BRACEWELL

INSIGHTS

Avoid a Fall Out With the Feds: Planning for Increased Cyber Regulations

May 17, 2021

By: ***Seth D. DuCharme***

The cyber landscape is changing once again, in terms of impact, policy and potential exposure. In the wake of the Colonial Pipeline ***hack***, the Biden administration released a long-awaited Executive ***Order*** intended to strengthen US cybersecurity infrastructure. The order, released on May 12, triggers the rulemaking process to modernize cybersecurity within federal government systems and increase regulation of federal contractors. While much of the substance and posture of the Order is a continuation of historical trends, a few notable developments have materially changed the operating environment, including the prospect of greater federal regulation.

Because of recent cyber events and increased government attention to cyber, many private corporations are reassessing their cyber incident response plans, as evolving expectations present new challenges to maintaining resilience and public trust. A well-prepared organization must continually assess whether its plan is sufficient to (1) mitigate the direct and collateral consequences of technical attacks, (2) quickly analyze legal exposure, and (3) communicate effectively with stake holders, regulators and the public to meet or exceed expectations.

It's no secret that the federal government wants to bolster cyber infrastructure and enforcement of cybersecurity standards, and has for some time. Last month, for example, the Department of Energy ***released*** a 100-day cybersecurity pilot program, and the Federal Energy Regulatory Commission is one of many government agencies taking ***steps*** towards establishing incentive-based programs for cybersecurity investments.

The May 12 Executive Order, much like past federal guidance, emphasizes the government's interest in public-private partnerships in the realm of cybersecurity. But if and when the proposed rules are finalized, they will be the first to impose cybersecurity standards on private companies. Notably, the rules outlined in the Executive Order are only applicable to the federal government and IT/OT federal government contractors, but the announcement signals that regulations for other industries may be forthcoming. Organizations thus need to be prepared not only for the evolving technical threat landscape, but also for increased regulation and scrutiny by regulators and stakeholders.

The best way to mitigate the fallout of a cyber incident is to have a comprehensive cybersecurity plan, both for prevention and response, that meets or exceeds industry standards. Cybersecurity plans aren't just about making sure that technology is up to snuff, however: legal analysis and clear communication strategies are just as essential.

In assessing whether an organization's plan is sufficient, it's important to understand that cyber vulnerabilities remain largely human behavior challenges, including in the post-incident phase. Consider, for example, phishing attacks – by now, most employees know what a phishing attack is and that they are supposed to take care to avoid clicking on suspicious links. But human beings are impulsive in cyber-space, and as phishing techniques and all other forms of cyber attacks get more sophisticated, it becomes increasingly difficult to avoid each lure.

In light of the need to rapidly adapt to evolving threats, the best cybersecurity plans are living and breathing resources, capable of adjusting as the landscape evolves and nimble enough to execute in real time. To ensure flexibility, effectiveness and fidelity, every aspect of a cybersecurity plan should account for the relationships between technical, legal, policy and behavioral concerns. This is particularly true in the absence of standardized, concrete federal requirements, and as organizations face increased scrutiny of cyber incident responses.

A key feature in a human-behavior-oriented cybersecurity plan is a context-conscious communications strategy. A properly contextualized communications strategy isn't just about defining communications parameters for the company writ-large; it also requires plans tailored to individual roles. Both internal and external communication are critical to understanding and managing a breach, as employees can aggravate the harm if they lack a clear understanding of the limits of their areas of responsibility and the dangers of misinforming management, the public or investigators. Training employees to responsibly protect the organization in the legal and reputational environments is part of a comprehensive strategy to come through an incident intact, especially as expectations evolve and scrutiny increases.

Beyond being imperative for reputation management, clear communications plans can also minimize technical and legal hurdles. If every member of your company is trained appropriately according to their role, ideally through modularized training, cyber responses can be conducted more swiftly. Similarly, if everyone knows his or her role is in a cyber event, it will be much easier to quickly contain and, thus, to reassure government agencies, shareholders and employees that the situation is under control. This can help to mitigate both reputational and legal consequences of a cyber attack, and can even bolster the organization, like a ship that weathers a ferocious storm.[1]

The worst case scenario in the event of a cyber attack is having no plan at all. Cyber incidents are incredibly sensitive, particularly from a legal perspective, and any response will need to be tailored both to the incident and to your specific organization. Involving counsel early and often can help prevent situations where an organization is making decisions about employees' sensitive data, intellectual property, or, even worse, its actual operations with a virtual gun to its head.[2]

If your organization does not have a cyber plan that accounts for the current landscape, now is the time to make one. Company leadership should coordinate with IT, inside and outside counsel, and communications teams in order to develop a plan that at least meets, if not exceeds, industry standards. Outside counsel can provide particularly helpful perspective on how to make sure that a plan appropriately considers human behavior and properly contextualizes your organization's needs.

If your organization does have a plan, and you think it's a particularly good one, now is a great time to publicize your success.[3] Shareholders are increasingly interested in the strength of

companies' cyber programs, and, importantly, the rules discussed in the new Executive Order have yet to be written. Now is a good time to consult with counsel and government relations specialists about how to influence the future of cybersecurity legislation and regulation.

Lastly, whether you're formulating an entirely new plan or updating an existing one, consider fine tuning for efficiencies and highlighting interests that are aligned with the federal government, which will assist you in working with partners who may be essential to long term survival. As additional rules and regulations impose new standards on private industry, companies should seek advice from counsel about how to craft a cybersecurity plan that correlates as closely as possible with government priorities, while finding opportunities to prepare the overall environment for success.

Hackers and regulators have put all of us on notice: new and significant challenges lie ahead. Bracewell's seasoned attorneys and government relations experts are ready to help organizations formulate and carry out thoughtful and effective cybersecurity plans as federal oversight increases.

---

1. For example, it is important for publicly traded companies to have a clear communications plan regarding disclosures, as both under- and over-disclosure can ***lead*** to both government enforcement actions and civil litigation.

2. A common and particularly frightening example of this type of scenario is a ransomware attack, which have cost unsuspecting ***municipalities*** millions of dollars in recent years.

3. Without over-disclosing, of course. Organizations should consider engaging counsel before publicly sharing details of its cybersecurity plan.