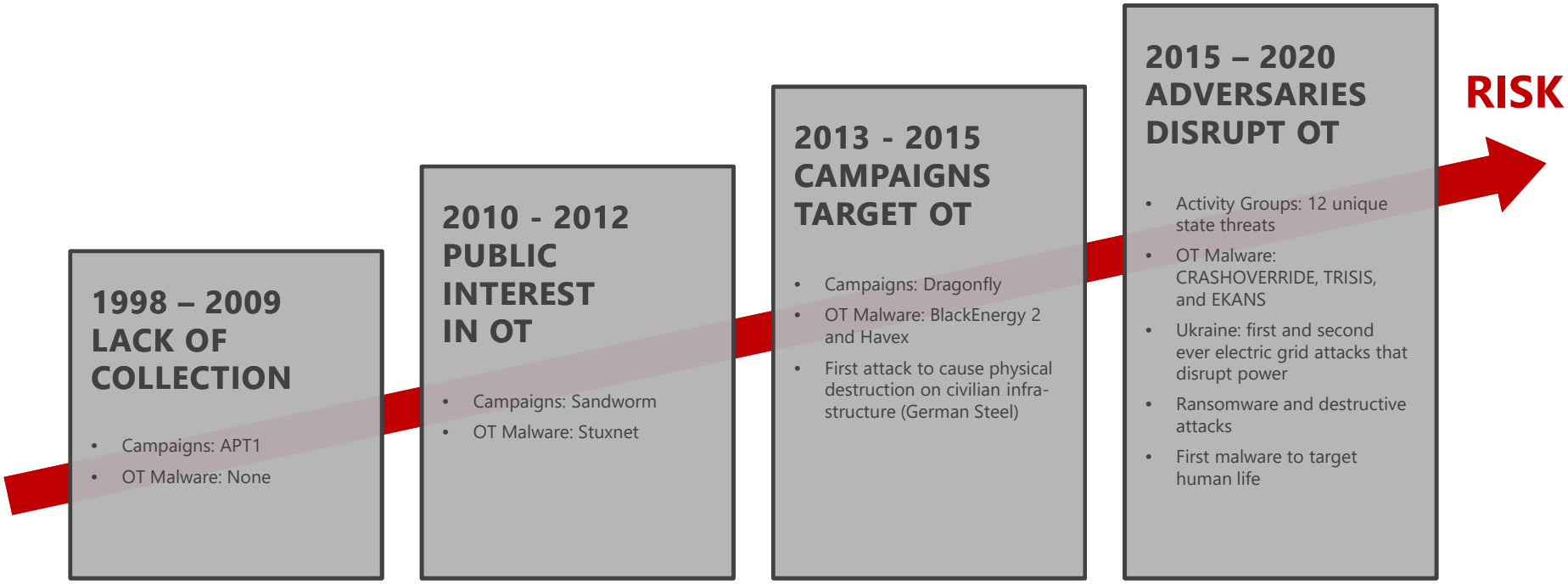
- OT Cyber Risk
- Real World Scenarios
- Lessons Learned


OT Cyber Risk
MAYER | BROWN
DRAGOS

Operational Technology (OT)

- Sometimes referred to as **Industrial Control Systems (ICS)**
- Operates **essential** infrastructure for society
- **Complex, engineered** systems comprising various vendor technologies
- Disruption can cause **significant impact** to human **safety** and / or **revenue**, and associated **legal consequences**
- Examples:
  - Manufacturing assembly line
  - Pharmaceutical production
  - Petroleum refining
  - Chemical production
  - Power generation and distribution

Attacks Growing in Frequency and Sophistication



OT/ICS Cybersecurity Challenges

ASSET VISIBILITY

What's on my network?
How has it changed over time?

- Focus on **safety** and **uptime**
- **Diverse** systems & technology
- Complex change management **processes & patching** challenges

THREAT VISIBILITY

Am I compromised?
What do I do about it?

- **Long** system lifecycles
- Unmonitored networks
- Often **insecure** by design
- Largely **unknown** threat landscape

IT-OT GAP

How do we do this together?
Who can I partner with for OT security expertise?

