MAYER | BROWN

Cyber Spotlight: *Managing Cyber Legal Risks to Industrial Systems*

Stephen Lilley
Partner

Veronica Glick
Partner

October 2021

Today's Speakers

Stephen Lilley
Partner
+1 202 263 3865
slilley@mayerbrown.com

Veronica Glick
Partner
+1 202 263 3389
vglick@mayerbrown.com

Industrial Cyber Threats and Legal Risks

MAYER | BROWN

Industrial Cybersecurity in Context

Enterprise Cybersecurity	Focused on protection of confidential data and systems that are critical to business operations.
Industrial Cybersecurity	Focused on protection of industrial systems that control physical devices and processes, or adjacent systems.
Privacy/Data Protection	Focused on collection, use, and sharing of personal data, including across borders.

Key Risks and Recent Incidents

Key Risks
Safety
Business disruption
Environmental harm
Product integrity
Financial loss
Reputational harm

- The May 2021 **ransomware attack on a major U.S. pipeline** led to a halt in operations, intense public scrutiny, and litigation.
- In February 2021, a hacker attempted to alter chemical levels in a **Florida municipality's water** supply.
- In 2019, a **metals and mining** company reportedly suffered **~$70M-$80M** in losses due to a ransomware attack that forced the company to switch to manual operations.
- In 2017, **NotPetya** disrupted a global company's **shipping, oil and gas production and drilling services.**

Legal Risks

Litigation:

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

Regulation:

- Rising expectations across industries and possible increase of regulatory requirements going forward.
- 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.
- Unfavourable contractual provisions.

Government Scrutiny is Intensifying

- The Biden Administration is raising expectations for cybersecurity related to critical infrastructure and other industrial systems.
  - Cyber Executive Order on Improving the Nation's Cybersecurity – May 12, 2021
  - National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems – July 28, 2021
  - TSA Security Directives for Critical Pipelines – May/July 2021
- Congress also is considering numerous legislative proposals regarding critical infrastructure cybersecurity, including with respect to incident reporting.

Mitigating Cyber Legal Risk

MAYER | BROWN

Mitigating Legal Risk

Risk Assessment	• Identifying and evaluating significant legal risks posed by the company's current industrial cybersecurity posture.
Governance	• Developing appropriate plans and policies as well as coordination, escalation, or oversight bodies.
Preparedness	• Ensuring incident response plans are appropriately tailored to the company's needs and practicing in tabletop exercises.
Gov't Engagement	• Engaging with regulatory, national security, and law enforcement agencies in a way that mitigates company's legal risk.
Incident Response	• Guiding company through cyber attacks on industrial systems, including investigation and analysis of legal obligations.

Risk Assessment

- Understanding the company's industrial cybersecurity risk profile allows the company to make informed decisions and prioritize its actions.
- An assessment can review policies and procedures, or dive into detailed technical questions, with the help of a security vendor.
- Key questions include:
  - Are policies and procedures sufficient?
  - Does business meet evolving legal expectations?
  - Are roles and responsibilities clearly defined?
  - Does the company have adequate visibility?
  - Are adequate technical controls in place?
- Perform under privilege as appropriate.

Governance

Effective oversight by senior management and the Board of Directors will reduce legal risk to the business, as well as those officers and directors

- Vulnerability management
  - Best practices include: maintain and implement a tailored vulnerability management policy; employ other risk mitigation techniques; and perform penetration testing.
- Supply chain/vendor management
  - Vendor cyber legal risk management includes tiering vendors by risk level, ensuring contracts cover legal requirements, mitigating risks associated with the compromise of vendor services, and developing relationships with vendor security personnel.
- Legal privilege, confidentiality, and data retention

Incident Response Plan

- An incident response plan helps a company to respond effectively to industrial cyber incidents by:
  - Clearly stating goals and objectives
  - Categorizing incidents to which the plan applies
  - Establishing incident severity categories and corresponding levels of deployment
  - Identifying response team members and their respective roles
  - Defining a process that enables agile decision-making by the response team
- Companies will likely benefit from a tailored plan for response to an industrial cyber incident – often the company's data breach response plan and business continuity/disaster recovery plan provide insufficient guidance.

Tabletop Exercises

- Training and practice ensure that the effort and resources expended to prepare for a cyber incidents are deployed efficiently and effectively when it counts.
  - Build preparedness through practice
  - Identify potential pitfalls and process gaps
  - Meet regulatory expectations
  - 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 across all key groups
  - Capture lessons learned

Effective Incident Response

- Key elements of an effective response to cyber incidents typically include:
  - Understanding of roles and responsibilities in a response
  - Timely coordination among stakeholders within an organization
  - Sound judgments by appropriate stakeholders, including internal escalation
  - Third-party resources (e.g. forensics firm, outside counsel, communications consultant)
- Companies experiencing industrial cyber incidents will need to consider whether they have obligations to report incidents – or otherwise would benefit from disclosing the incident.
  - Regulators increasingly require notification about incidents on short timelines.
  - Relevant contracts also may require disclosure and public companies may need to disclose incidents to investors.

Americas | Asia | Europe | Middle East

mayerbrown.com