5 Steps For Legal Teams To Mitigate Industrial Cyber Risk

By **Stephen Lilley, Veronica Glick and Ben Miller** (July 19, 2021)

Stephen Lilley

Veronica Glick

Ben Miller

Recent events have left no doubt: Cyberattacks present a substantial threat to critical infrastructure and other industrial systems. Companies operating in the energy, chemicals, transportation, manufacturing, infrastructure and other relevant sectors should understand and respond to these threats.

Indeed, numerous reports have described sophisticated nation-state actors' efforts to compromise electric grids, as well as destructive attacks on industrial systems around the world.

An attack on a Florida municipality's water system, for example, highlighted how attacks can lead to physical injury or environmental impacts. Likewise, the recent pipeline shutdown showed how cyberattacks on critical infrastructure could have substantial ripple effects across the economy.

These attacks can cause severe business disruption, create safety risks or cause significant reputational harm. Legal risks from industrial cyberattacks likewise are substantial.

While specific legal risks vary by sector, relevant businesses may face regulatory enforcement, consumer class action or mass tort litigation, commercial litigation, securities or derivative litigation, or other forms of suit.

Likewise, companies may face substantial reputational risk from a publicly disclosed attack or vulnerability, including public scrutiny of their engagement with the government, decision on whether to pay ransom and their handling of other elements of their response.

This scrutiny will continue to increase as governments prioritize strengthening critical infrastructure cybersecurity.

In the U.S., for example, the National Security Agency recently warned companies about the cybersecurity risks to industrial systems. And President Joe Biden's Executive Order 14208 on improving the nation's cybersecurity expressly highlights the operational technology that supports critical infrastructure.

It urges the private sector to "adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace." Likewise, the Biden administration already has moved to impose new cybersecurity regulatory requirements on the pipeline industry.

Managing cyber risk consequently is a priority for operators of critical infrastructure and other industrial systems — and legal departments have an important role to play.

Industrial cybersecurity presents distinct legal risks from traditional enterprise cybersecurity. An attack that halts an industrial compressor is very different than a

compromise of personal data. Still, legal teams — working with partners on the security team and elsewhere in the organization — can draw upon familiar risk management practices to mitigate these risks.

Here are five steps companies can take now to strengthen their industrial cybersecurity posture and reduce associated legal risks.

1. Understand Your Risk

Understanding the risks a company faces from industrial cyber threats can provide a strong foundation on which a legal team can build. While the specifics will vary by company, answering three component questions can help a legal team understand its applicable regulatory, litigation and contractual risk under governing frameworks.

First, evaluate the maturity of the company's industrial cybersecurity program. To be clear, the legal team should not expect to be able to offer an opinion on the adequacy of technical security controls or architectures.

However, basic questions can still allow a legal team to quickly understand the cybersecurity program's general posture; i.e, the nature and scale of threats that it faces, the quality of its defenses and its readiness to respond effectively if those defenses fail.

For example, a legal team can ask whether the company has performed a cyber risk assessment for the systems it operates and, if so, what actions the company has taken in response to that assessment. Likewise, the legal team can review relevant policies and procedures to evaluate whether they address necessary topics and if they provide sufficient guidance to the relevant teams.

The legal team can also review existing contracts to determine whether responsibility and liability are appropriately allocated between themselves and their vendors. Moreover, the legal team can evaluate existing governance mechanisms to understand whether industrial cyber risk is managed effectively across stakeholder groups and overseen effectively by senior management.

Through these and related inquiries, the legal team can quickly understand the overall state of the company's program for managing industrial cyber risk.

Second, consider how technical or administrative hurdles may complicate cyber risk mitigation. Industrial systems are often not visible to company administrators, for example, and a company may not be readily able to patch machines or take them offline when an incident occurs.

Industrial machines are not smartphones, after all, but have high uptime requirements and extended lifecycles, including beyond their support date in many instances, and must be managed differently as a result. Understanding how such practical constraints apply in the context of their business will help legal departments better understand relevant legal risks.

Third, identify existing touch points with the government, along with likely government expectations for future engagement. Operators of critical infrastructure in particular should anticipate a diverse range of government stakeholders to take interest in their activities.

Whether through regulatory or nonregulatory agencies, this engagement can bear significant risks for companies. Understanding the likely touch points can help companies

avoid being caught off guard by such risks.

One practical tip: Legal teams should be skeptical of claims that a company does not need to focus on cybersecurity, because its industrial systems are not connected to the internet or are too old to be hacked. A legal team may need to pressure test such claims in order to mitigate cyber risk effectively, including by suggesting that a third-party expert validate such statements through a pen test or other means.

2. Have a Plan

A well-tailored incident response plan can be the difference between an effective response to a cyber incident and a response that compounds the problems caused by a cyber incident.

