Top Cybersecurity Threats In 2018

Landscape: The Security Architecture And Operations Playbook

by Josh Zelonis

November 27, 2017

Why Read This Report

Security and risk (S&R) professionals have the challenging task of using finite budgets to protect their business from every possible attack type in the threat landscape. One strategy for approaching this challenge is to use historical attack trends to prioritize protections against attacks that are the most probable. This report analyzes common attack patterns responsible for breaches in 2017 to help S&R pros prepare for 2018.

Key Takeaways

We're Leaving The Door Open For Attackers
Software vulnerabilities are a leading cause of breaches, and poor patch management practices are reducing the sophistication attackers need to compromise systems.

We've Lost Our Identity
A consequence of the continued loss of personally identifiable information data is that knowledge-based authentication (KBA) methods such as passwords and other anecdotal data can no longer be trusted as shared secrets.

Contaminated Updates Are A Growing Threat
While many organizations struggle with getting patches applied in a timely manner, a new trend of watering hole attack targets organizations that implicitly trust supplied updates.

Top Cybersecurity Threats In 2018

Landscape: The Security Architecture And Operations Playbook

by Josh Zelonis
with Stephanie Balaouras, Bill Barringham, and Peggy Dostie

November 27, 2017

Table Of Contents

Related Research Documents

The Forrester Wave™: Digital Risk Monitoring, Q3 2016

Ransomware Protection: Five Best Practices

Vendor Landscape: Third-Party Risk Intelligence

Vendor Landscape: Vulnerability Management, 2017

FORRESTER®

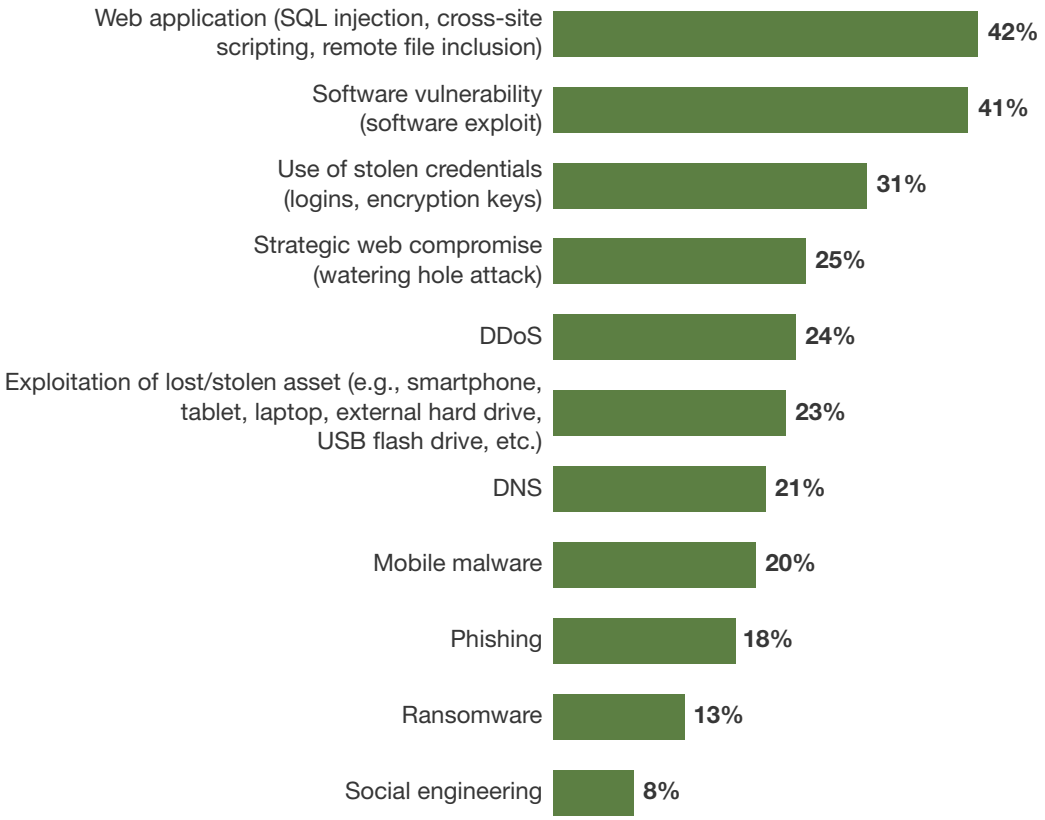
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

