

Cybersecurity & Data Privacy

STRATEGIC THINKING AND PRACTICAL LEGAL ADVICE

5 Considerations for General Counsels Regarding Developing a Cyber Incident Playbook

To facilitate cyber incident response in practice, many organizations are building “cybersecurity playbooks” that provide tailored, practical guidance that enhances organizational readiness. During a cyber incident, easy access to actionable material can be central to an effective response. The content, audience and goals for a playbook may vary. For example, they may contain highly technical materials for IT teams, guides for cross-functional and cross-border management, or primers for executive leadership. Whatever its focus, a playbook, and the process of making one, can help steer incident response procedures in the right direction, save precious time and serve as a reminder to prevent common mistakes that heighten legal and business risks.

We briefly discuss below five things that general counsels should consider when developing a cyber incident playbook.

Enhancing Organizational Readiness in Light of Evolving Threats. Cybercrime costs the global economy as much as \$3 trillion annually by some estimates, and cyber threats continue to become more sophisticated and severe. A “cybersecurity playbook”, and the process of making one, can enhance cybersecurity preparedness, help steer incident response procedures in the right direction, save precious time and serve as a reminder to prevent common mistakes that heighten legal and business risks.

Tailoring Playbooks to Facilitate

Decision-Making. A company may decide to set up a series of playbooks for different regions and/or departments. Playbooks can be highly technical, but they can also provide guidance to a non-technical audience, including by setting out key factors to facilitate decision-making and addressing governance and incident response procedures.

Preparing a Legal Cybersecurity

Playbook. A playbook for a general counsel’s office, for example, could include a summary of key actions that relevant lawyers should plan to carry out during incident response, such as:

- Providing legal guidance and identifying legal risks;
- Establishing and maintaining attorney-client privilege;
- Analyzing whether contractual obligations are implicated, for example, in a vendor breach or with regard to institutional clients;
- Assisting with information flows—both internally (board of directors, impacted system stakeholders) and externally (law enforcement, regulators, clients/customers and third parties);
- Taking steps in anticipation of litigation;
- Maintaining a record and timeline of the good faith efforts to identify the source and nature of the incident and the steps taken during incident response; and

- Protecting the privacy rights of all clients/customers, employees or other individuals whose data may be implicated.

Balancing Practical, Confidential Guidance with Providing Documentation of Cyber Preparedness. Once a cybersecurity playbook is in place, it can serve as helpful documentation to demonstrate the company’s commitment to reasonable cybersecurity practices. However, some elements of the playbook may benefit from full and frank legal guidance. Further, there is a risk that sharing playbooks with regulators or other third parties may increase scrutiny for potential gaps between stated goals and actual responses. With these factors in mind, organizations should consider what portion of a playbook, if any, they would be willing to share with regulators. Ultimately, it is important to balance how best to maintain practical, confidential guidance while providing useful documentation of cyber preparedness.

Testing and Improving Playbooks through Training and Tabletop Exercises. The *NIST Guide for Cybersecurity Event Recovery* notes that these “exercises help identify gaps that can be addressed before a crisis situation, reducing their business impact.” Such exercises can also help to surface internal process or communications challenges and can improve a company’s response to cyber incidents.

For more information about these topics, please contact any of the following lawyers.

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

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

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world’s leading companies and financial institutions on their most complex deals and disputes. With extensive reach

across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world’s three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our “one-firm” culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit www.mayerbrown.com for comprehensive contact information for all our offices.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the “Mayer Brown Practices”) and non-legal service providers, which provide consultancy services (the “Mayer Brown Consultancies”). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. “Mayer Brown” and the Mayer Brown logo are the trademarks of Mayer Brown.

© 2018 Mayer Brown. All rights reserved.