LAWFARE

CYBERSECURITY

# What Is a Cybersecurity Legal Practice?

By **Daniel Sutherland** Friday, April 2, 2021, 11:10 AM

**DayZero: Cybersecurity Law and Policy**

Recent surveys by the Association of Corporate Counsel (ACC) consistently reveal that one of the top concerns for general counsel at private companies is cybersecurity. This concern is certainly well placed, given the steady stream of alarming incidents involving the security of sensitive data. As a result, corporate general counsel are increasingly hiring, or aware of the need for, an attorney who focuses on "cybersecurity." But what does that specifically mean? What should be in that lawyer's portfolio?

This is a question I have confronted in the past several years as I helped build the Office of the Chief Counsel at the new Cybersecurity and Infrastructure Security Agency (CISA). Our team of lawyers has a broad portfolio, including supporting responses to the most complex cyber incidents facing the country, negotiating complex technology agreements, developing legal and governance frameworks to address threats of emerging technologies and nation-states intent on compromising them, drafting legislation, and responding to audits and investigations. CISA, of course, is not a private company, but I hope my experience in building a cybersecurity practice for CISA will help general counsel seeking to build a cybersecurity practice within their company. (Our practice of law is much broader than cybersecurity, as CISA helps its stakeholders to build more secure and resilient infrastructure. Thus the office focuses on the broader law of critical infrastructure and, as is typical in a corporate law office, the legal issues associated with managing the business operations of a growing organization.)

Moreover, it is in CISA's strong interest to see the discipline of cybersecurity law develop and mature. Too often, the agency's offers to help a company that is under attack are delayed for days (or even weeks) because a corporate counsel's office is trying to become familiar with the subject matter. Government agencies such as CISA will be more successful in helping companies if corporate attorneys are knowledgeable about the law in this area.

### What is the current state of the cybersecurity practice of law?

In the past five years, the ACC has conducted three surveys of corporate law departments regarding how they approach data security and privacy issues. In the latest survey, published in the fall of 2020, almost 50 percent of chief legal officers expect their (already substantial) role in cybersecurity to continue to increase. For example, more than 70 percent of corporate legal departments play a "significant role" in setting the company's policies on information sharing with the government. Moreover, the role of chief legal officers in responding to data breaches is growing. In 2015, chief legal officers said they were the primary point of contact for leading the company's response to a data breach in only 4.6 percent of cases; in the 2020 survey, that proportion had jumped to 21.2 percent.

But the data also shows that the practice of cybersecurity law is still very much in the early stages. According to the surveys, companies are all over the map when it comes to personnel responsible for leading the response to a data breach—companies have identified seven different senior corporate positions as the primary incident response leader (CEO, chief information officer [CIO], chief information security officer [CISO], "head of IT," privacy officer, chief risk officer and chief legal officer). The 2020 survey also shows that almost 75 percent of corporate legal departments have not developed internal processes to leverage existing information-sharing statutes such as the Cybersecurity Information Sharing Act of 2015. When asked why the company does not share information with the government, the vast majority of respondents, almost 75 percent, answered: "Our organization does not have the resources or knowledge base to engage in these types of programs." If these surveys are any indication, the practice of cybersecurity law is still quite nascent.

### Where does the cybersecurity attorney fit in an organization?

A cybersecurity attorney is not an auditor; this attorney does not sit in an ivory tower doing oversight of the company's information technology work. Instead, corporate officers must recognize that a cybersecurity attorney must be a part of the operational team. The attorney should be as involved in the company's operations as the information technology expert deploying new defensive measures in the company's networks. An effective cybersecurity attorney has to be in the trenches, helping to develop the statements of work for new contracts, negotiating information-sharing agreements, advising on legal risks associated with the many and varied daily decisions of securing networks, and managing the hour-by-hour response during an incident.

### What legal grounding does the cybersecurity attorney need?

A cybersecurity attorney must establish a strong base in foundational cybersecurity statutes in order to contribute effectively to the company's operations. These statutes include the Electronic Communications Privacy Act (including the Computer Fraud and Abuse Act and the Stored Communications Act), the critical infrastructure provisions of the Homeland Security Act, the Cybersecurity Information Sharing Act of 2015, the Federal Trade Commission Act (FTCA), data breach notification laws, applicable sector-specific state and federal laws (particularly for the financial, health care and government contracting sectors), and many others.

The cybersecurity attorney also needs a firm understanding of privacy law. While the two disciplines are distinct, one of the core functions of a cybersecurity attorney is to ensure the company properly stewards the data entrusted to it. Therefore, the cybersecurity attorney must be—at a minimum—conversant in privacy law. Privacy regimes impose requirements to improve the security of data because security enables data to remain private.