S&R Pros Must Understand And Adapt To The Threat Landscape

Companies are under attack: 58% of global enterprise respondents say their firms have experienced at least one breach during the past 12 months.[1] Of these, 50% say their firm suffered at least one internal incident, and 36% suffered at least one attack or incident involving a business partner or third-party supplier.[2] Internal incidents can involve employees who simply make poor decisions regarding the handling and use of the firm's sensitive data or employees who have malicious intent.[3] These malicious insiders can also work in concert with external threat actors. This year, 70% of global enterprise respondents whose firms experienced a breach say at least one was at the hands of external threat actors.[4] Year to year, many of the macrotrends for external attacks are similar, but how these attacks are carried out is constantly evolving. To help S&R pros better defend against these, we identified and analyzed the top methods of intrusion (see Figure 1).

FIGURE 1 External Intrusion Methods

"How was the external attack carried out?"
(Multiple responses accepted)



Base: 245 network security decision makers whose firms have had an external security breach in the past 12 months (1,000+ employees)
Source: Forrester Data Global Business Technographics® Security Survey, 2017

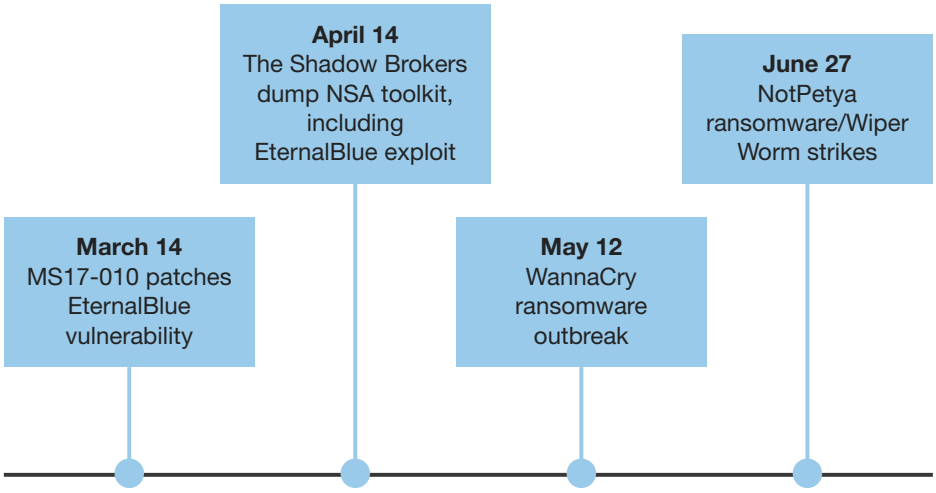
No. 1: Ineffective Vulnerability Management Will Make Firms Victims Of Destructive Attacks

According to Forrester's 2017 global security survey, software vulnerabilities were responsible for 41% of external data breaches last year. A shocking demonstration of our inability to effectively patch vulnerable systems was the sequence of events following EternalBlue — the exploit responsible for the massive outbreak of WannaCry and NotPetya ransomware. This exploit targeted the Server Message Block (SMBv1) service, which Microsoft has enabled by default on every Windows operating system for decades, creating an enormous attack surface area.[5] While remediation was listed as "critical" by Microsoft, these attacks created global damage months after patch availability.[6]

› **What you need to know: High-profile breaches are the result of unpatched systems.** Hackers released the WannaCry ransomware worm to devastating effect approximately 60 days after Microsoft made the patch (MS17-010) available. This very well publicized attack affected patient care at the National Health Service (NHS) in the UK and infected approximately 300,000 systems worldwide. A full 30 days later, 90 days after Microsoft had released a critical fix for this issue, NotPetya again caused catastrophic damage — exploiting the same vulnerability (see Figure 2). Just how devastating was this second wave? The pharmaceutical giant Merck & Co. has estimated losses over $275 million from the NotPetya attack.[7]

