MAYER | BROWN

Managing Industrial Cyber Legal Risks in the Chemical Industry

Chemical companies face growing cyber threats to the industrial systems that monitor and control processes at the heart of the industry – often referred to as "industrial control systems" or "operational technology." Companies across the chemical sector face significant risks from these threats, including from highly sophisticated adversaries that are specifically targeting industrial systems. Public reports have revealed, for example, that chemical companies have suffered significant disruptions to their operations because of attacks on the industrial control systems on which they depend. Lloyds of London recently warned insurers that they should be more attentive to the risk of major physical damage in manufacturing environments. Leading industrial security companies have reported on specific attacks and continuing threats to the chemical sector. Likewise, numerous government agencies have sounded the alarm, warning operators of industrial systems of the dangers posed by cyber attacks, including process degradation, production stoppages, and safety risks.

These threats bring corresponding legal risk. An attack on industrial systems may generate substantial litigation exposure, from mass tort claims to breach of contract actions, to derivative actions or securities class actions. Likewise, an incident or even internal missteps prior to an incident could lead to companies facing significant compliance risk and corresponding penalties. For example, the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security has the authority to impose penalties on certain chemical facilities for failures to comply with the Chemical Facility Anti-Terrorism Standards.

This legal scrutiny is only going to increase in the coming years. Regulatory expectations for industrial cybersecurity are increasing as the Biden Administration prioritizes the protection of critical infrastructure. So too is visibility into industrial cybersecurity practices: recently passed legislation, for example, granted the Department of Homeland Security new authority to subpoena internet service providers to help identify owners of vulnerable systems. Litigation risk similarly will grow along with the industrial cyber threats that companies face.

Mitigating legal risks relating to industrial cybersecurity consequently should be a priority for legal departments across a broad range of chemical companies. Legal teams fortunately can draw upon many of the risk management tools from enterprise cybersecurity and other contexts to identify, assess, and mitigate these

legal risks. These tools include risk assessments, development of appropriate policies and procedures, and management of attorney-client privilege. The risks may be substantial, in other words, but legal departments are well-positioned to address them.

Solutions are not simple, however. The industrial context presents unique challenges that require tailored approaches. A data breach response plan is unlikely to be adequate to guide a company through an industrial cyber incident, for example. Nor are business continuity plans or disaster recovery plans likely to suffice. Those plans may not include the correct stakeholders or escalation protocols, for example, or may not address the key questions that a company must be prepared to resolve during an industrial cybersecurity incident.

Practical challenges also may raise further hurdles. While a legal team may have deep relationships with the information technology/security function, it may have no such relationship—at least with respect to cyber matters—with the team responsible for securing industrial environments. This may create threshold challenges—including with respect to the basic question of who to call—as well as lead to ongoing implementation challenges that could be more easily met if established relationships were in place.

Likewise, the legal challenges faced by a company may be greater in this context because of practical limitations of industrial systems. A company may have limited visibility into its operational environments, for example, and likely will be operating older systems, with longer lifecycles, that are not readily patched and may be beyond their support lifecycle. As a result, a company may face greater challenges than in the traditional enterprise context when it responds to cybersecurity incidents or vulnerability disclosures affecting industrial systems.

> *"As we have seen with the wave of ransomware attacks and intrusions into critical infrastructure, cyber threats are coming dangerously close to threatening our lives."*
> — DHS Secretary Alejandro Mayorkas.

The chemical sector faces significant industrial cyber threats. In 2019, for example, a ransomware attack reportedly impacted multiple chemical companies, forcing some to switch to manual operations. Cyber attacks on chemical sector industrial systems threaten potentially catastrophic consequences including large scale failures of critical infrastructure, compromise of safety systems at facilities, or personal injury or death. The substantial scale of potential legal risk associated with such terrible outcomes is readily apparent.

A chemical company need not even experience a catastrophic attack to be exposed to significant legal risk. Even a relatively limited cyber incident affecting industrial systems can lead to significant regulatory or litigation exposure. A successful intrusion or disclosed vulnerability in a manufacturing, critical infrastructure, or other system can create diverse legal risks, including under governing contracts, guidance requiring disclosure of incidents, or through engagement with non-regulatory agencies.

The good news: these legal risks can be mitigated through reasonable steps that companies can take in advance of experiencing industrial cyber incidents, including developing an appropriate understanding of the legal risks facing the company, putting in place appropriate plans and policies, as well as other governance mechanisms, and practicing use of those policies.