Finally, a cybersecurity attorney must be multilingual in the jargon of both law and tech. One of the key jobs of such an attorney is to translate legal requirements (such as obligations imposed by regulations) into design requirements *and* to understand the technical details enough to ask probing questions, spot legal issues and translate risks to organizational leadership. The attorney must be a Rosetta Stone—translating the law into language technologists can understand—and vice versa. Therefore, the attorney needs to understand the basics of technology, or at least have a curiosity and drive to learn.

**What subject areas should be in the attorney's portfolio?**

*Government*

In cybersecurity, companies must expect to engage with government—it is inevitable. A cybersecurity attorney must understand the delineation of each government agency's authorities. The attorney should know the answer to the question: "What can X do to us?" But the attorney should also know the answer to the question that is often not asked (primarily due to ignorance): "How can X *help* us?" Congress has given CISA, the FBI and other government agencies authorities that permit them to be significant assets to a private company. The agencies can even go as far as providing needed capabilities and tools. Moreover, government lawyers often seek to negotiate novel public-private arrangements that benefit both the company and the larger ecosystem. Corporate counsel need to have a strong grounding in cyber and national security law so that they do not evaluate the proposed deal as a simple commercial contract but, rather, as an opportunity for the company to access and leverage uniquely sensitive government data.

Beyond knowledge of statutes, the cybersecurity attorney should also be able to help the company build relationships with key government agencies. Relationships with agencies such as CISA, the FBI, the state attorney's general office, the Securities and Exchange Commission, the Federal Trade Commission (FTC) and others are critical. The attorney can often be helpful in establishing and maintaining those relationships. For instance, many government agencies approach companies from a law enforcement or regulatory perspective, so they are comfortable dealing with attorneys. The cybersecurity attorney and the company's CIO and CISO should all have relationships with these agencies.

A cybersecurity attorney needs to understand the regulatory landscape. This should include, for example, the work of the FTC under Section 5 of the FTCA, a law with significant data security implications for many companies. The attorney should fully understand the regulations that govern the company's work, and should work closely with the cybersecurity team to document the alignment of the company's policies and controls to those regulatory provisions. The attorney should also ensure a process is in place for each control associated with a regulatory requirement to be monitored for adoption and performance. More broadly, the attorney should understand regulatory frameworks in other sectors; the regulations adopted in one sector might be adopted in others, and the enforcement actions taken in one sector might be taken with regard to companies in others.

Finally, a cybersecurity attorney must also be aware of emerging legislation—and not just react to laws after they have been passed. This includes an awareness of provisions in major legislation as they are being discussed and drafted on Capitol Hill and in state legislatures, and, if advising a global company, the additional applicable jurisdictions. This knowledge would allow organizations to monitor what changes are likely to be necessary and plan accordingly, rather than rush to apply an ad hoc change. Some companies may even be able to task their attorneys with working with lawmakers to develop laws that are informed with industry expertise.

*Litigation*

The cybersecurity attorney must understand the litigation landscape. Decisions issued by federal and state courts may impact the company in its cybersecurity efforts. For example, what is the significance of the federal criminal indictment of the former CISO of a company who failed to report a data breach? What is the significance of the recent federal court decision regarding whether a security report prepared by an incident response company can be protected under the attorney-client privilege? The cybersecurity attorney should track applicable litigation and develop advice to help guide the company.

*Internal Practices*

*The risk assessment process*. The cybersecurity attorney must have a strong role within the company. For example, the attorney should be involved in the company's cybersecurity risk assessments. This could include ensuring that the assessment is crafted to reduce potential liability, and to determine whether privilege may be appropriate to protect some aspects of the risk assessment. The cybersecurity attorney should be a key player in developing the entire cybersecurity program, including how identified risks are documented, escalated, "decisioned" and resolved.

*Communications with leadership and the board of directors.* The cybersecurity attorney must be integrally involved in board and senior management communications. The attorney should review all cybersecurity-related communications to the board and senior management to ensure they are being adequately briefed on these subjects and that communications are crafted in a manner that appropriately describes risk to the firm, minimizes misinterpretation and limits potential liability. For publicly traded companies, cybersecurity attorneys should also be involved in reviewing relevant portions of financial disclosure risk statements.