› **What to do about it: Vulnerability management needs board-level attention.** We are seeing boards getting more involved in understanding cybersecurity issues, and it is becoming more common that they are homing in on patch management policies. While the security of your organization shouldn't rest on applying patches, the ability to perform rote security tasks such as patch management is a great predictor of overall security posture.[8]

FIGURE 2 Rapid Patching Of Zero Day Exploits Is Imperative



No. 2: Insecure Cloud Services Will Continue To Hemorrhage Sensitive Data

During the last few years, we have seen a number of large data leaks due to misconfigured cloud services such as MongoDB and Amazon's Simple Storage Service (S3). In Q3 of 2017 alone, major companies such as Time Warner, Verizon, and Viacom experienced this type of data leak — losing encryption keys, customer account details, and other sensitive data.[9] While third parties were directly responsible for the loss of customer data in both the Time Warner and Verizon situations, it's important to recognize whose name ends up in the press when shared customer data is lost.[10]

- **What you need to know: Public S3 shares are a decision, not a default.** It's important to understand that for all the negative attention Amazon has received in the press regarding these leaky S3 buckets, they are not public by default.[11] According to Chris Vickery, director of cyber risk research at UpGuard, "Somebody [who] had administrative control over this data either made a decision to make it public or didn't realize what they were doing was going to make it public."[12] Whether this is a shadow IT issue or incompetence, this problem is real, and it keeps happening. In fact, this is so pervasive that according to Rick Holland of digital risk monitoring (DRM) firm Digital Shadows, "In eight weeks of enumeration, Digital Shadows detected just over 5,580 Amazon S3 buckets containing over 233 million files."
- **What do about it: You must be proactive in managing your digital risk.** You need to have visibility into how your admins configure publicly facing services. While this may be accomplished through periodic red team exercises or internal auditing, Forrester recommends working with a digital risk monitoring (DRM) company to monitor your infrastructure externally in real time.[13]

No 3: The Equifax Breach Will Render Knowledge-Based Authentication Ineffective

Our global enterprise survey respondents told us that 42% of breaches targeted personally identifiable information (PII), making it the most common type of data targeted by attackers (see Figure 3).[14] While stolen card data and credentials have more obvious monetization paths, these data types are more easily changed than information like names, birthdays, and social security numbers (SSNs). With the information stolen in the Equifax breach, identity thieves now have everything they need to access your medical records, bank accounts, and tax returns.[15]

- **What you need to know: Knowledge-based authentication is losing its effectiveness.** There are no longer secrets. The model of your first car, your mother's maiden name, and now, in the US, even your SSN must be assumed to be public information. There is nothing you know about yourself that someone else can't answer, and this applies to your customers as well. The Equifax breach has changed the game forever, and while we're waiting for the fallout, it's time to plan for a future without knowledge-based authentication.
- **What to do about it: Treat identity as an assertion, and authorize based on confidence.** This is an area where the retail segment may have a head start on the rest of the security industry. Although not explicitly a security measure, limiting friction to ensure completion of a transaction versus fraud risk is a balancing act all organizations must now perform. Outside the cyberdomain, lenders have been putting fraud holds on credit cards when purchasing patterns change. Begin using customer insight data to perform behavior-based analytics when validating identity, and increase authorization of the account based on confidence.[16]

FIGURE 3 PII Was A Top Target Of Breaches In 2017

Corporation	Date made public	Industry	Impact
America's JobLink	3/17/2017	Technology	• Around 4.8 million customer accounts were breached. Impacted account holders were from Alabama, Arizona, Arkansas, Delaware, Idaho, Illinois, Kansas, Maine, Oklahoma, and Vermont. • Information breached included full names, birth dates, and social security numbers.
Chipotle	4/25/2017	Food and beverage	• Malware stole names and credit card information from cash registers. • Most restaurants were affected.
Deep Root Analytics and Republican National Committee	6/12/2017	Technology and politics, respectively	• The personal data on 198 million American voters, including names, birth dates, home addresses, phone numbers, and voter registration details was leaked. • Data was exposed via a misconfigured database owned by the RNC-contracted marketing firm Deep Root Analytics.
Deloitte	9/25/2017	Professional services	• Review of impact is ongoing as of this writing. • Hackers potentially had access to user names, passwords, IP addresses, architectural diagrams, and health information.
Dow Jones	7/17/2017	Media	• Between 2.2 million and 4 million subscribers' information, including names, internal customer IDs, home and business addresses, the last four digits of credit card numbers, as well as email addresses, were exposed.
Dun & Bradstreet	3/15/2017	Professional services	• 33.7 million email addresses and contact information were exposed. Includes names, job titles, job functions, work email addresses, and phone numbers. • Brought to light risks posed by third-party vendors.

