ALM | LAW.COM

New York Law Journal

Cyber Health Checkup for 2025

By Olivia Greer and Taya Bokert

March 03, 2025

In today's modern digital environment, every business is a possible, and even likely, target of cyberattack – a broad term that encompasses any malicious activity designed to control, disrupt, or destroy an organization's information systems. In our work with clients across industries, we have seen how advance preparation leads to more successful responses when an incident does occur, limiting exposure and liability.

The Legal Landscape of Cybersecurity

Legal standards related to cybersecurity form a varied patchwork across state, federal, and international laws. Some laws and regulations proscribe specific cybersecurity measures, while others impose legal standards that leave room to differ in practice. For example, businesses that are subject to the EU or UK General Data Protection Regulation (GDPR) are required to "implement *appropriate* technical and organisational measures to ensure a level of security appropriate to the risk."

Businesses that are subject to the California Consumer Privacy Act (CCPA), and other comprehensive state privacy laws, are required to "implement *reasonable* security procedures and practices appropriate to the nature of the personal information." Both the GDPR and CCPA

Credit: Vadym/Adobe Stock

leave room for different security approaches to be "appropriate" or "reasonable," depending on the categories of data processed by a business and the level of risk to that data associated with that business's data-related activities.

In the U.S., the cybersecurity landscape is further complicated by the intricacies of industry-specific regulations that impose precise cybersecurity obligations (including preventative measures, as well as required reporting of incidents) on businesses handling sensitive categories of information, such as health information (under HIPAA and related state laws) or financial information pursuant to FTC, SEC and other rulemaking under the Gramm-Leach-Bliley Act.

State agencies also impose cybersecurity obligations, such as the New York State Department of Financial Services cybersecurity regulation. Finally, organizations must navigate fifty separate state breach notification statutes, each of which have distinct procedures a business must follow for notifying impacted state residents in the event of an incident.

With varying legal standards to incorporate, and the number and cost of cyberattacks increasing across the U.S., businesses should regularly take stock of their cybersecurity postures and take proactive steps to establish, and improve upon, their "cyber health." The below cybersecurity practices are critical, regardless of what laws a business is subject to, in order to protect against bad actors, litigation, and regulatory action;

Cyber Health Checklist

- **People and Governance.** From dedicated security professionals to rank-and-file employees, each member of an organization plays a role in preventing, and responding to, cyberattacks. Businesses should clearly delineate the cybersecurity-related duties of each team and/or individual and provide adequate training so that each person can perform their responsibilities properly.
- Importantly, the reporting obligations of all employees in the event of a cyberattack should be established and communicated, as prompt escalation of these incidents to those who will contain and remediate them, as well as analyze them for potential disclosure, is key to incident response and something that regulators will pay attention to. The SEC, for instance, has regularly fined organizations – and even individuals – based on identified failures to maintain appropriate escalation and disclosure protocols.
- In 2021, the SEC imposed fines when senior executives were not notified of a cybersecurity vulnerability identified by the information security team. And in 2023, the SEC took action directly against a CEO who was found to have failed to protect customer data after being alerted to security vulnerabilities two years prior.
- Although the details of implementation will vary depending on the size, structure, and activities of the business, all businesses should have dedicated security personnel, a management readiness team and/or steering committee, and cybersecurity responsibility and oversight at the Board level. Businesses should also incorporate annual security awareness training for all personnel and implement periodic testing of the security of the organization's operations.
- **Third-Party Support.** According to IBM's 2024 *Cost of a Data Breach Report*, the average cost of a cyberattack is nearly $4.9 million. A good cyber insurance policy is typically a critical factor in a business's ability to address and absorb losses associated with an incident.
- General commercial insurance policies may not cover cyber incidents (as in 2011, when a company's commercial insurance would not cover losses associated with a significant data breach), so businesses should factor a stand-alone cyber policy into their insurance packages.
- A significant cost that should be primarily covered by insurance is fees associated with outside legal and technical advisors. Ideally, outside advisors should be vetted and engaged ahead of a cyberattack, in order to get to know the business and key contacts, which leads to significant efficiencies in assisting with a response when an incident does occur. Technical advisors, such as cyber

forensics experts, will help contain the incident and evaluate its impact, as well as make recommendations for remediation.

- Legal counsel will advise on reporting obligations, contractual requirements, communications and overall strategy, and interface with third parties like customers or vendors. IT support technicians, whether they are a part of an in-house team, or are outside advisors (and, ideally, both), should be utilized at least annually, regardless of whether a cyberattack has occurred, to conduct security auditing and testing for the business to identify and address security vulnerabilities preventatively.
- **Internal Controls.** Written cybersecurity policies and procedures, such as an information security policy, an incident response plan, and a business continuity policy, are legal requirements for entities in regulated industries, as well as under certain state laws. State and federal regulators have regularly imposed fines for business's failures to adopt and implement documentation in compliance with various laws and regulations.
- But—importantly—even if written policies and procedures are not legally required for a business, they should still be adopted, because they are imperative to establishing clear guidelines and mitigating the risk associated with an incident. A business's internal processes should also include, at a minimum, technical access controls, such as endpoint security software, anti-phishing email filters, and multi-factor authentication.
- In addition, businesses should establish procedures to track cybersecurity obligations in contracts with customers and other third parties, as well as to effectively oversee third-party providers of services to the business (which is a requirement of certain cybersecurity regulations and has also been the basis of enforcement actions). The effectiveness of a business' overall information security program should be audited and reviewed at least annually.
- **Public Statements.** Businesses are often required to make public statements regarding privacy and cybersecurity, and must vet all public statements with vigilance.
- Businesses of all kinds must disclose how they collect, use, share and protect personal information in their privacy policies; public companies have detailed cybersecurity-related disclosure obligations; and other regulated organizations are subject to varied disclosure and reporting requirements. Any perceived lack of transparency or misleading messaging in these public statements can draw scrutiny and enforcement from regulators.

Cyberattacks can be costly, reputation-impacting events, but advance preparation and regular "cyber health" checks can materially enhance an organization's ability to mitigate the impact of an incident.

Olivia Greer *is a partner in Weil's Technology & IP Transactions practice and Head of U.S. Privacy and Cybersecurity, as well as a co-lead of the Firm's AI Task Force.* **Taya Bokert** *is an associate in Weil's Technology & IP Transactions practice and is based in New York.*