THE NATIONAL LAW JOURNAL
APRIL 18, 2016
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

Cybersecurity Compliance Just Got Tougher

Companies need specific, well-executed plans to meet growing demands of federal and state agencies.

BY NICK AKERMAN AND DAN GOLDBERGER

KIRILL_SAVENKO/ISTOCKPHOTO.COM

While cybersecurity risks have increased, government regulation has traditionally lagged behind. Recently, some government entities have tried to catch up by mandating that companies take a proactive approach toward protecting personal and competitively sensitive data. The move is a departure from the traditional reactive response of simply notifying consumers after their personal data is breached.

With this shift in emphasis, companies are asking the obvious questions: "What are we expected to do and what is a proactive cybersecurity compliance program?"

Both on the state level and through federal regulatory agencies, the government is beginning to dictate a comprehensive compliance approach to data protection. Late last year, the U.S. Securities and Exchange Commission's Cybersecurity Examination Initiative directed broker-dealers to "further assess cybersecurity preparedness in the securities industry." Thus, the SEC announced that it "will focus on key topics including governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response."

In January, the Financial Industry Regulator Authority announced that in reviewing a securities firm's approaches to cybersecurity risk management its examinations may include "governance, risk assessment, technical controls, incident response, vendor management, data loss prevention and staff training." On the state level, Massachusetts is the only state thus far to require all businesses that store personal data of its residents to secure that data through a compliance program modeled after the federal sentencing guidelines.

The framework under the federal sentencing guidelines is the gold standard for an effective compliance program. Having expanded well beyond its original goal of detecting and preventing criminal activities, it is fast becoming the corporate framework to protect data. These guidelines establish seven steps for companies to follow: first, promulgate standards and procedures; second, establish high-level corporate oversight including the board of directors that

must provide adequate funding of the program in proportion to the size of the company and the risk; third, place responsibility with individuals who do not pose a risk for unethical behavior; fourth, communicate the program to the entire workforce; fifth, conduct periodic audits of the effectiveness of the program; sixth consistently enforce the polices; seventh establish mechanisms for reporting violations.

COLLABORATION IS CRITICAL

Because a compliance program must be tailored to an organization's culture, it is critical to its success that all data-protection stakeholders collaborate in its creation and daily operation. This means that data compliance is not just an issue for information-technology security. Other stakeholders include human resources and legal, which are responsible for company rules, employee agreements and training, and may assist in responding to company data breaches; risk management, which may determine, along with legal, the adequacy of the company's cyber insurance; and compliance, which is often the logical focus of the company's data protection efforts.

Stakeholders in turn should focus on six areas of risk when developing a company-specific compliance program to minimize the risks posed by each area.

First, hiring is the time to explain to new employees the rules in place to protect the company's data. Additionally, companies must approach hiring defensively, ensuring new employees do not bring into the workplace data that belongs to a competitor that can result in civil or criminal liability.

Second, company rules and policies should spell out what employees can and cannot do with the company network and form the foundation of top-to-bottom workforce training. At least one court has recognized that such "explicit policies are nothing but security measures employers may implement to prevent individuals from doing things in an improper manner on the employer's computer systems." (*American Furukawa v. Hossain*).

Third, agreements with employees and other third parties are a key component of data protection. Employee agreements are an opportunity to reinforce the lack of an expectation of privacy in using company computers and define the scope of authorized access. When company data is outsourced to a cloud provider, agreements formalize the responsibilities of that third party to protect the company's data.

Fourth, technology can be employed not only to secure data but to define who is authorized to access what portion of the network and provide admissible evidence of a breach. Information-technology security, working with legal, can prepare mechanisms to capture audit trails in the network that can be used to identify the source and scope of a breach.

Fifth, effective termination procedures are critical. This is when insiders are most likely to steal company data to use at their next job. This is also the last opportunity to remind departing employees of their postemployment obligations to maintain the secrecy of company data, to return all company data and for the company to inventory the data returned.

Finally, if a breach occurs, it is important to have protocols in place to quickly determine the scope of the breach and the appropriate response. Companies must therefore have in place an overarching plan to investigate suspected breaches and to mobilize internal and external resources.

For a data-compliance program to work consistently, it must be a collaborative effort among all stakeholders and comprehensively focus on mitigating the risks to the company's data from multiple and unexpected sources.


NICK AKERMAN *and* **DAN GOLDBERGER** *are partners in the New York office of Dorsey & Whitney. Akerman's practice focuses on the Computer Fraud and Abuse Act and the Racketeer Influenced and Corrupt Organizations Act. Goldberger's practice focuses on financial services, intellectual property, trade secrets and data protection.*