Predictions 2017: Cybersecurity Risks Intensify

Landscape: The S&R Practice Playbook

by Amy DeMartine, Jeff Pollard, Joseph Blankenship, Andras Cser, Heidi Shey, Christopher McClean, Josh Zelonis, and Merritt Maxim

November 1, 2016

Why Read This Brief

The connected world has arrived; we live and work in it. In this new reality, the next 12 months will see battles rage that will determine the amount of control individuals have over their own data and right to privacy as well as the offensive and defensive responsibilities of our governments. This report guides security and risk (S&R) pros through five predictions for 2017 that highlight escalating ramifications of poor security hygiene and how to mitigate potential damage.

Key Takeaways

Changes In IoT And Healthcare Will Make Them Especially Susceptible To Attacks

Data collection and analysis by companies is exploding as IoT, machine learning, and artificial intelligence become the norm. Name, telephone number, and address are now paired with genetic markers and biometric identifiers in what's considered personally identifiable information. It's a guarantee that cybercriminals will want to monetize this valuable data.

There Is No Panacea Coming For Security Practitioners

There isn't a single product, service, or innovation that will become the "Easy" button for security in the near future. Instead, CISOs must maximize gains by focusing on skills development, strategic vendor selection, and optimizing their information security programs.

Starting Now, Security Must Pick The Winnable Fights

The reality facing security professionals is that they've been trying to win every battle even when it was impossible. But complexity, volume, and skill shortages make continuing that a fool's errand. The new plan has to assume failure, strategize for resilience, and execute based on how detection, prevention, and response work together.

Predictions 2017: Cybersecurity Risks Intensify

Landscape: The S&R Practice Playbook

by Amy DeMartine, Jeff Pollard, Joseph Blankenship, Andras Cser, Heidi Shey, Christopher McClean, Josh Zelonis, and Merritt Maxim
with Stephanie Balaouras, Trevor Lyness, and Peggy Dostie

November 1, 2016

Five Cybersecurity Predictions For S&R Pros In 2017

In 2016, we predicted that cybersecurity would be a major issue in the presidential election and that an executive would step down due to a breach. Both came true in one fell swoop with the Democratic National Committee's (DNC) email hack, which resulted in the resignation of DNC chairwoman, Debbie Wasserman Schultz.[1] If 2016 was the year of how companies and countries responded to breaches, 2017 will be about how companies resolve to avoid breaches. Here's what Forrester predicts security and risk (S&R) pros will face in 2017:

- **A Fortune 1000 company will fail because of a cyberbreach.** There have been multiple cases of companies shuttering business after a cyberattack. In 2011, Dutch certificate authority DigiNotar filed for bankruptcy after an attacker gained hundreds of fraudulent digital certificates criminals could use to target online customers.[2] In 2012, cybersecurity services firm HBGary agreed to acquisition by ManTech after devastating attacks from Anonymous revealed sensitive client records.[3] Broader connectivity and growing investment in digital business creates new implications for devices, data, and corporate resilience. IoT, in conjunction with cloud and BYOD, alters the fundamental ways we plan for resilience. Targeted espionage, ransomware, IP theft, denial of service, privacy breaches, and loss of customer trust all carry more weight today. In 2017, we will see a Fortune 1000 company disappear — through bankruptcy, acquisition, or regulatory enforcement — because of a cyberattack.

  Action: Identify the cybersecurity risks that have the biggest impact on your firm. Attacks don't affect all organizations in the same way; the impact of a cybersecurity event depends on size, industry, location, regulators, and brand promises. What would prove a death blow to your organization? Is it ransomware shutting down critical systems that provide patient care, manufacture goods, or enable financial systems? Perhaps IP theft, such as code from a SaaS application, would cripple your business, particularly when it comes to regional expansion or navigating international copyright laws. Would your business face a recall due to vulnerabilities in IoT devices in heavily regulated industries with no ability to patch or update? Make sure you're spending time protecting the assets and systems that matter most.

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

- **Healthcare breaches will become as large and common as retail breaches.** The 2015 breach of Anthem that affected as many as 80 million patients will become commonplace in the future.[4] As a result of mergers, acquisitions, and other partnership arrangements, large healthcare insurer and provider conglomerates are only increasing in size — as is the critical patient information they store.[5] After Aetna's planned acquisition of Humana, the combined entity will have 60 million patients/customers who fill 600 million prescriptions annually.[6] Why is 2017 a turning point for healthcare providers? First, the consolidation of providers leaves security fragmented with varying security levels. Second, patient data carries tremendous unique, permanent information, such as genetic markers, and biometric data, such as fingerprints.[7] For malicious attackers interested in ransom, blackmail, and espionage, this data will be too tempting not to gain.