FIGURE 3 PII Was A Top Target Of Breaches In 2017 (Cont.)

Corporation	Date made public	Industry	Impact
Edmodo	5/11/2017	Education	• 78 million customers had user account details, including user names, email addresses, and hashed passwords, stolen.
Equifax	9/8/2017	Credit risk assessment	• Personal data for 143 million people was exposed. • Made one of the worst breach responses possible.
Kansas Department of Commerce	3/17/2017	Public sector	• Personal information for more than 5.5 million people from 16 states was compromised in a breach of the Kansas Department of Commerce database. • The exposed data included social security numbers, but there was also personal information breached for 850,000 additional accounts that did not include SSNs.
OneLogin	5/31/2017	Technology	• Accessed database tables with information about users, apps, and keys. • Number of customers effected was not disclosed.
US Securities and Exchange Commission	9/17/2017	Federal government	• Hackers infiltrated a database that stores public company financial filings, potentially enabling insider trading.
Verizon	7/12/2017	Telecommunications	• Phone numbers, names, and pin codes for 6 million Verizon customers was exposed. • Cloud server that was affected was owned by a third-party vendor.

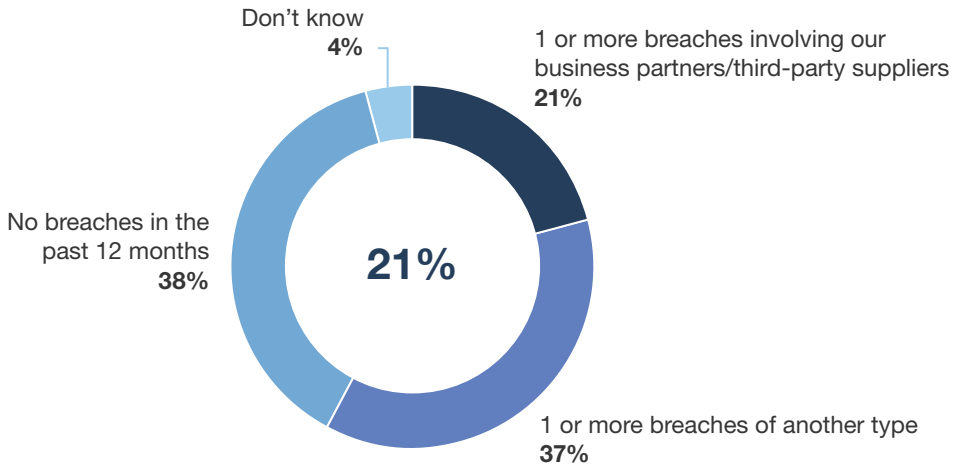
No. 4: Strategic Compromise Will Allow Attackers To Undermine Your Supply Chain

Your partners are also under threat: 21% of global enterprise network security decision makers have experienced a security incident involving a third party (see Figure 4). Third-party risk is frequently discussed as an exposure due to data shared with partner companies and data processors. This type of downstream risk can sometimes put people in mortal danger as with the TigerSwan breach, where a third party leaked resume information for foreign nationals that included admissions of their complicity with US forces and home contact information.[17] Too frequently, supply chain issues that are upstream to your organization are ignored and incidents go unnoticed and unpublicized.[18]

