security firm SpiderOak. The company warns that the increased risk is driven by both state-sponsored and individual bad actors.

Dec. 05, 2017

The coming year will see a massive escalation of cybersecurity risk, according to technology security firm SpiderOak. The company warns that the increased risk is driven by both state-sponsored and individual bad actors.

"As organizations and individuals become increasingly reliant on IoT for critical functions, the risks that we are taking are becoming greater and greater," says Christopher Skinner, CEO of SpiderOak. "Attack surfaces are exploding – the nearly four billion people online worldwide means four billion different entry points for criminals. We trust our devices and systems to drive our cars, deliver vital medical treatments, and protect our homes and supply chains, but these have never been more insecure."

The following are 10 threats and trends that Skinner says organizations need to look out for across business, governmental, and personal arenas:

1. **Software updates – the new Trojan Horse.** When your company pushes out a software update to clients, how do you know that update is real? Criminals are using the normal software update process to get companies to infect all of their clients, which then affects everyone down their software supply chain. In fall of 2017, the popular CCleaner application – designed to optimize software performance on computers – was breached by hackers who installed a backdoor in the software, affecting more than 2 million users. "This is the kind of breach that destroys trust between users and software providers," says Skinner, "and makes consumers want to avoid doing business with the provider in the future."

2. **Installing spies on your phone.** When Russia wanted intelligence on NATO

Equifax breach affecting 145.5 million people. "Fake tax returns will likely explode this year given all the Social Security numbers now exposed," says Skinner. While Chinese hackers remain the prime suspects in the Equifax case, taxes are a favorite target of another state: Russia. On the eve of this year's Constitution Day in the Ukraine – during which the country celebrates its independence from the Soviet Union – accountants in the former SSR were hit with a massive cyberattack, the largest in Ukraine's history. The virus infected the software that businesses are required to use to file tax returns, causing havoc for both the companies and the governmental computers to which they are connected.

4. **One hack, many votes.** "If you can plug it in, you can hack it, and this puts the 2018 elections at risk," says Skinner. "The move to prevent election meddling is far behind where it needs to be, and there are vulnerabilities everywhere from the storage of voter rolls to easily hackable electronic voting machines." Twenty-one states' voting systems were targeted by Russian hackers in the 2016 election cycle, but, he says, "this process starts far ahead of the election itself – it's happening now."
5. **PsyOps on your Facebook feed.** Congressional testimony from Facebook, Google, and Twitter in November revealed the extent of Russia's influence campaign on social media during the last presidential election cycle. More than 126 million of its users were served Russian propaganda, Facebook finally admitted, after months of downplaying the extent of the threat. "The volume of fake news stories was clearly too large for the companies to handle, even with the extensive use of third-party contractors hired specifically to address this threat," says Skinner. "If even tech companies with huge resources are having trouble controlling the spread of fake news and accounts, most other technology and media companies will be even more at risk."
6. **Criminals are patient.** "One of the most frightening things about the breaches at Equifax, Target, and elsewhere is what we haven't seen – yet," warns Skinner. Once

criminals have stolen the data they need – including Social Security numbers,

billion Yahoo accounts and passwords being hacked reflects the catastrophic implications of a breach, and companies are realizing that passwords alone aren't going to cut it. There has to be a one-two punch of both authentication and encryption to secure your data."

8. **Compliance gets your security up-to-date – about 10 years too late.** "The problem with regulations is that they address what's gone before – not thinking about what's to come," says Skinner. "Hackers are forward thinking and creative, staying far ahead of current security protocols. All it takes is one employee who isn't trained in how to safeguard his or her computer and log-ins. The smart hacker takes advantage of this weak link, enters through that employee's credentials, and then has access to your whole system. Checking the boxes on compliance doesn't begin to secure systems and data the way they need to be."
9. **Too many people have the master key.** "Imagine if a landlord gave a master key to all apartments to every single resident in the building – that's how most companies' systems are structured," says Skinner. "When one computer or set of credentials is breached, you have now opened the door to the whole system. In the vast majority of companies, employees have far too much access to information that they don't even need. And given the interconnected systems companies have with their vendors, and then their vendors' vendors, they don't even know how far out their connected system stretches. This opens companies up to so many risks that they don't even know about."
0. **Breach fatigue.** "A real problem with all the bad news we see about hacks and leaks and breaches is that we're becoming desensitized to them," Skinner says. "It's easy for employees to get complacent, and the consequences of this can be extremely harmful to a business. Even upper management can deprioritize security when trying to get out a release or an update before an important sales deadline, and CEOs and boards need to make sure that no corners are cut that can put the

company at greater risk. Ultimately, cybersecurity is going to be only as strong as

(NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.