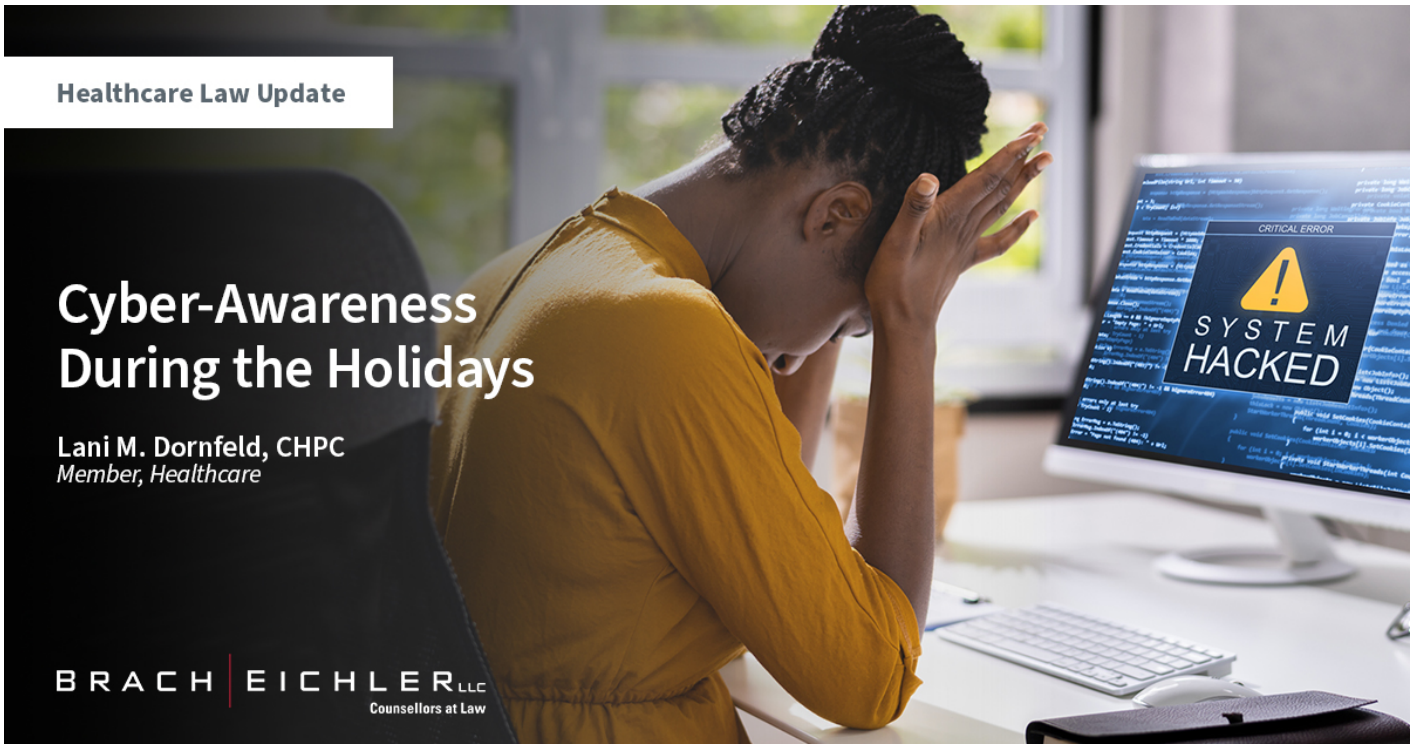
Cyber-Awareness During the Holidays



A global study performed by Cybereason indicates that cyber attackers don't take time off and are increasingly targeting weekends and holidays for ransomware attacks, when fewer people are around to detect or respond to attacks. Resultingly, the research indicates that the victim organizations:

- Took longer to assemble a response team
- Took longer to stop the attack
- Took longer to recover from the attack
- Lost more money
- Took longer to assess the scope of the attack.

As part of the study, Cybereason asked organizations what steps they are taking to address the heightened ransomware threat. Responses included that organizations are planning to implement new detection capabilities specifically for ransomware that have better detection efficacy (38%), are augmenting staff so they can respond faster (31%), are pursuing automation to accelerate attack detection and response (29%), are learning to negotiate with ransomware actors (27%), and are setting up cryto wallets in the event they decide to pay (27%).

The bottom line: targeted victim organizations are more vulnerable to cyber attacks during off-hours, including weekends and holidays. Cybereason recommends that organizations:

- Explore different staffing models for security operations center analysts and incident responders—look to hospital emergency rooms or other emergency response organizations for models.

- Identify optimal staffing for weekends and holidays— what's the least amount of coverage you can get away

The bottom line: targeted victim organizations are more vulnerable to cyber attacks during off-hours

Took longer to assemble a response team with and still reduce risk?

• Pursue a managed detection and response (MOR) strategy—augment existing staff with expert, third party 24/7/365 coverage.

• Lock down privileged accounts during off-peak hours— highest privilege accounts are rarely used on weekends and holidays.

• Implement clear isolation practices—to prevent attackers from making any further ingress on the network and from spreading the ransomware to other devices.

• Replace traditional antivirus products with next generation antivirus and endpoint detection and response solutions—look specifically for behavior-based tools capable of identifying ransomware attacks in their earliest stages, based on suspicious behaviors the tools are seeing across the organization's network.

Click here to read the entire November 2022 Healthcare Law Update

For more information or if you need assistance with your HIPAA compliance program, please contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com