"STOP. THINK. CONNECT.": Using Your Personnel To Enhance Your Cybersecurity.

Insights
4.05.16

In February 2016, President Barack Obama directed his Administration to implement a Cybersecurity National Action Plan (CNAP) that "takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security." (Fact Sheet: Cybersecurity National Action Plan, 2/9/2016) As part of that plan, the President highlighted the STOP. THINK. CONNECT. campaign, a global cybersecurity awareness campaign appealing for individuals to play a more significant role in Internet and network security.

While most companies focus on hardware, software and other technological measures to protect private company, employee and customer data, they often overlook their most valuable asset – people. In this case, "people" includes not just IT personnel but all employees – i.e., anyone who manages or has access to a network. It's everyone's responsibility to protect company and agency data. This is the message of the Stop. Think. Connect. initiative, which provides individuals with valuable information and guidance for the protection of data. Companies wishing to effectively protect their data should remember that it is the people who manage and use their network systems that will make the difference. With this in mind, here are some tips in how to enhance your cybersecurity with a particular emphasis on the effective use of personnel:

- Create a cybersecurity plan that addresses the specific security guidelines for the entire company—e.g., what removable external devices may be used and how; what steps to take in the event of a breach; etc.
- Educate all personnel on the cybersecurity plan so they know the importance of security and the role they play in protecting data.
- Conduct periodic cybersecurity audits to ensure all personnel are following the proper procedures.
- Provide your IT team with the tools (hardware and software) to identify and thwart potential cyberattacks/data breaches.
- Have your IT team periodically practice how to respond to a cybersecurity breach (similar to a fire drill).

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.

- Immediately correct any security risks identified through cybersecurity audits/drills, and train personnel on these issues and solutions.

Remember that cybersecurity is a responsibility shared by everyone in the workplace and any effective cybersecurity system and plan must address this simple fact.

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.