- **What you need to know: You may be drinking from a poisoned well.** Forrester has been tracking a dangerous trend in which cybercriminals use compromised update servers to distribute malware, a trend that just this year has already affected Apple, IBM, and Google.[19] This issue is particularly pernicious as it doesn't require end user interaction, allowing attackers to deploy signed malware directly to your servers using trusted channels.[20] The very channels you're using to obtain security updates, cybercriminals are using against you.
- **What you need to do about it: Perform threat assessments of your supply chain.** This year, the US Department of Homeland Security (DHS) issued a directive banning the use of Kaspersky software by federal agencies.[21] There has been a split in the security community, with some people questioning this decision and even demanding evidence of malfeasance. While Kaspersky has even gone to the effort of providing source code to vindicate themselves, the ability to push malicious updates has been discussed as an unacceptable risk.[22] The decisions you make may not rival the global scale of this scenario, but you should be reviewing the amount of trust you place in suppliers and how seamlessly their software updates get deployed in your environment.[23]

FIGURE 4 One-Fifth Of Enterprise Respondents Reported A Third-Party Breach

Enterprise third-party breaches in the past 12 months



Base: 604 global network security decision makers (1,000+ employees)
Source: Forrester Data Global Business Technographics® Security Survey, 2017

No. 5: Ransomware Will Expose Lack Of Cybersecurity And Business Continuity Prep

Ransomware represents a shift toward direct monetization of system compromise by cybercriminals — away from more traditional tactics of leveraging a compromise to steal and sell data. The problem for enterprises is business interruption due to ransomware that triggers disaster recovery scenarios with recovery time objectives (RTO) that may not have been tested effectively. Trends in ransomware are changing the requirements on BCP/DR from unlikely scenarios to eventualities.

› **What you need to know: Business continuity requires extensive planning and testing.** Following the NotPetya attack in June, pharmaceutical company Merck still hadn't fully recovered by its quarterly earnings report a month later.[24] A recent joint Forrester/Disaster Recovery Journal survey showed that 77% of organizations have documented response plans for data/information tampering, but only 27% are testing these plans on more than an annual basis.[25] Data that is critical enough to back up on a daily basis needs to be tested more than annually by both operations and security teams to mitigate the impact of an eventual disaster.

› **What you need to do: Test your recovery capabilities end-to-end.** Recovery from a cyberattack requires cooperation between multiple teams within your organization. When the shipping company Maersk was hit with NotPetya, it took their security team a full 24 hours to just contain the attack, and it was another day before they were able to accept new shipping manifests from current customers.[26] When doing business continuity planning, be sure to engage your security, operations,

and the lines of business to build a holistic understanding of what the organization requires to recover and generate realistic recovery time objectives — then do end-to-end testing to ensure your organization can meet these objectives.

Supplemental Material

Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2017, was fielded between May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Data'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. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Data's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] We surveyed 604 global network security decision makers at firms with 1,000 employees or more. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[2] We surveyed 349 global network security decision makers at firms with 1,000 employees or more and whose firms have had a security breach in the past 12 months. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[3] In 2017, Forrester found that of the 173 enterprise network security decision makers whose firms had had an internal security breach in the past 12 months, 50% of the breaches were attributable to abuse or malicious intent (e.g., authorized or terminated user exploiting access rights or gaining unauthorized access), 42% to inadvertent misuse or an accident (e.g., authorized users inappropriately disclosing sensitive information by accident), and 8% to both. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[4] We surveyed 349 global network security decision makers at firms with 1,000 employees or more and whose firms have had a security breach in the past 12 months. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[5] Source: "How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server," Microsoft Support, September 27, 2017 (https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and).

[6] Source: "Microsoft Security Bulletin MS17-010 - Critical: Security Update for Microsoft Windows SMB Server (4013389)," Microsoft TechNet, March 14, 2017 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx) and see the Forrester report "Ransomware Protection: Five Best Practices."

[7] Source: Lee Mathews, "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million," Forbes, August 16, 2017 (https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#608d26474f9a).

[8] See the Forrester report "Vendor Landscape: Vulnerability Management, 2017."

[9] Source: Iain Thomson, "Viacom exposes crown jewels to world+dog in AWS S3 bucket blunder," The Register, September 19, 2017 (https://www.theregister.co.uk/2017/09/19/viacom_exposure_in_aws3_bucket_blunder/).

