Claire Rosston

Partner
208.383.3960
Boise
ccrosston@hollandhart.com

Despite Increased Awareness and Employee Training, Ransomware Is Still the Healthcare Industry's No. 1 Threat

Employee Training Can Prevent Attacks and Punishing Employees for HIPAA Violations Can Prevent Penalties

Insight — 05/09/2019

Ransomware accounted for more than 1 in 10 healthcare data breaches reported to the government during the last three years, according to analysis by Bloomberg Law. Cybercriminals capitalize on lack of employee training by sending emails with malicious attachments to gain access to healthcare providers' and business partners' networks. With this access, the ransomware typically encrypts all of the data within the organization's network that cannot be recovered until the ransom is paid for the decryption key.

Guidance from the HHS Office of Civil Rights (“OCR”) makes it clear that a ransomware attack usually results in a breach under the Health Insurance Portability and Accountability Act (“HIPAA”) that requires compliance with costly notification rules.

Training employees to be highly suspicious of attachments and unknown hyperlinks is key to preventing these phishing attacks. Employers should educate employees on how to spot emails that attempt to masquerade as legitimate emails from co-workers and business contacts but often contain a number of these tells:

1. The email address is not associated with the business's website (e.g., “hollandhart@online.com” rather than “webalert@hollandhart.com”).
2. The email is sent with high importance.
3. The link in the email isn't actually a real URL. Place your pointer over the link—without clicking!—and compare the URL in the pop-up window to the link. If they don't match, don't click.
4. The email contains criminally bad spelling and punctuation errors.

Punishing employees who violate HIPAA can decrease the possibility of OCR imposing a penalty, according to Bloomberg Law's research. Nearly 1 in 6 of the breaches in 2016 and 2017 reported to OCR did not result in a penalty or resolution agreement because the organization had already punished employees for HIPAA violations.

For more information about how to respond to a ransomware attack in

compliance with OCR's guidance on ransomware, visit this article.

For questions regarding this update, please contact:
Claire Rosston
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: ccrosston@hollandhart.com, phone: 208.383.3960
