SECURITY

Experts predict 2017's biggest cybersecurity threats

From internal threats to creative ransomware to the industrial Internet of Things, security experts illuminate business cybersecurity threats likely to materialize in the next year.

By Dan Patterson | December 13, 2016, 8:16 AM PST

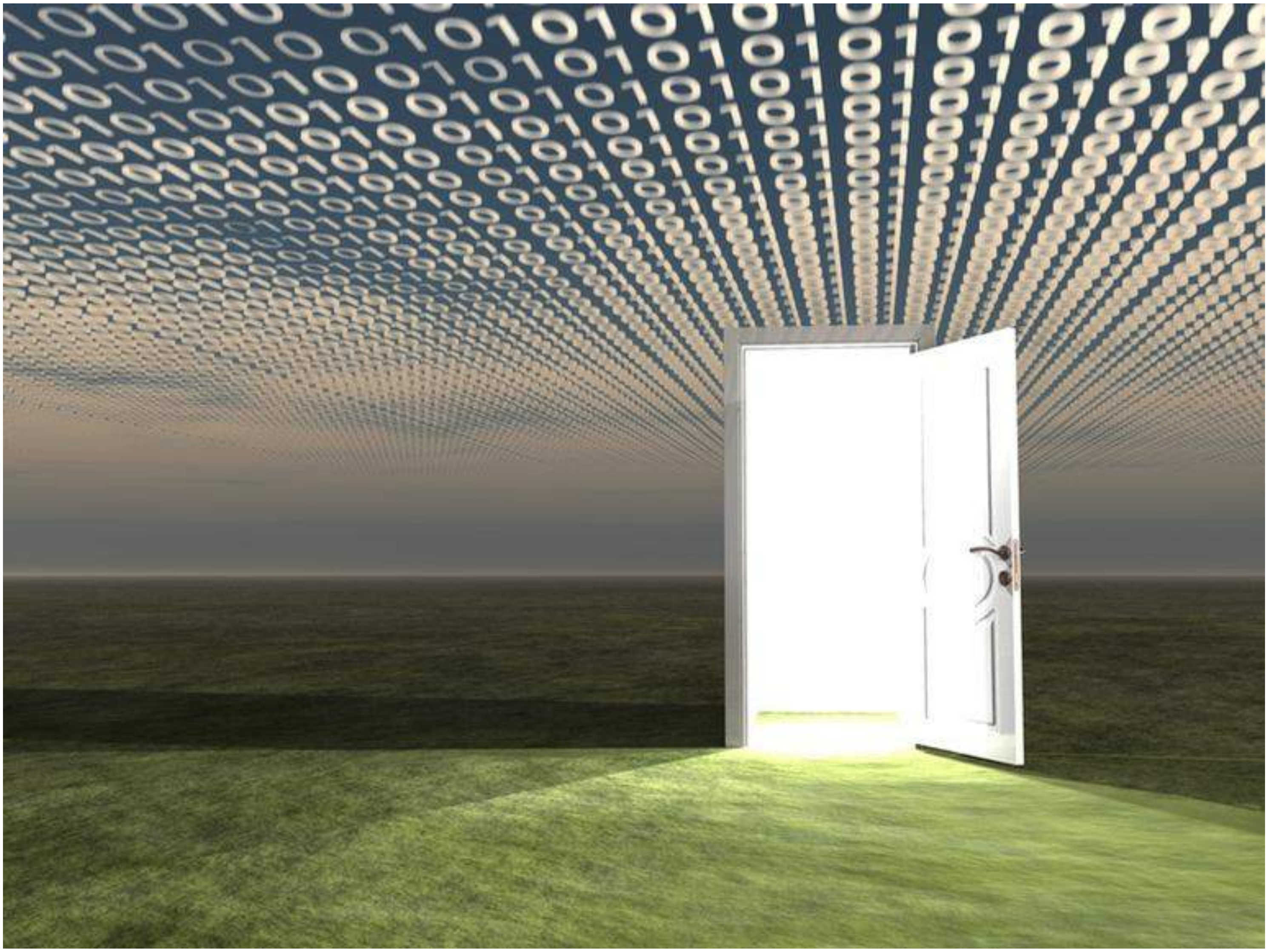


Image: iStock / bestdesigns

If 2016 was the year hacking went mainstream, 2017 will be the year hackers innovate, said Adam Meyer, chief security strategist at SurfWatch Labs. Meyer analyzes large and diverse piles of data to help companies identify emerging cyber-threat trends. "2017 will be the year of increasingly creative [hacks]," he said. In the past, cybersecurity was considered the realm of IT departments, Meyer explained, but no longer. As smart companies systematically integrate security into their systems, the culture hackers too will evolve.

