Jagler: 10 ideas to enhance cybersecurity

Steve Jagler , **Milwaukee Journal Sentinel**   1:00 p.m. CT Jan. 14, 2017

(Photo: Steve Jagler / Milwaukee Journal Sentinel)

The 2016 presidential election was historic in numerous ways, aside from the upset victory by Donald Trump.

It was the first election in which the emails of the Democratic National Committee were hacked and released to the public. It also was the first election influenced by "fake news" promoted through social media.

The threats to cybersecurity are a national crisis, according to Jim Savage, president of Brookfield-based IT consulting firm Concurrency Inc. They're also a personal crisis for consumers and businesses of all sizes, Savage says.

"Nothing is going to surprise me anymore from a security standpoint. There are inherent vulnerabilities," Savage said. "That it took down an election — that is the most significant hack to date. We should definitely be scared. You need end-point security on every device."

Savage noted that a recent survey of more than 600 corporate board directors reported that only 19% believe their boards have a high level of understanding of cybersecurity risks.

Savage can speak from personal experience. Concurrency was nearly the victim of a "spearfishing" scam, in which a hacker determined the email addresses of Savage and a key assistant. The hacker then sent the assistant an email that appeared to be from Savage, directing the assistant to send $45,000 in a wire deposit to an overseas account.

Fortunately, the assistant double-checked with Savage about the expense, and they were able to stop payment on the deposit before it was cashed.

"Our company wired out $45k per a carefully crafted and addressed criminal email request, but fortunately caught it before the perpetrator withdrew funds from the destination bank," Savage said.

I asked Savage to provide 10 practical considerations business leaders should consider to minimize their vulnerabilities to cyberthreats and protect their customers' data.

1. **Acknowledge the threats are real.** "Cybersecurity is a real and pervasive threat that needs to be addressed by any business that wishes to take advantage of the benefits of the global internet. To quote from FBI Director James Comey, 'There are two kinds of big companies in the United States: those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.'"
2. **Avoid the fear paralysis reflex.** "Organizations and/or responsible individuals within organizations are often afraid of looking too deeply into security because of fear of getting blamed for what they expect to find and uncertainty about what to do."
3. **Designate an information security leader.** "A responsible individual identified within the organization needs to be given the responsibility, authority and resources to effectively and economically address the increasing challenge of information security. To be successful in addressing cybersecurity threats, organizations need an established hierarchy of responsibility starting with a top information security role or function."
4. **Protect your data.** "When allocating resources, consider what is at stake. What if Chinese corporate espionage hackers stole the complete AutoCAD drawings for your key manufacturing product? What if Russian hackers stole all your customer names, addresses and credit numbers? Treat information technology as if you are in a regulated industry, regardless of whether you are or aren't."
5. **Upgrade your operating systems.** "A dirty little secret in IT is much of the inherent insecurity in modern business computing is a function of old operating systems. Organizations running two, three and four major operating system

revision levels behind are putting their organization at undue risk. The increasing pervasiveness of mobile and cloud computing requires that businesses address end-points with the same rigor as their perimeter security."

6. **Leverage third-parties' outsourcing where appropriate.** "Look to experts with long and successful track records of implementing the technologies in question for organizations your size."

7. **Go to the cloud.** "Increasingly, businesses with fewer than 1,000 employees are finding it very difficult to economically beat the information security provided by major market cloud providers. In five years, it will be difficult for on-premises-only businesses to compete effectively with businesses that effectively embrace cloud architectures."

8. **Implement service management.** "IT service management refers to the collection of policies, processes and procedures performed by organizations to plan, design, deliver, operate and control information technology. A maturing, standards-based service management effort is one of the most important things an organization can do to address security in addition to managing the costs and complexity of IT."

9. **Leverage best practices.** "Apply the wisdom of those that have gone before us. From planning through execution, be sure to take advantage of industry standards and established methodologies."

10. **Train employees.** "End user training and employee awareness about cybersecurity must accompany good policy and the right security technology investments…There's a lot of room for humans to do the wrong thing."

Steve Jagler is the business editor of the Milwaukee Journal Sentinel. Send C-Level ideas to him at steve.jagler@journalsentinel.com.

James Savage

President

Concurrency Inc., Brookfield, with offices in Chicago and Minneapolis

Expertise: Microsoft-focused systems integration

Previous experience: Enterprise software, business process automation, enterprise content management, information security, IT service management, project and portfolio management

Education: Bachelor of arts, economics and history, University of Wisconsin-Milwaukee

Best advice ever received: "Do what you love. …The money will come."

Favorite movie: Anything by Guy Ritchie or Wes Anderson

Favorite musical act: Radiohead

Favorite Wisconsin restaurant: Palmer's Steakhouse in Hartland

Personal: "I dropped out of Brookfield East in my sophomore year, took the GED and started college while graduating classmates were high school seniors."

Read or Share this story: http://on.jsonl.in/2ix0E8G