TOP 10 MOST OVERLOOKED CYBERSECURITY RISKS

Unpacking the greatest threats to the public sector in 2017

1 BYOD

As more government employees use their personal devices for work and become increasingly mobile, vulnerabilities arise when these devices are not under centralized enterprise control.

2 Outdated Policies

Government policies may go years without major revisions or updates, which can create gaps and unforeseen liabilities as new technologies continue to challenge existing operating structures and methods.

3 Print Environment

An often-ignored, vulnerable area of cybersecurity is the print environment. A recent Center for Digital Government survey found agencies are aware their print environment is just as vulnerable to threats as other endpoints, but they face challenges in securing it.

4 Legacy Equipment

Many Internet-connected legacy machines no longer receive security updates from their manufacturers and can be easily compromised as a gateway into a network.

5 Social Engineering

Social, or human, engineering is another overlooked attack that is accomplished by someone manipulating a government employee to divulge information. Training employees on how to respond to these situations is important.

6 Third-Party Software

Many government employees prefer to use their own third-party tools, but if they are not built with security features, they can become a back door into secure networks for malicious software.

7 Remote Workers

Remote employees are commonplace within agencies across the country, but how and where employees access government systems can create significant liability.

8 Outdated Training

Every new government employee goes through some form of training during the onboarding process, but without having a regular security training program in place, employees are ill-equipped to identify and address the latest cybersecurity threats.

9 Vendor Management

Government agencies interact with countless vendors, but many do not have a robust vendor management strategy in place. Without one, outside vendors may continue to have access to systems or facilities they no longer service, creating a threat to data security.

10 Public Wi-Fi

Although convenient, public Wi-Fi must be properly separated from secure networks to prevent unauthorized access to secure documents or devices.