  Action: Increase spending on security for healthcare now. Healthcare security spending continues to lag other industries. According to our surveys, public sector and healthcare firms spend 3 percentage points less (23% versus 26% of the IT budget) on security compared with all other firms.[8] Until the recent spate of ransomware attacks and, of course, Anthem's massive breach, many healthcare CISOs approached security as a means of achieving HIPAA compliance, not as a function to protect patients and the hospital from malicious cybercriminals and insiders. Given the critical nature of the services and the sensitivity of the data at risk, healthcare firms should spend on par with other critical infrastructure industries — utilities and telecom spend 35% of their IT budget on security.[9]

- **More than 500,000 IoT devices will suffer a compromise — dwarfing Heartbleed.** Heartbleed demonstrated the danger inherent in using open source components.[10] Today, firms are developing IoT firmware with open source components in a rush to market.[11] Unfortunately, many are delivering these IoT solutions without good plans for updates, leaving them open to not only vulnerabilities but vulnerabilities security teams cannot remediate quickly.[12] When smart thermostats alone exceed over 1 million devices, it's not hard to imagine a vulnerability that easily exceeds the scale of Heartbleed, especially if multiple IoT solutions include the same open source component.[13] Verticals and applications especially vulnerable are fleet management in transportation, security and surveillance apps in government, inventory and warehouse management apps in retail, and industrial asset management in primary manufacturing.[14]

  Action: Require quick remediation and fully automated, scripted security testing. Security as an afterthought for IoT devices is not an option, especially when you can't patch IoT firmware because the vendor didn't plan for over-the-air patching or the IoT device doesn't have reliable network connectivity. Whether you're evaluating IoT solutions or your firm develops them, or both, insist on over-the-air patching or plan ahead to work around any network connectivity issues in a deployment plan to be ready for any remediation. Also, you should treat IoT smart applications like any other software application. Security teams should integrate security testing for vulnerabilities into SDLC processes for development, staging, production, and other environments to reduce risks.

- **The talent gap will force CISOs to allocate 25% to external expertise, automation.** The complexity curve facing enterprises hasn't reached its peak yet, which leaves security stuck solving problems of capacity and capability with limited resources already burdened with too many technologies, too many alerts, and too much to do. With too few internal resources, CISOs will turn to external services and automation tools for relief. We estimate that security services and automation will combine to consume 25% of security budgets in 2017. This combined spending will include security outsourcing, managed security services, security consultants and integrators, and security automation technologies.

  Action: Embrace automation and orchestration. Historical use of on-premises technologies that lack integration or fears of inadequate data protection in the cloud have led security practitioners to fear automation. However, a rising number of threats and limited resources require a combination of human decision-making and repeatable machine tasks to overcome the problems of scaling security expertise. For automated response and remediation to work properly, CISOs must develop rules of engagement for automated response.[15] With a high confidence level that an alert is a real security threat to the business, automated processes can respond to mitigate the threat without waiting for human intervention. CISOs will still need capable talent, so be prepared to compete with vendors for talent while also determining what security services to offer in-house rather than outsourced, considering resource constraints.

- **Within the first 100 days, the new president will face a cybercrisis.** During the US presidential election, many credible sources linked the breach and leak of DNC emails to Russia. As a result of the public allegations, an auction of supposed exploit kits used by the NSA emerged online. Ongoing throughout the election, there have been significant concerns that cybercriminals — nation-state or hacktivists — would attempt to undermine the integrity of voting. The momentum of winning the election gives new presidents the public sponsorship to follow through on key initiatives of their campaigns. However, the 45th president will lose that momentum coming into office by finding themselves facing a cybersecurity incident.