Plans can vary substantially across companies based on their culture, organization, and specific legal risks and obligations. At bottom, however, incident response plans typically describe the process that companies will follow in responding to incidents, and roles and responsibilities of identified stakeholders — and such plans are appropriately tailored to the company.

Putting such a plan in place is a critical first step. Importantly, companies that operate critical infrastructure or other industrial systems should not assume that a business continuity plan or disaster recovery plan will adequately address the full range of cyber incidents that a company may experience.

Likewise, a critical infrastructure company should not assume that its plan for responding to attacks on its traditional IT systems, or to a data breach, will provide sufficient guidance for responding to incidents involving industrial systems. Rather, they should ensure that their plans leverage appropriate technical teams and escalation protocols, given the types of industrial systems at issue and the internal allocation of responsibilities.

Over time, a critical infrastructure company should ensure that its incident response plan continues to provide relevant and timely guidance. For example, a plan or plans should provide guidance for likely scenarios, including attacks on information technology systems at the convergence with industrial systems, as well as attacks on operational technology itself.

The incident response plan also should guide the relevant team through decisions a company may have to resolve — including when and how to engage with law enforcement and other government stakeholders, and whether to pay a ransom. Similarly, an incident response plan should incorporate lessons learned from prior incidents and exercises.

Finally, the incident response plans should map to capabilities. Monitoring and logging systems are critical to response efforts, and are often missing within critical infrastructure environments. This lack of visibility is a huge challenge for many, and must be understood and accounted for in the incident response plans.

3. Build Relationships

Delivering timely advice to the right stakeholders is critical to effectively reducing a company's risk from industrial cyber threats. That will require groups responsible for securing, operating or supporting industrial systems to know why, when and how to work with the legal team on industrial cybersecurity matters.

This in turn requires the prior development of working relationships with those stakeholders — whether in engineering, safety, plant management or other groups. That work can take time, particularly if the legal team must win their buy-in, and educate them on the legal department's role in industrial cybersecurity. Nonetheless, it is work that pays dividends.

Engaging with those stakeholders will allow the legal team to explain how it can help reduce relevant risks, as well as when those stakeholders should reach out to the legal team for assistance. Likewise, it will enable the legal team to understand roles and responsibilities within the organization, potential sources of friction or uncertainty, and potential gaps in the company's approach.

Whether through formal training or informal outreach, those relationships can be extremely valuable for understanding how to navigate industrial cyber risk management challenges within the company, as well as for building trust that the team can draw upon during an incident.

Companies with more mature programs may well have established relationships in place. While the heavy lifting may largely be done for those organizations, maintaining strong relationships is an ongoing process — whether because stakeholders change positions or leave the company, or because new challenges or internal questions may strain existing relationships.

Key relationships also may reach beyond the company itself. Attacks on industrial systems in particular demand expertise specific to the industrial systems a company operates. Putting those resources in place in advance of any future incident can facilitate an effective response and reduce legal risk.

4. Practice

An organization should not test out its incident response plan for the first time during an actual cyberattack on industrial systems.

Instead, companies should use tabletop exercises to prepare to handle a real incident, and to capture any lessons learned for further refinement of governing plans and policies.

The tabletop scenario should be tailored to risks faced by the company, to ensure these exercises are as realistic and effective as possible. Such exercises can contribute with the relationship building discussed above, as well as further clarify appropriate roles and responsibilities across groups.

They also can feed back into the legal team's ongoing assessment of the company's cybersecurity posture, by allowing the legal team to determine how the company's team, policies and procedures fare when facing a realistic, if hypothetical, scenario.

In this way, tabletop exercises can play an important role in a company's ongoing strengthening of its cybersecurity program.

5. Engage Company Leadership

Industrial cyber risks frequently are among the most significant risks facing critical infrastructure companies and other businesses in relevant sectors.

Effectively managing those risks can require substantial ongoing investment in systems and personnel, as well as broad-based engagement by a wide range of stakeholders across the business. Securing support from senior executives and the board of directors will be critical to the long-term success of this work.

As a result, the legal team and business leaders will be well served to ensure appropriate mechanisms are in place to provide relevant and timely information to the company's senior leadership, so that it can properly understand and oversee the company's approach to managing industrial cyber risks.

Companies may wish to consider, for example, whether an internal, cross-functional committee structure or another approach will provide the best mechanism for organizing efforts across the company and enabling effective oversight by senior leadership.

In doing so, companies should remain attuned to directors' fiduciary duty to oversee risk management efforts, as well as consider whether lessons can be drawn from other companies' approaches to managing enterprise cyber risk at the board level.

For example, public companies may wish to consider whether management of industrial cyber risk should be assigned to a particular committee of the board.

Stephen Lilley and Veronica Glick are partners at Mayer Brown LLP.

Ben Miller is vice president of professional services and R&D at Dragos.