concluded government computers, and those of contractors that work for the government, face "an evolving array of cyber-based threats."

Sep. 10, 2015

Retail giants aren't the only target of hackers who infiltrate computer systems to gain access to sensitive information.

The federal government also falls victim, such as recently when the Obama administration revealed that 21.5 million people were affected by a breach at the Office of Personnel Management.

Social Security numbers and other records were stolen, and likely anyone given a government background check in the last 15 years was affected.

That's disturbing, both because it happened and because of the ease with which the hackers were able to circumvent government security measures, says cybersecurity expert Michael J. Daugherty.

"The government is quick to criticize security breaches and weaknesses in the private sector, but isn't able to shore up its own weaknesses," says Daugherty, author of the book "The Devil Inside the Beltway: The Shocking Expose of the U.S. Government's Surveillance and Overreach into Cybersecurity, Medicine and Small Business" (www.michaeljdaugherty.com).

The U.S. Government Accountability Office conducted a review this year that concluded government computers, and those of contractors that work for the government, face "an evolving array of cyber-based threats."

"These threats can be unintentional – for example, from equipment failure, careless or poorly trained employees – or intentional," the GAO report said.

Those intentional threats include targeted or untargeted attacks from criminals,

"You would think the federal government would have better safeguards, but ultimately they are only as strong as their weakest employee," says Daugherty, who has spoken at cybersecurity gatherings. "That boils down to knowledge and training."

Daugherty says security risks are one reason there are concerns about Hillary Clinton using a private server for her email when she was secretary of state.

"The potential for sensitive emails to be lost is the issue," he says. "Whether they actually were or were not lost is not the issue, so Hillary's email headache isn't going away anytime soon."

He suggests tips that both government agencies and private businesses need to remember to defend against hackers:

- **Anyone can be a target.** Individual employees may think hackers target the system and that they have nothing to worry about, but that's not the case, Daugherty says. Hackers often gain entry to a system by targeting the individuals who use that system. Employees both in government and the private sector need to be aware of that they are an important line of defense and should be cautious about opening strange emails and attachments.

- **Education is critical.** Government agencies and private businesses should not rely on their employees to figure out cybersecurity concerns and safeguards on their own. Training employees can go a long way toward helping to reduce the chances of a breach.

- **Reminders never hurt.** Even employees educated about the threats can slip up because being on the lookout for potential cyber breaches is just one in a long list of their responsibilities. Routine reminders – whether through an email, at staff meetings or in a newsletter or memo – can help keep employees on their toes.

“Cybersecurity handled poorly costs jobs, safety and billions of dollars,” Daugherty

FCC. That’s not who should play this game. This is really a national security issue and falls under the role of the military.”

———————-

Michael J Daugherty is Founder, President & CEO of LabMD, a cancer detection laboratory based in Atlanta, Georgia, as well as the author of the book “The Devil Inside the Beltway, The Shocking Expose of the US Government’s Surveillance and Overreach into Cybersecurity, Medicine and Small Business.” The book details Daugherty’s battle with the Federal Trade Commission over its investigation into LabMD’s data security practices. It is an insider’s look at how agencies exploit the Administrative Procedure Act to grab for power by exploiting the small and weak to control the big and powerful.

Because of his work, Daugherty has testified before the House of Representatives House Oversight Committee and regularly keynotes in front of healthcare, law, business and technology audience educating them on what to expect when the Federal Government investigates you. He spoke at the Gartner Security Summit in Washington, D.C., in June and in August will speak at a Black Hat USA security gathering in Las Vegas. He holds a BA in Economics from University of Michigan-Ann Arbor, regularly blogs at www.michaeljdaugherty.com and sits on the board of Snoopwall, a privacy company based in Nashua, N.H. He is also a pilot and resides in Atlanta, Ga.

Security • Small Business • Technology

Sponsors.