  Action: Prepare for nation-states and ideologies looking to disrupt and degrade. In 2015 and 2016, the US and China made public promises they would de-escalate aggressive attacks against one another, but companies operating in either region should remain skeptical that diplomatic promises will become the new reality. North Korea and Iran both continue to build capabilities for offensive purposes. Political ideologies use electronic means to both recruit and spread information. DDoS attacks using IoT devices are becoming a common means of disrupting operations for companies or individuals that threat actors disagree with. A company can become a target not just because of its size or global presence but also because of its political donations or public statements. If you've never factored geopolitical concerns into your security risk analysis, you ignore them at your own firm's peril.[16]

Supplemental Material

Survey Methodology

Forrester's Global Business Technographics® Security Survey, 2016 was fielded in March to May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. ResearchNow fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

For its Global Business Technographics Security Survey, 2015, Forrester conducted an online survey fielded in April through June 2015 of 3,543 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics provides demand-side insight into the priorities, investments, and customer journeys of business and technology decision-makers and the workforce across the globe. Forrester collects data insights from qualified respondents in 10 countries spanning the Americas, Europe, and Asia. Forrester's Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

For its Business Technographics Global Security Survey, 2014, Forrester conducted a mixed methodology phone and online survey, fielded in April and May 2014, of 3,305 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Each calendar year, Forrester's Business Technographics fields business-to-business technology studies in 10 countries spanning North America, Latin America, Europe, and Asia Pacific. For quality control, we carefully screen respondents according to job title and function. Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Forrester's Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Endnotes

[1] For more information about Forrester's predictions for 2016, please see the "Predictions 2016: Cybersecurity Swings To Prevention" Forrester report and see the "Predictions 2016: The C-Suite And Cybersecurity" Forrester report.

[2] Source: Mike Lennon, "ManTech Completes Acquisition of HBGary," Security Week, April 2, 2012 (http://www.securityweek.com/mantech-completes-acquisition-hbgary).

[3] Source: Kim Zetter, "DigiNotar Files for Bankruptcy in Wake of Devastating Hack," Wired, September 20, 2011 (https://www.wired.com/2011/09/diginotar-bankruptcy/).

[4] Source: Elizabeth Weise, "Massive breach at health care company Anthem Inc.," USA Today, February 5, 2015 (http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/).

[5] Source: David Lewis, "The (2nd) year of the healthcare hack," Information Age, August 5, 2016 (http://www.information-age.com/technology/security/123461796/2nd-year-healthcare-hack).

[6] Source: "Aetna to acquire Humana, combined entity to drive consumer-focused, high-value health care," Aetna press release, August 2015 (https://news.aetna.com/2015/08/aetna-to-acquire-humana/).

[7] Source: Michael Specter, "How the DNA Revolution Is Changing Us," National Geographic, August, 2016 (http://www.nationalgeographic.com/magazine/2016/08/dna-crispr-gene-editing-science-ethics/).

[8] Source: Forrester's Global Business Technographics Security Survey, 2016.

[9] Source: Forrester's Global Business Technographics Security Survey, 2016.

[10] Source: Richard Nieva, "Heartbleed bug: What you need to know (FAQ)," CNET, April 11, 2014 (https://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/).

[11] For more information about IoT's dependence on open source and the security ramifications, see the "The IoT Attack Surface Transcends The Digital-Physical Divide" Forrester report.

[12] Forrester recommends the ability to release fast and ability to deploy quickly. For more information, see the "IoT Success Requires A DevOps Mindset" Forrester report.

[13] Source: Aaron Tilley, "Thermostat Wars: With Help From Apple HomeKit, Ecobee Takes Number Two Place Behind Nest," Forbes, September 28, 2015 (http://www.forbes.com/sites/aarontilley/2015/09/28/thermostat-wars-with-help-from-apple-ecobee-takes-number-two-place-behind-nest/#135933bd1940).

[14] Internet-of-things-enabled applications are poised to revolutionize digital customer experience and enhance digital operational excellence. Some key IoT-enabled applications such as security and surveillance and building management apply across multiple industries, while others, including inventory management, supply chain, and asset management, provide higher value in specific industries. For more information on identifying where the ripest opportunities lie, please see the "The Internet Of Things Heat Map, 2016" Forrester report.

[15] As the remediation costs, customer impacts, and reputational damage of a data breach continue to skyrocket, the security industry must find new ways to prevent the exfiltration of proprietary data by cybercriminals and other malicious actors. Developing more automated threat response processes and a set of cyber rules of engagement will empower security professionals to act more quickly and aggressively and stop data breaches before they impact the business. For more information, please see the "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

[16] Geopolitical conflict is one of the most talked about issues in politics, news outlets, and our daily lives. Yet, businesses worldwide continue to ignore and misinterpret the way such conflicts affect the cybersecurity risk landscape and threaten their survival. Failing to formally incorporate geopolitical considerations in your risk management processes could ultimately mean havoc for your international presence, global customer base, third-party relationships, and business continuity. For more information, see the "Ignore Geopolitical Risks At Your Peril" Forrester report.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

› Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.