Debevoise & Plimpton

Cybersecurity Desk Guide for Counsel – Outline

Foreword

Compared to other areas of business risk, the rapid rise of cybersecurity as a key business priority has been unprecedented. As the risks and regulations surrounding cybersecurity continue to evolve, so does the role of counsel.

Just ten years ago, legal departments were fortunate if they had a dedicated privacy counsel, and a dedicated “cybersecurity counsel” was virtually non-existent. There were very few regulations covering cybersecurity, and even those were high-level.

Today, new cybersecurity specific laws and the expectations around “reasonable security” borne out from litigation and enforcement actions have greatly changed the relationship between the legal function and information security teams. Many organizations have a dedicated cyber lawyer, and highly regulated companies may even have a team of cyber lawyers. In contrast, others rely on privacy or regulatory counsel to cover cyber, and even smaller legal departments may leave it to one of the generalists.

Though counsel have an increasingly important role to play here, cybersecurity can often feel like an impenetrable subject. It is a vast, fast paced, and quickly developing area that combines legal analysis, risk and compliance. It can be highly technical, and has increasingly serious consequences for getting it wrong.

Unsurprisingly, we are therefore often asked by clients: But what does cybersecurity involve? Where should I start? Who should I work with? And what should I look out for?

This guide is meant to serve as a desk reference for counsel on the many facets in which the legal department could engage in the cybersecurity function. Please reach out to us if you would like to discuss any of these topics in more detail, or receive a copy of the Desk Guide.

Debevoise Data Strategy & Security Team

Debevoise & Plimpton LLP is offering this guide for informational purposes only. The guide is not intended nor is it to be used as a substitute for legal advice. This publication is neither a solicitation nor an offer to represent you. The information provided to you in the guide is not intended to create and does not create an attorney-client relationship with Debevoise or with any lawyer at Debevoise. You may inquire about legal representation by contacting the appropriate person at Debevoise.

Index

Compliance & Governance

Incident Response

Partnerships

Other Topics

Outline

1. Compliance with the Legal Landscape

While counsel is a legal role, it often requires substantial compliance work, including tracking, understanding and implementing changes required by new laws and regulations. Unlike lawyers who deal with a settled body of law, like the Employee Retirement Income Security Act (“ERISA”), lawyers working in cyber law must respond to a legal landscape that is constantly in flux and developing in tandem with the proliferation of new technologies. Additionally, many organizations have not yet staffed a cybersecurity subject matter expert on the compliance team. As a result, counsel with responsibilities for managing cyber-related legal risk should be constantly monitoring for potentially relevant new developments and compliance obligations.

2. Security Technology Counseling: Cybersecurity by Design

The President’s National Cybersecurity Strategy calls for a fundamental shift in liability for software vulnerabilities. Whether adopted or not, the perspective is important: security by design is top of mind to the government and regulators. Security technology counseling goes beyond a typical “legal role.” This is more “legal adjacent,” as it calls on the counsel’s role to bring the lens of information security regulations and jurisprudence to new issues relating to new technology. This will require partnering with Risk, Compliance, and many other teams in order to (i) evaluate product security, (ii) design new product/service offerings, (iii) determine the ramifications of certain features, and (iv) implement user security initiatives.