*Responding to incidents.* The cybersecurity attorney must be a key player in responding to cybersecurity incidents. This critical work begins well before the company has to confront such an event. Developing and practicing sound, coherent incident response plans is a huge undertaking and absolutely essential to the company's success in dealing with such events. Developing incident response plans is a multidisciplinary project in which the attorney has to be a central player. The company has to confront questions such as: Who is on the response team? Who leads that team? At what point is our company obligated to report data events to state or federal regulators? What contracts do we need to have in place in case we need to notify employees or customers of a breach? Under privacy laws, state employment law or our company's policies, are we obligated to notify our employees? Notify our customers? Who is responsible for paying for all the remedial activities that need to be taken now?

*Evaluating contracts.* The cybersecurity attorney must be a subject matter expert on contract clauses. This expertise is essential in many instances, including reviewing and negotiating software licensing provisions, the purchase of hardware, an organization's agreements with security vendors, and any agreements for cloud computing services. The cybersecurity attorney should establish approved cybersecurity and technology-related contract clauses—for both customer and vendor contracts—and approve and track any deviations from these established provisions. The cybersecurity attorney's knowledge of the regulatory space should be used to ensure that provisions regarding appropriate notice and audit rights, among other things, are included in the pertinent contracts.

*Vendor risk management*. The cybersecurity attorney must be involved in the third-party vendor risk management process. This is particularly relevant since the United States is still grappling with the SolarWinds intrusion, one of the largest supply chain-related incidents in the history of the internet. Few organizations operate on an island without third-party hardware, software or technology services. As such, organizations must seek to limit risks flowing from third-party companies that supply these technologies and tools. The companies with which the cybersecurity attorney's organization does business either are or soon will be auditing the company's supply chain risk decisions. It is also important to anticipate the government's views as to whether these organizations are adequately secure for the applicable industry. If the government views the third-party vendor as insufficiently secure, or as a security risk in and of itself, the government could take action against the company and cause difficulties in the cybersecurity attorney's organization. In some industries, the use of such vendors might even expose the purchasing organization to liability. These potential complications make it essential that the cybersecurity attorney knows about the numerous statutes, executive orders and decisions by federal courts (in cases like Kaspersky Labs and Huawei) in this area.

*Mergers and acquisitions*. The cybersecurity attorney working for a growing company must be cognizant of the risks associated with mergers, acquisitions and divestitures. Prior to a merger or an acquisition, the cybersecurity attorney should evaluate the potential addition for cyber risks, as well as its practices in stewarding data. As the organizations are merged or one is acquired, cybersecurity best practices should be adopted and shared—with any necessary training provided to employees—throughout the whole organization. This process should go beyond dictating that one organization's practices be applied to the acquired or merged organization. Rather, policies, practices and procedures should be assessed to see what fits best.

*Insurance.* Finally, much of the cybersecurity attorney's responsibility will involve decisions around avoiding, mitigating or accepting risk. The attorney should also consider where transferring cyber risk, such as through insurance, is appropriate. These decisions should involve subject matter experts, but a cybersecurity attorney can and should advise the company on the scope and nature of any risk-transferring devices. Where an insurance policy is deemed appropriate, the cybersecurity attorney must ensure that the contract provides acceptable levels of coverage, in terms of both the amount of coverage and the scope of coverage, ensuring that it matches the company's major areas of cyber-related liability risks. For example, in some instances, the policy may need to cover only direct damages such as the loss of hardware. In other cases, however, this may be woefully inadequate, and coverage may be needed for things like professional services liability, downtime, breach response expenses and potential civil liability. The cybersecurity attorney should assess the means and needs of the organization when evaluating risk-transferring devices.

## Conclusion

It has been fascinating to watch the field of cybersecurity develop these past several years and to see how attorneys function within this maturing field. Too often, companies have a poor cyber defense posture due to a lack of substantive knowledge about cybersecurity. My hope is that this post assists general counsel supporting the development of robust cybersecurity legal practices in their offices, which benefits their companies and, in turn, the entire cyber ecosystem.

*The author wishes to thank several colleagues for their meaningful contributions to this post, including Eric Goldstein, executive assistant director for cybersecurity, CISA; Robert Kang, chief counsel, cyber and national security, Southern California Edison; and Craig Sharkey, deputy general counsel and chief privacy and data governance officer, Western Union.*

**Topics: Cybersecurity**

**Tags: CISA**

---

Daniel Sutherland is the Chief Counsel for CISA, the Cybersecurity and Infrastructure Security Agency. CISA is the nation's risk advisor, working with stakeholders to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. Mr. Sutherland's office negotiates complex technology agreements, provides daily operational support to the agency's hunt, incident response and vulnerability management divisions, advocates the agency's positions in litigation, drafts and negotiates legislation, and responds to audits and investigations, among other things.