"Cybercriminals follow the money trail," Meyer said, and smart companies should adopt proactive policies. Ransomware attacks grew quickly, he said, because the attacks are "cheap to operate, and many organizations are not yet applying the proper analysis and decision-making to appropriately defend against this threat."

SEE: How risk analytics can help your organization plug security holes (http://www.techproresearch.com/article/how-risk-analytics-can-help-your-organization-plug-security-holes/) (Tech Pro Research)

It's equally cheap to identify internal vulnerability to hacks and to apply preventative best practices (http://www.zdnet.com/article/to-stop-the-hackers-security-teams-need-to-share-more-data-on-attacks/), Meyer said. But for many companies it's not as easy to understand the cybersecurity threats most likely to impact business. To help, TechRepublic spoke with a number of prominent security experts about their predictions for near-future cybersecurity trends likely to impact enterprise and small business in 2017.

Cyber-offense and cyber-defense capacities will increase - Mark Testoni, CEO at SAP's national security arm, NS2

We will see an increased rate of sharing of cyber capabilities between the commercial and government spaces. Commercial threat intelligence capabilities will be adopted more broadly by organizations and corporations... High performance computing (HPC), in conjunction with adaptive machine learning (ML) capabilities, will be an essential part of network flow processing because forensic analysis can't stop an impending attack. HPC + adaptive ML capabilities will be required to implement real-time network event forecasting based on prior network behavior and current network operations... [Companies will] use HPC and adaptive ML to implement real-time behavior and pattern analysis to evaluate all network activity based on individual user roles and responsibilities to identify potential individuals within an organization that exhibit "out of the ordinary" tendencies with respect to their use of corporate data and application access.

Ransomware and extortion will increase - Stephen Gates, chief research intelligence analyst at NSFOCUS

The days of single-target ransomware will soon be a thing of the past. Next-generation ransomware paints a pretty dark picture as the self-propagating worms of the past, such as Conficker, Nimda, and Code Red, will return to prominence—but this time they will carry ransomware payloads capable of infecting hundreds of machines in an incredibly short timespan. We have already seen this start to come to fruition with the recent attack on the San Francisco Municipal Transport Agency, where over 2,000 systems were completely locked with ransomware and likely spread on its own as a self-propagating worm. As cybercriminals become more adept at carrying out these tactics, there is a good chance that these attacks will become more common.

As more devices become internet-enabled and accessible and the security measures in place continue to lag behind, the associated risks are on the rise. Aside from the obvious risks for attacks on consumer IoT devices, there is a growing threat against industrial and municipal IoT as well. As leading manufacturers and grid power producers transition to Industry 4.0, sufficient safeguards are lacking. Not only do these IoT devices run the risk of being used to attack others, but their vulnerabilities leave them open to being used against the industrial organizations operating critical infrastructure themselves. This can lead to theft of intellectual property, collecting competitive intelligence, and even the disruption or destruction of critical infrastructure. Not only is the potential scale of these attacks larger, most of these industrial firms do not have the skills in place to deal with web attacks in real-time, which can cause long-lasting, damaging results. This alone will become one of the greatest threats that countries and corporations need to brace themselves for in 2017 and beyond.

Industrial IoT hacks will increase - Adam Meyer, chief security strategist at SurfWatch Labs

IoT security threats have been talked about, but not really worried about by most because a serious incident had yet to occur. With the 2016 DDoS attack on Dyn, and the ripple effect it created, we

More about IT Security

will see more scrutiny on security within the IoT marketplace. Vendors will work in new security precautions, but at the same time, criminals will also increase their attention on new ways to leverage IoT devices for their own malicious purposes. There are plenty of "As-A- Service" attack capabilities on the Dark Web for hire now and we should expect creative new IoT hack services to pop up in the near future.