3. Working with the Information Security Team

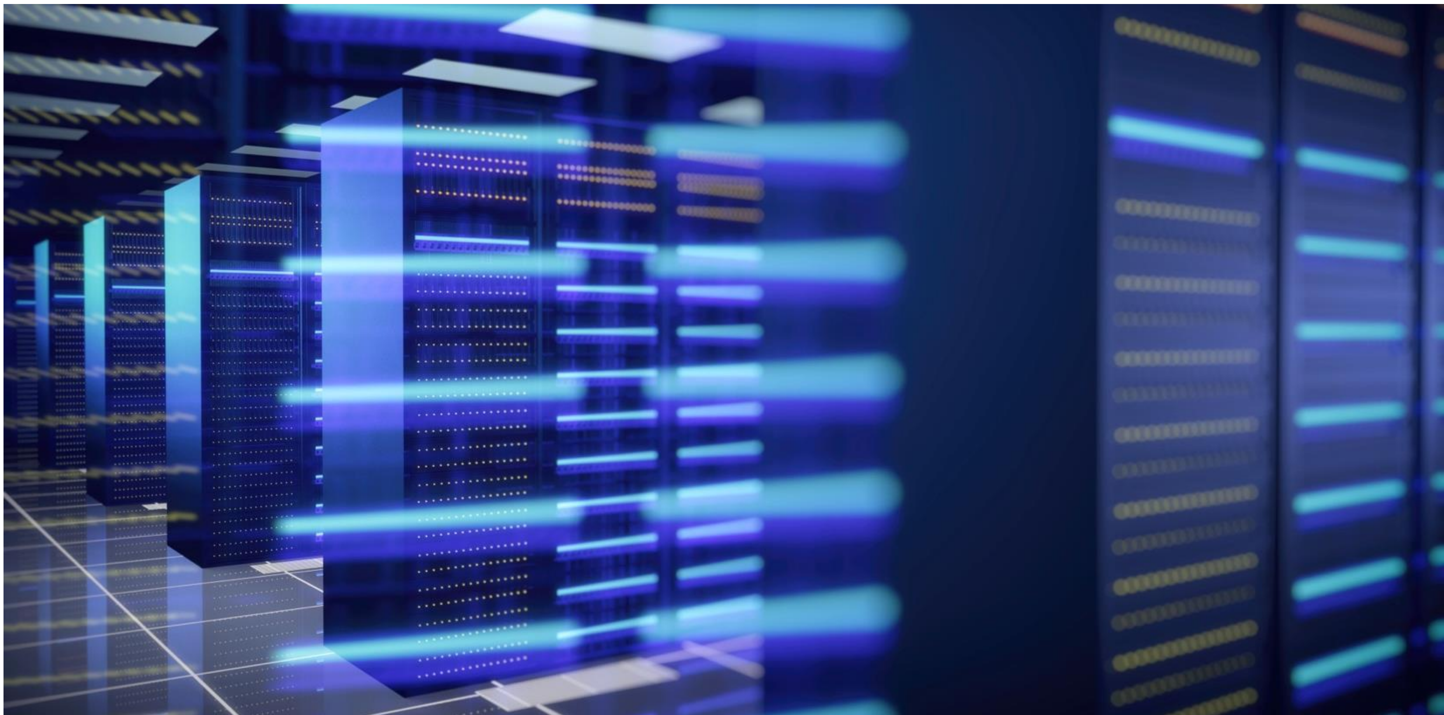
When it comes to managing cybersecurity risk, counsel can serve as true partners to the information security team, integrated with them and even sitting with the Securities Operations Center. Counsel in this capacity may have a function outside of legal role, opining on risk, governance and many of the other issues in this Handbook. Sometimes the model is different, with counsel serving solely as advisers on legal issues. In either model, and those in between, a strong and dynamic partnership between these two roles is key to maintain the entity’s security.

4. Interacting with the Board of Directors

CISOs have been providing cybersecurity briefings to the board for years, or at least to the audit or risk committees. These briefings were helpful for the board to fulfill its obligations to oversee risks to the enterprise, but they were not technically required. In 2017, NYDFS passed Part 500, which included a requirement of board reporting. Even for those not regulated by NYDFS, the wave of regulations upped the ante on what “reasonable security” consists of, and it certainly consists of board updates. Sometimes counsel joins, but even without joining for the briefing, having counsel check compliance with regulatory expectations is critical.

5. Cybersecurity Training and Awareness

Comprehensive cybersecurity training and awareness is a key pillar of any effective cybersecurity program. Particularly as workplaces continue to employ hybrid and remote work models, counsel should consider how best to ensure that all employees understand and follow the company’s cybersecurity protocols. Companies may benefit from providing role-based security awareness training that is tailored for employees or affiliated persons in particular roles, such as members of technical teams, incident response teams, persons who wire money, executive management and board members. Typically, CISOs and privacy counsel are in charge of developing cybersecurity trainings for employees; but counsel can collaborate with these stakeholders to develop cybersecurity trainings for employees to ensure they meet applicable legal requirements.



6. Data Minimization and Hygiene

Data is vital for businesses and also a source of risk. Various cybersecurity and privacy laws now require companies to dispose of certain categories of data when no longer needed for a legitimate business purpose. To help the company comply with these obligations, and otherwise mitigate risk, counsel should take steps to understand (i) what types of data the company collects, processes, or retains, (ii) for what purpose the company is collecting that data, (iii) with whom that data is shared, and (iv) the company's retention and data governance policies surrounding that data.

7. Insider Risks

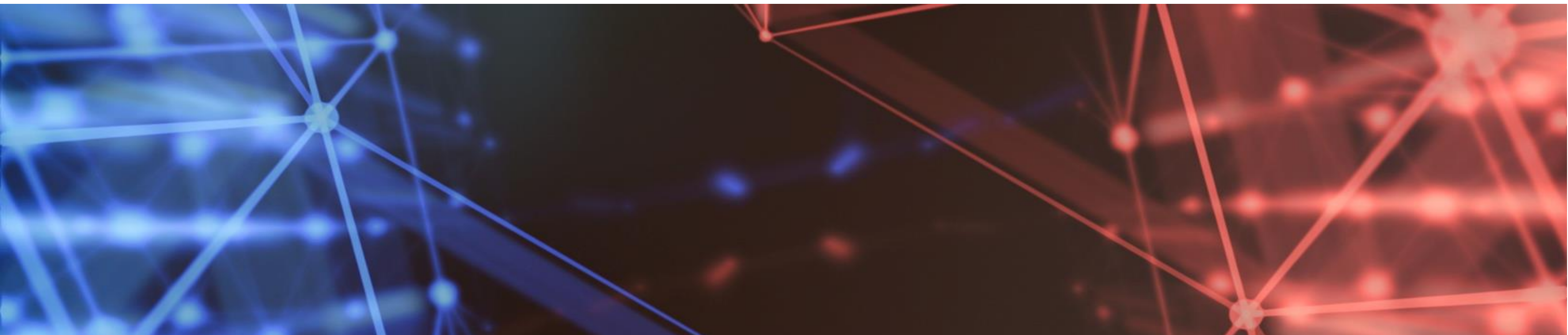
Not all risks originate from external sources. Inhouse Counsel need to be prepared to deal with internal threats that affect critical assets – whether from malicious or unintentional actors.