[10] Source: Dan O'Sullivan, "Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts," UpGuard, July 12, 2017 (https://www.upguard.com/breaches/verizon-cloud-leak) and Dell Cameron, "Millions of Time Warner Cable Customer Records Exposed in Third-Party Data Leak," Gizmodo, September 1, 2017 (https://gizmodo.com/millions-of-time-warner-customer-records-exposed-in-thi-1798701579).

[11] Source: "Permissions for the Amazon S3 Bucket," AWS Config (https://docs.aws.amazon.com/config/latest/developerguide/s3-bucket-policy.html).

[12] Source: Chris Brook, "Chris Vickery on Amazon S3 Data Leaks," Threatpost, September 25, 2017 (https://threatpost.com/chris-vickery-on-amazon-s3-data-leaks/128120/).

[13] See the Forrester report "The Forrester Wave™: Digital Risk Monitoring, Q3 2016."

[14] Source: Forrester Data Global Business Technographics Security Survey, 2017.

[15] Source: Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," The New York Times, September 7, 2017 (https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html).

[16] See the Forrester report "The Future Of Identity And Access Management."

[17] Source: Dan O'Sullivan, "Insecure: How A Private Military Contractor's Hiring Files Leaked," UpGuard, September 2, 2017 (https://www.upguard.com/breaches/cloud-leak-tigerswan).

[18] Source: Brian Krebs, "How to Bury a Major Breach Notification," KrebsOnSecurity, February 21, 2017 (https://krebsonsecurity.com/2017/02/how-to-bury-a-major-breach-notification/).

[19] Source: Dan Goodin, "After phishing attacks, Chrome extensions push adware to millions," Ars Technica, August 3, 2017 (https://arstechnica.com/information-technology/2017/08/after-phishing-attacks-chrome-extensions-push-adware-to-millions/); Sean Gallagher, "Apple deleted server supplier after finding infected firmware in servers [Updated]," Ars Technica, February 25, 2017 (https://arstechnica.com/information-technology/2017/02/apple-axed-supermicro-servers-from-datacenters-because-of-bad-firmware-update/); Oren Koriat, "Preinstalled Malware Targeting Mobile Users," Check Point blog, March 10, 2017 (https://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/); and Lorenzo Franceschi-Bicchierai, "IBM Shipped USB Drives Filled With Malware to Customers," Motherboard, May 3, 2017 (https://motherboard.vice.com/en_us/article/ibm-malware-usb-drives-storwize?utm_source=mbtwitter).

[20] Source: Andy Greenberg, "Software Has A Serious Supply-Chain Security Problem," Wired, September 18, 2017 (https://www.wired.com/story/ccleaner-malware-supply-chain-software-security/).

[21] Source: Stefan Becket, "DHS bans government use of Kaspersky Lab software, citing ties to Russia," CBS News, September 13, 2017 (https://www.cbsnews.com/news/dhs-bans-kaspersky-lab-software-citing-ties-to-russian-government/).

[22] Source: Lily Hay Newman, "Security News This Week: Russian Security Giant Kaspersky Lets The Feds Review Its Code," Wired, July 8, 2017 (https://www.wired.com/story/security-news-kaspersky/).

[23] There is a plethora of security solutions to protect endpoints, mobile devices, and employees, but there is a deeper threat vector security pros often ignore. This threat is built into the very technology enabling today's digital businesses — hardcoded into the hardware and firmware of everything from point-of-sale (POS) devices to consumer electronics to high-end computing systems. See the Forrester report "Hardcoded For Failure."

[24] Source: "Merck Announces Second-Quarter 2017 Financial Results," Merck press release, July 28, 2017 (http://www.mrknewsroom.com/news-release/corporate-news/merck-announces-second-quarter-2017-financial-results) and see the Forrester report "Identify And Estimate The Costs Of Downtime On Your Business."

[25] Source: Stephanie Balaouras, "The State of Enterprise Risk Management 2016," Disaster Recovery Journal (http://drj.com/images/surveys_pdf/forrester/2015-Forrester-Survey.pdf).

[26] Source: Michael Mimoso, "Maersk Shipping Reports $300M Loss Stemming From NotPetya Attack," Threatpost, August 16, 2017 (https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/).

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.