Internal threats will increase - James Maude, senior security engineer at Avecto

As organizations adopt more effective strategies to defeat malware, attackers will shift their approach and start to use legitimate credentials and software - think physical insiders, credential theft, man-in-the-app. The increased targeting of social media and personal email bypasses many network defenses, like email scans and URL filters. The most dangerous aspect is how attackers manipulate victims with offers or threats that they would not want to present to an employer, like employment offers or illicit content. Defenders will begin to appreciate that inconsistent user behaviors are the most effective way to differentiate malware and insider threats from safe and acceptable content.

Video: 5 things to know about ethical hacking (http://www.techrepublic.com/article/5-things-to-know-about-ethical-hacking/)

Five ways to maintain your privacy on your smartphone, no downloads required (http://www.techrepublic.com/article/ways-to-maintain-your-privacy-on-your-smartphone-no-downloads-required/)

Firms that force you to change your password are clueless says cyber security chief (http://www.techrepublic.com/article/that-force-you-to-change-your-password-are-clueless-says-cyber-security-chief/)

Subscribe to TechRepublic's Cybersecurity Insider newsletter (http://www.techrepublic.com/newsle

SEE: Threat intelligence: Forewarned is forearmed (http://www.techproresearch.com/article/threat-intelligence-forewarned-is-forearmed/) (Tech Pro Research)

A big part of the challenge with cyberattacks is how businesses think threats can be filtered at the perimeter. Be warned that this is not the case. Attackers are aware of how to directly target users and endpoints using social engineering. The industry needs to be more proactive in thinking about how to reduce the attack surface, as opposed to chasing known threats and detecting millions of unknown threats. With an increasingly mobile workforce and threats coming through both personal and business devices and services, the impact of perimeter defenses has decreased. Security needs to be built from the endpoint outwards.

Business security spending will increase - Ed Solis, Director of Strategy & Business Development at CommScope

Security is part of every business and IT discussion these days and it will only become more intense in 2017. We see an increase in the demand for video for surveillance, both for government and private businesses. This issue includes physical security—securing the building, people, and assets—as well as network and data security... In 2017, security conversations will continue to intensify around not only securing data and networks but physical security as well-think buildings, people, and assets. We also expect to see an increased demand for video surveillance across the public sector and private business.

SEE: Cybersecurity spotlight: The ransomware battle (http://www.techproresearch.com/downloads/cybersecurity-spotlight-the-ransomware-battle/) (Tech Pro Research)

Security will no longer be an afterthought - Signal Sciences' Co-Founder & Chief Security Officer, Zane Lackey

2017 will be a critical year for security, starting with how it's built into technology. DevOps and security will change the way they work together as they realize the need to integrate with each other in order to survive. With IoT on the rise, security will continue to be the primary obstacle preventing consumers from fully welcoming connected devices into their homes and lifestyles. Consumers and businesses are getting smarter and security vendors will be held more accountable in keeping them safe.