- **Increasing** threat activity
- Digital transformation **initiatives**

Consequences

A cyberattack against OT systems can risk injury to employees or the public, system shut down, or other physical and business-impacting consequences:

- TRISIS malware put a refinery in an unsafe state resulting in shutdown
- NotPetya led to +$10B in estimated damages
- Supply chain threats are impacting telecommunications, managed service providers, and ISPs in particular
- Ransomware and commodity malware – like Ryuk and Emotet – can bridge the IT/OT gap to disrupt operations
- Escalating geopolitical tensions increase the chance that offensive cyber operations against ICS will be employed more regularly putting critical infrastructure and human life at higher risk

Legal Consequences

Litigation:

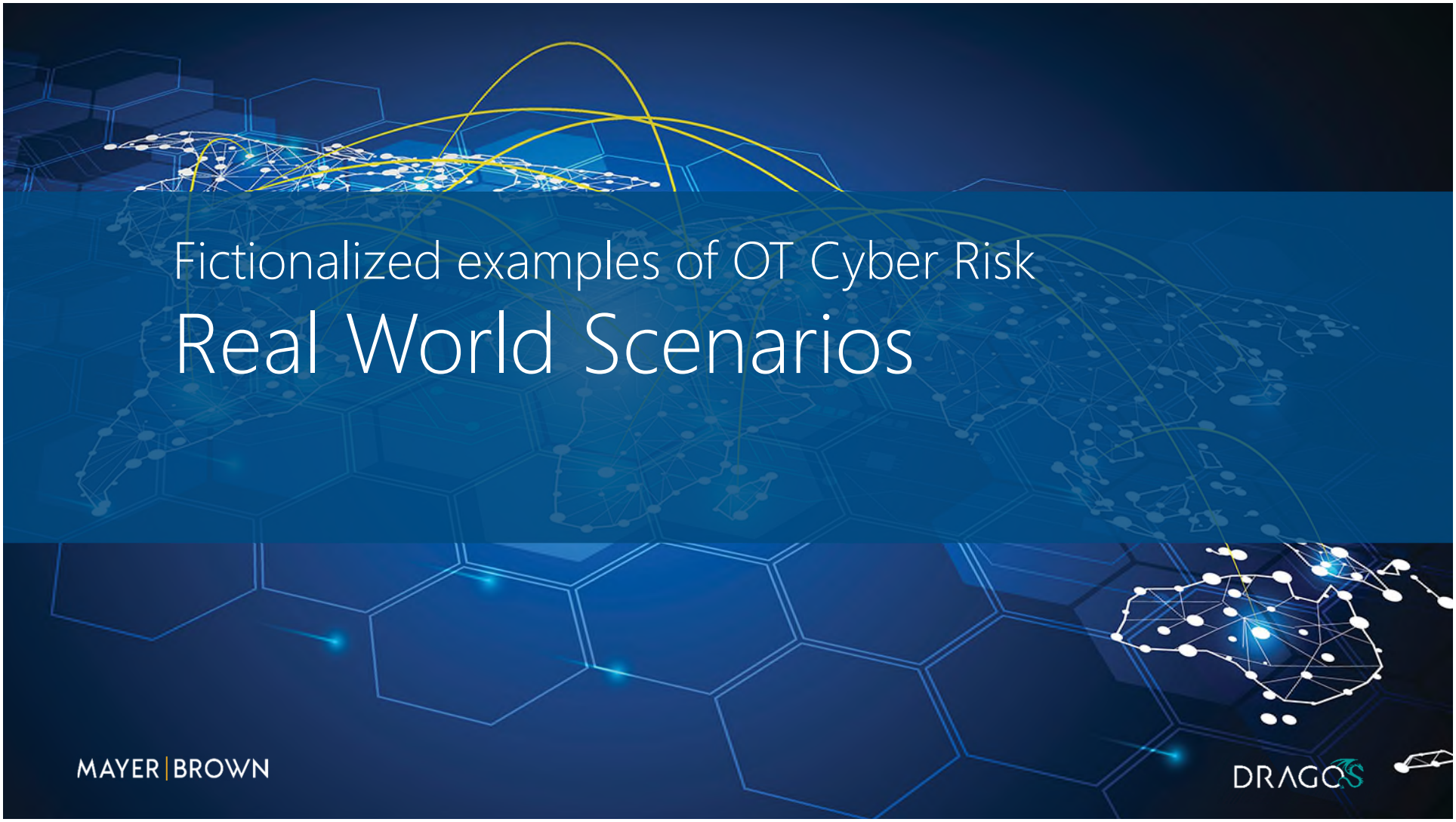
- Mass tort actions.
- Litigation with business partners.
- **Derivative actions** alleging failure to oversee an effective cybersecurity program.
- **Securities class actions** alleging that public disclosures after an incident were misleading.

Regulation:

- Rising expectations across industries and possible increase of regulatory requirements in Biden administration.
- Regulatory enforcement actions after an incident or in the event of disclosure of inadequate security practices.

Legal Risk Multipliers

- Unclear allocation of roles and responsibilities.
- Lack of policies and procedures.
- Lack of internal training/education.
- Failure to address common security errors.
- Unfavorable contractual provisions.

