SpencerFane®

Cyber-attacks – A Universal Issue

AUGUST 31, 2017| PUBLICATIONS

The Federal Bureau of Investigation ("FBI") has cautioned organizations, regardless of industry, that cyber-attacks continue to increase and evolve. Cyber-attacks often target digital files containing sensitive and proprietary data. Thus, the operational, financial and reputational impact caused by cyber-attacks to an organization, either directly or through its service providers, can be significant.

While experts acknowledge that it is not possible to anticipate and stop every cyber-attack, organizations need to design their cybersecurity programs to prepare for and respond to these attacks. By doing so, organizations position themselves to protect the organization and their clients against the next cybersecurity attack or data breach.

To illustrate the widespread acknowledgement across industries of the importance of cybersecurity, this article describes: 1) best practices identified by the Securities and Exchange Commission Office of Compliance Inspections and Examinations ("OCIE") for *designing* cybersecurity programs, and 2) guidance issued by the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") under the Health Insurance Portability and Accountability Act ("HIPAA") for *responding* to cyber-attacks.

Cybersecurity Design

In April 2014, the OCIE announced its Cybersecurity Initiative to assess cybersecurity preparedness in the securities industry. The OCIE issued a Risk Alert on May 17, 2017 that identified specific practices that broker-dealers, investment advisers and investment companies should consider when designing their cybersecurity programs. These practices are:

- Cyber-risk Assessment: Conduct periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences.
- Penetration Tests: Conduct penetration tests and vulnerability scans on critical systems of the organization.
- System Maintenance: Implement procedures for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities.

In addition to designing an effective cybersecurity program, organizations need to be ready to respond to a cyber-attack when it occurs.

Cybersecurity Response

HHS has posted educational material on its website regarding cybersecurity. Specifically, the website includes a checklist for HIPAA covered entities (health care providers and health plans) and their business associates on how to respond to cyber-attacks. Suggested responses by an organization to a cyber-attack include:

- Execute Plan: Immediately respond to a cyber-attack by implementing the organization's cybersecurity program to address any access or system issues and to mitigate any impermissible disclosures of protected data.
- Report Incident: Report the cyber-attack to appropriate law enforcement agencies. Such agencies may include state or local law enforcement, the FBI, and/or the Secret Service. In addition, an organization should report the incident to federal and information-sharing and analysis organizations, including the Department of Homeland Security.
- Report Breach: An organization must report a data breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals. An organization must also notify affected individuals and the media, unless law enforcement requests a delay in the reporting.

While the details associated with designing a cybersecurity program or responding to an attack may vary depending

AUTHORS

- Beth Miller

RELATED PRACTICES

- Employee Benefits

BLOG TOPICS

- Benefits in Brief
  - HIPAA Privacy and Security
  - Investment Adviser

on the specific industry and type of data, the fundamentals of any organization's program – assess, test, maintain, execute and report – are universal. To mitigate the significant impacts of cyber-attacks, organizations should carefully review their cybersecurity programs, as well as their service providers' programs, to assess preparedness and response in connection with cyber-attacks and data breaches.

This blog post was drafted by Beth Miller, an attorney in the Spencer Fane LLP Overland Park, KS office. For more information, visit spencerfane.com.