8. Managing the Relationship Between Privacy & Counsel

Cybersecurity and data privacy are two sides of the same coin. In the broadest possible terms, cybersecurity looks at protecting data from the outside (and inside), whereas data privacy is concerned with what a company does with the personal data. For many companies, the same attorney is counsel for both privacy and cyber. But increasingly, cyber counsel and privacy counsel are different roles. For companies that implement separate roles, it is therefore important for the two roles to closely collaborate.

9. Incident Response: Preparations

It is common (and at times required) for companies to have a suite of policies and procedures in place that will allow them to effectively respond to a range of incident types. Counsel should help prepare incident response plans and participate in tabletop exercises and onboarding of vendors.



10. Incident Response: How to Respond to an Incident

Given the myriad of potential legal and regulatory issues involved, Counsel has an important role to play in cybersecurity incident response ("IR"), although the nature of that role will vary significantly based on the structure of the company and how IR roles are delineated. At a minimum, it can be helpful for Counsel to be aware of the general steps that occur when a breach happens, so they can provide advice and assistance when needed during the overall IR process. The timeline and events described herein are provided for illustrative purposes only, as they will vary significantly company-to-company and incident to incident.

11. Incident Response: Post Incident

After an incident is remediated, contained and systems are restored, the post-incident process begins. Companies may find it useful – and some make it part of their written response plan – to take steps to review and document the incident, and to consider opportunities for improvements to its cybersecurity program and IR policies and procedures.

12. External Engagement: Law Enforcement, Regulators, Trade Groups, Etc.

As a field with rapidly evolving threats, law and regulations, it is critical for counsel to stay abreast of developments. Additionally, understanding how other companies are dealing with the regulations is a critical piece of information to help benchmark. Counsel can assist the company's cybersecurity risk management by facilitating strong external connections between the company and law enforcement, regulators, and trade groups. In other fields (*e.g.*, white collar crime), law enforcement and regulators are often adverse to companies. But for cyber there is a shared purpose, even with most regulators. Building trust and cooperation is key.

13. Cybersecurity Insurance

Cyber insurance can be essential in helping companies deal with the expense of responding to, and recovering from, a cybersecurity incident. Counsel and CISOs should be closely involved with all insurance-related interactions to ensure that the company has suitable policy coverage, and that the coverage is not accidentally invalidated by the company's action when responding to an incident.

14. Bug Bounty / Vulnerability Disclosure

In order to respond to increasingly sophisticated and diverse cyberattack techniques, companies have to take proactive measures to reduce the likelihood of a cybersecurity incident. This may include implementing technical-facing measures such as a bug bounty and vulnerability disclosure program. While they can provide invaluable feedback to companies on the strength of their environment's security, the legal and risk landscape surrounding bug bounty and vulnerability programs can be complex to navigate. Counsel can add value by remaining closely involved in creating and overseeing these programs.

15. Third Party Risk Management

Vendors, service providers, and other third-parties likely play an important role in your company, but these key relationships could also present unique cybersecurity and privacy risks if not managed and monitored diligently. Inhouse Counsel may want to be involved in reviewing and overseeing these relationships to help minimize the risks.

16. Diligence, Corporate Transactions, and Integration

Nearly every transactional deal requires cybersecurity and privacy diligence to understand the key cybersecurity issues faced by the target, including its technical frameworks for identifying, treating, and managing cyber risk. While information security teams are tasked with a review of technical controls, often they are not given hands-on access to assess those controls. Counsel are uniquely positioned to work alongside the InfoSec teams to spot potential issues through the target's reports, regulatory reviews, and other documentation. Counsel can then communicate these concerns to the management team in a clear and non-technical description so they can help evaluate the transaction and address any transition.

17. Other Hot Topics

Cybersecurity is a vast, multifaceted subject area that cannot be condensed into one desk guide. In our final topic we highlight other topics of interest that should be on the radar of counsel including takedowns, lost devices, electronic communications, wire diversions and vulnerability and patch management.