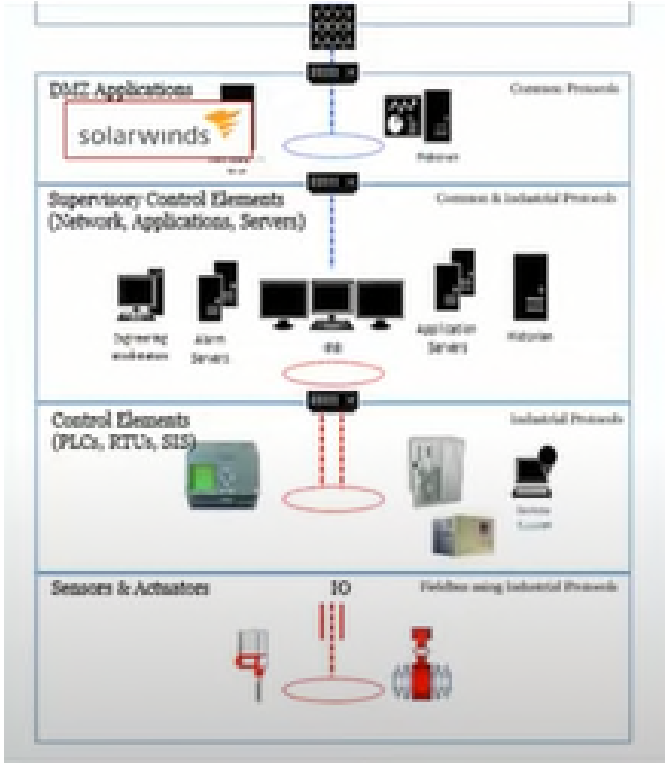

Fictionalized examples of OT Cyber Risk
Real World Scenarios
MAYER | BROWN
DRAGOS

Restoration From Maintenance Fails

- **Gas compressor trips upon start**
- 3 hours lapse then console operators unable to logon to system
- No RCA; 3 consoles rebuilt
- 5 days later compressor trips again
- Rogue device discovered and removed followed by widespread Denial of View
- **Key Challenge: Lack of visibility makes it difficult for security team to identify full scope of issue and remediate as appropriate.**

SolarWinds Review

- **SolarWinds Orion installation discovered**
- Company identifies SolarWinds Orion installations in environment, including OEM versions and "rogue" installations
- **Key Challenge: SolarWinds shut off is not safe solution in OT environment**



Penetration Test

- **Manufacturer performs penetration test**
- Penetration test on OT systems identifies:
  - Vulnerabilities that company is not able to mitigate fully or promptly; and
  - Policy violations and other missteps by internal teams.
- **Key Challenge: Lack of internal preparation for penetration test.**

High Profile Vulnerability Disclosure

- **Energy company responds to the disclosure of significant OT vulnerability.**
- Company works to identify affected systems and develop a remediation plan.
- However, company struggles to settle on remediation strategy given business implications.
- **Key Challenge: Lack of internal policies makes it difficult for company to respond effectively and consistently across facilities and geographies.**

Dragos reported that no patch was available for 26% of the vulnerabilities reported in ICS advisories in 2019.


Strategies for Managing OT Cyber Risk
Lessons Learned
MAYER | BROWN
DRAGOS

Understand Risk

- Conduct technical and policy assessment.
- Key questions:
  - Does the company have adequate visibility?
  - Are adequate technical controls in place?
  - Are policies and procedures sufficient?
  - Does business meet evolving legal expectations?
- Perform under privilege where possible.

Maintain Appropriate Plans and Policies

- Ensure that company has appropriate plans and policies both to ensure legal compliance and to maintain a robust security posture.
- Ensure that IR plan is adequate. Be careful about reliance upon disaster recovery plan, business continuity plan, or data breach response plan.
- Ensure that have appropriate vulnerability management plan.
- Ensure that have effective vendor management.
- Focus on supply-chain management as necessary.

Practice

- Training and practice ensure that the effort and resources expended to prepare for a cyber incident are deployed efficiently and effectively when it counts.
    - Build preparedness through practice;
    - Identify potential pitfalls and process gaps;
    - Meet regulatory expectations; and
    - Clarify roles and responsibilities and build relationships.
- To make tabletops and training most effective:
    - Tailor scenarios to business and relevant cyber risk;
    - Include appropriate stakeholders;
    - Capture lessons learned

Prioritize Within the Organization

- Support resource allocation during period of constrained budgets.
- Build relationships between security and legal teams, and other stakeholder groups within the business.
- Elevate to senior management and the board as appropriate.

Manage Legal Privilege

- Managing legal privilege across OT cybersecurity contexts can help facilitate candid discussions of security posture and associated legal risk in a safe manner.
- Examples of projects that may be undertaken under privilege include:
  - Cyber incident response;
  - Security posture assessment;
  - Penetration test
  - Response to vulnerability disclosure;
  - Tabletop exercise;
  - Policy development.
- Privilege should be managed according to relevant recent legal guidance, as reflected in the *Capital One* decision and other recent decisions.

Americas | Asia | Europe | Middle East

mayerbrown.com