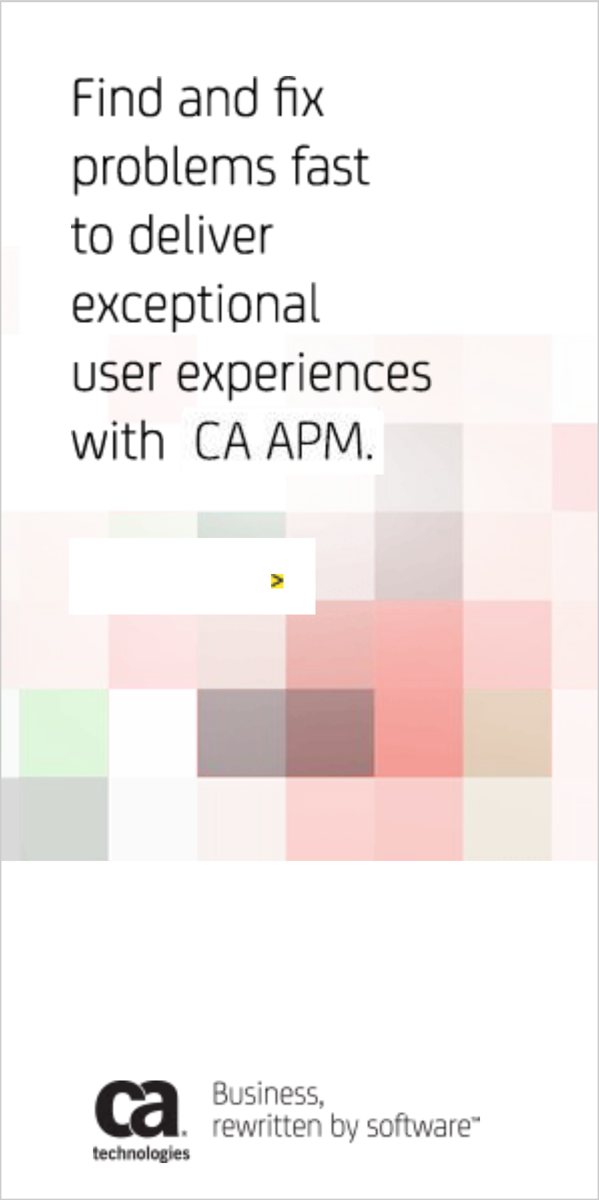
Read more

- Interview with a hacker: S1ege from Ghost Squad Hackers (http://www.techrepublic.com/article/interview-with-a-hacker-s1ege-from-ghost-squad-hackers/) (TechRepublic)
- Interview with a hacker: Gh0s7, leader of Shad0wS3c (http://www.techrepublic.com/article/interview-with-a-hacker-gh0s7-leader-of-shad0ws3c/) (TechRepublic)
- Gallery: The 10 biggest business hacks of 2016 (http://www.techrepublic.com/pictures/gallery-the-10-biggest-business-hacks-of-2016/) (TechRepublic)
- Poll: What new cybersecurity trends will dominate 2017? (http://www.techrepublic.com/article/what-new-cybersecurity-trends-will-dominate-2017/) (TechRepublic)
- 2017 cybercrime trends: Expect a fresh wave of ransomware and IoT hacks (http://www.techrepublic.com/article/2017-cybercrime-trends-expect-a-fresh-wave-of-ransomware-and-iot-hacks/) (TechRepublic)

- Five essential cybersecurity audiobooks (http://www.techrepublic.com/article/five-essential-cybersecurity-audiobooks/) (TechRepublic)
- Five essential cybersecurity podcasts for IT professionals (http://www.techrepublic.com/article/five-essential-cybersecurity-podcasts-for-it-professionals/) (TechRepublic)
- Cyberwar: The smart person's guide (http://www.techrepublic.com/article/cyberwar-the-smart-persons-guide/) (TechRepublic)
- How to safely access and navigate the Dark Web (http://www.techrepublic.com/article/how-to-safely-access-and-navigate-the-dark-web/) (TechRepublic)
- IT Security in the Snowden Era (http://www.zdnet.com/topic/it-security-in-the-snowden-era/) (ZDNet)
- How the Dark Web works (http://www.zdnet.com/article/how-the-dark-web-works/) (ZDNet)
- Cybersecurity sleuths learn to think like hackers (https://www.cnet.com/news/cybersecurity-sleuths-learn-to-think-like-hackers/) (CNET)
- Inside look at the race to outsmart hackers (http://www.cbsnews.com/news/hackers-cybersecurity-crowdstrike-dan-larson-dnc-world-antidoping-agency-state-elections/) (CBS News)

About Dan Patterson

Dan is a Senior Writer for TechRepublic. He covers cybersecurity and the intersection of technology, politics and government.



FEATURED CONTENT

Wise startup advice

Gates, Jobs & Sandberg share business tips for entrepreneurs

How to hire Gen-Y

3 expert tips for recruiting millennial talent

EDITOR'S PICKS

IBM Watson: The inside story

Rise of the million-dollar smartphone

The world's smartest cities

The undercover war on your internet secrets

RECOMMENDED

FREE NEWSLETTERS, IN YOUR INBOX

Tech News You Can Use

We deliver the top business tech news stories about the companies, the people, and the products revolutionizing the planet.

Delivered Daily

SUBSCRIBE

Best of the Week

Our editors highlight the TechRepublic articles, galleries, and videos that you absolutely cannot miss to stay current on the latest IT news, innovations, and tips.

Delivered Fridays

SUBSCRIBE