STRATEGIC MANAGEMENT SERVICES

Phishing Attacks Remain A Serious Compliance Threat

Richard P. Kusserow | **May 27, 2021**

Key Points:

- **Data breaches are on the rise.**
- **Tips for compliance officers to counter information security threats are included below.**

In 2020, data breaches involving 500 or more records were reported to the Department of Health and Human Services Office for Civil Rights (OCR) at a rate of more than 1.76 per day. An article published earlier this year indicates that health care providers, payors, clearinghouses, and business associates cumulatively reported 642 large data breaches. Notably, the number of reports increased by 25 percent from 2019. Because the frequency of data breaches appears to be increasing, organizations need to reinforce messaging and prevention efforts. Employees are the single greatest risk factor; one employee who lets their guard down provides a sufficient opportunity for attackers to access data.

According to information from the Society for Corporate Compliance and Ethics (SCCE) and the Health Care Compliance Association (HCCA), phishing attacks continue to be one of the most serious cybersecurity threats. They occur when attackers attempt to obtain sensitive information such as usernames, passwords, or credit card details by impersonating trustworthy entities in digital communications. The data stolen in such attacks may result in breaches of protected health information. The methods used in phishing attacks include: (A) Embedding a link that routes the user to a fictitious website that requests login credentials; (B) Spoofing an email address to appear as a reputable entity; (C) Including an email attachment with malware that can exploit system loopholes; and (D) Impersonating a company vendor or information technology department in telephone calls or text messages.

Implementing an effective security program to educate employees about phishing and other tactics used by cyber criminals is critical. Such programs should emphasize the following:

- The serious security, financial, and reputational risks phishing attacks represent;
- How to identify phishing emails through examination of the sender address, links, language, etc.;
- The need to be cautious of pop-up windows;
- A prohibition on providing sensitive information via email or telephone;
- The risks of opening attachments or clicking on links from unfamiliar sources;
- The importance of creating sound passwords and updating them periodically;
- Methods to report suspicious messages quickly and easily; and
- Mock phishing tests to reinforce the training messages.

For more information on this topic, contact Richard Kusserow at rkusserow@strategicm.com.