Our Capabilities

Mayer Brown's Cybersecurity & Data Privacy team has extensive experience advising companies on the management of cyber legal risk from industrial systems. From helping companies respond to attacks on their production lines to advising on the development of vulnerability management programs for industrial systems and counseling on the allocation of legal risk in governing contracts, our lawyers have helped companies navigate complex and cutting edge legal issues presented by industrial cyber risk.

Our team draws upon its extensive experience helping clients in the chemical industry and other sectors manage industrial cyber risk, as well as their diverse backgrounds in government service and other fields. Our team also leverages the extensive capabilities of our global firm, working with lawyers across the firm who have deep knowledge of relevant regulatory frameworks, industry practices, or the specific legal challenges that a client faces.

We are well-positioned to help you manage the most complex cyber legal risks, including through:

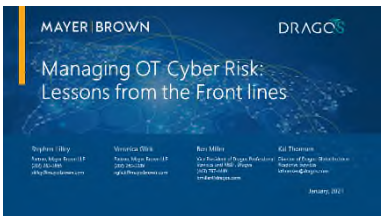
- **Legal risk assessment**—We help companies identify and mitigate significant legal risks posed by their current industrial cybersecurity posture, including with respect to high-profile vulnerability disclosures (e.g., SolarWinds). We work closely with security teams in privileged engagements to provide practical legal advice. In doing so, we help companies prioritize their management of cyber legal risk so that they can minimize legal exposure as efficiently as possible.
- **Governance**—We help companies organize their response to industrial cyber risk through appropriate governance tools. This includes advising companies on the development of appropriate plans and policies (e.g., industrial cyber incident response plan or vulnerability management plan) to ensure both effective internal coordination and regulatory compliance, as well on the creation or refinement of appropriate coordination, escalation, or oversight bodies.
- **Exercises**—We lead tabletop exercises for company stakeholders to practice use of incident response processes and to capture any lessons learned for further refinement of governing plans and policies. We focus on delivering tailored scenarios that help companies identify areas for improvement, build internal collaboration mechanisms, and gain experience using governing plans—all while managing associated legal risk.
- **Incident response**—We help guide clients through cyber attacks on industrial systems, including through thorough investigation of the incident, careful analysis of legal obligations, and practical guidance on overall risk management. We stay focused on the company's strategic interests while offering tailored, practical advice so that companies can reduce their legal exposure from cyber attacks or high-profile vulnerability disclosures.
- **Government engagement**—We work closely with clients as they engage with the broad set of regulatory, national security, and law enforcement agencies focused on the security of industrial systems. We provide tailored advice based on the unique legal risks facing a client, while remaining attuned to the broader trends in government engagement in this field—including the likely continued growth in government scrutiny of the security of industrial systems going forward.

Representative Matters

We regularly advise operators and manufacturers of industrial technologies, and other key stakeholders, on managing operational cyber legal risk. Illustrative examples of our experience include:

- Performing a cybersecurity legal risk assessment for a leading global chemical company and advising on revisions to governing policies and procedures.
- Advising a leading global manufacturer in response to a cybersecurity incident involving ransomware infections that affected production lines across multiple facilities internationally.
- Counseling a leading global manufacturer of operational technology on revisions to its coordinated disclosure and vulnerability management processes.
- Advising a global manufacturer of industrial equipment used in core critical infrastructure on engagement with government agencies regarding vulnerability testing.
- Counseling the board of directors of a publicly traded oil company on managing operational cyber risks.
- Leading an assessment of the impact of SolarWinds across the global technology footprint of a prominent pharmaceutical manufacturer.
- Advising a leading operational cybersecurity provider on contracts governing incident response services.
- Advising an information-sharing organization on legal protections for the sharing of cyber threat indicators relating to industrial control systems.
- Engaging with government agencies on behalf of a multinational manufacturer of critical infrastructure systems on the mitigation of potential national security risks.
- Counseling a communications company on its potential designation as "Section 9" critical infrastructure under Executive Order 13636.
- Advising a global automaker regarding a ransomware incident that stopped production at a Tier 1 supplier.

Recent Webinars



For more information about our recent webinars please click the thumbnails above.

Contacts

We would be happy to speak with you about how we can help your business reduce the legal risk posed by industrial cyber threats. For more information about our practice, please contact:

Rajesh De
Partner
rde@mayerbrown.com
+1 202 263 3366

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

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