Predictions 2015: Data Security And Privacy Are Competitive Differentiators

Governments, Criminals, Tech Giants, Customers, And Enterprises Spar Over Protections And Rights

by Heidi Shey, Nick Hayes, Renee Murphy, Ed Ferrara, and John Kindervag
with Stephanie Balaouras, Tyler Shields, J.P. Gownder, Cheryl McKinnon, and Claire O'Malley

WHY READ THIS BRIEF

Love him or hate him, Edward Snowden's revelations of widespread National Security Agency (NSA) government surveillance triggered an international discussion and debate on privacy. Suddenly, the European Union (EU) was threatening to scrap the Safe Harbor Agreement, enterprises shelved their plans to adopt cloud services from US-based providers, and tech giants like Apple and Google found it necessary to steadfastly deny any claims that they gave the NSA backdoor access to their customers' data. Eager to prove its privacy bona fides to customers around the world, and much to the dismay of the FBI, Apple now encrypts messages, mail, calendar, contacts, and photos in iOS 8 by default. This reignition of privacy rights, together with increasing cyberattacks and the ongoing deperimeterization of the digital enterprise, has forced security and risk (S&R) pros to move more and more protections closer to the data itself. It also demonstrates that in the battle to win, serve, and retain customers, data security and privacy have become competitive differentiators and, thus, a top business technology agenda item. In this report, we provide S&R pros with analysis and recommendations regarding our nine predictions for data security and privacy.

DATA-CENTRIC SECURITY IS ESSENTIAL TO THE BUSINESS TECHNOLOGY AGENDA

Data is the intellectual property (trade secrets, formulas, designs, code, search algorithms, etc.) that differentiates your enterprise's products and services. If competitors steal your intellectual property, they will beat you to market and steal your customers. Data is also your customers' personally identifiable information (PII), personal card information (PCI), and personal health information (PHI). Privacy abuses and intentional or accidental breaches of sensitive customer data undermine the trust relationship between your enterprise and its customers. If your customers don't trust you to rigorously protect and genuinely respect their sensitive data, they'll take their business elsewhere. Thus, if your enterprise wants to successfully win, serve, and retain customers, the people, process, and technology that underpin data security and privacy must be critical elements of its business technology agenda.

Encryption, Key Management Become Critical Even As Standards Wither

Firms will increasingly set their sights on key management as more and more S&R pros turn to pervasive encryption for protection that travels with the data itself and renders data unreadable to would-be cybercriminals. The need to secure data in the cloud and wariness over NSA, government, and cloud provider access to the enterprise's data is also fueling greater interest in encryption today, and especially options for customer-managed encryption keys. Attackers who compromise trust end up with the keys to the kingdom; APT1 and Mask are examples of advanced persistent threats and cyber operations that target certificates and keys.[1] In 2013, hackers compromised the US Emergency Alert System via a firmware update that exposed secure shell (SSH) keys.[2] In 2014, the Heartbleed bug allowed attackers to steal private encryption keys.[3]

Awareness of such threats is growing, and Cryptographic Keys and Digital Certificate Security Guidelines is one of the proposed special interest groups for 2015.[4] Standards like NIST SP 800-57 and ISO/IEC 11770 have thus far addressed various aspects of key management, and the Oasis Key Management Interoperability Protocol (KMIP) continues to evolve as well.[5] However, key management standards as a whole remain a limiting factor, and progress on these standards will stagnate due to market confusion and dissent as to what centralized key management means and how to best achieve this desired state.

- **What it means: Be proactive and reduce risk exposure with new cryptographic techniques.** Don't rely on final guidance from or an update to a particular standard before taking action to manage keys. A recent study estimated that the average $1 billion-plus enterprise has more than 17,000 keys and certificates and that trust-based attacks can cost an organization up to $398 million per incident, with an average projected loss of $35 million over the next two years.[6] Explore your options for key management early on to realize additional benefits like reduced operational complexity and risk. Look for new encryption and key management vendors to bubble up in 2015; the year may also see some established large security vendors snap up independent crypto-vendors and see a greater maturity of solutions that encrypt data before it is stored in a cloud and without the cloud provider having access to the keying material.

Rights Management Is No Longer A Dirty Word — It's A Prime Acquisition Target

Rights management in its various flavors, names, and abbreviations — DRM, IRM, ERM, eDRM — has typically conjured feelings of frustration and been labeled as a cumbersome and not-user-friendly technology. As a "tweener" technology, rights management doesn't fit strictly in security or information management. Deployment of rights management tools has historically been confined to departments within industries like aerospace, electronics, manufacturing, and intelligence services. Rights management has applications for protecting content for enterprise use and monetization, and for providing analytics about content use that would be of value to marketers and S&R pros alike.[7]

Forrester sees limited enterprise appeal of standalone rights management tools that don't integrate with classification, content management/collaboration, DLP, or other data security tools.[8] However, as S&R pros increasingly looking to place controls closer to the data itself and gather intelligence (e.g., real-time analytics and contextual information) about how the data is used, rights management as a capability plus analytics as a fully integrated feature become very attractive.[9] For example, many secure file sharing and collaboration solutions are moving fast on providing a rights management feature.[10] Rights management providers are also moving to ramp up analytics in their solutions.[11] As vendors scramble to meet demand, those with cash will move to acquire the necessary technology for their portfolio.

- **What it means: Look beyond the IRM label and ask providers for details.** Vendors will hop on the bandwagon, and as the market comes to a boil in rights management alphabet soup, S&R pros must be aware that one vendor's information rights management (IRM) is not another's enterprise rights management (ERM). You must answer questions such as: Is rights management integrated by default, and what else is it integrated with (e.g., identity)? Is it done through a partner (e.g., Microsoft, Adobe), and what's required to operationalize it? Does it require a plug-in or agent? What content controls — and for what file types — are you actually getting with the solution? Evolving privacy laws and a parade of data breaches are driving demand for encryption as well as reshaping the future of rights management. We are at an inflection point today of defining who has the rights to do what to data, and figuring out how to enforce the outcome.

Data Disposal Will Gain Attention And Traction In The Enterprise

Data disposal is the last, and often overlooked, piece of the data life cycle. As firms progress with data discovery and classification efforts to help define their data, they must identify and address old data that is of no use to the business as well. Unneeded and unused data is a liability to the business rather than an asset, and applies to both data and content on servers; peripherals like printers, USB flash drives, and hard drives; and physical documents that contain sensitive data. Security and risk professionals can play a bigger role in updating or executing on corporate retention policies. EU data protection discussions about the right to be forgotten (now the right to erasure) have also generated greater awareness and questions about policies, what is technologically feasible, and exceptions to adhering to this data disposal requirement. There are also 30 US states that have data disposal laws that apply to businesses.[12]

- **What it means: Have an end-of-life strategy for data and devices.** Neglecting data disposal puts the enterprise at risk, and improper data disposal can also lead to data breaches. In 2013, there were 69 publicly reported incidents involving improper disposal of paper documents containing sensitive data, compromising more than 300,000 records.[13] So far in 2014, this figure is up to 29 incidents and more than 53,000 records compromised.[14] In one such example, patient medical records from Midwest Women's Healthcare Specialists in Kansas City, Missouri, were found blowing in the wind because they were not shredded and simply disposed of in a trash can that turned over.[15] Consultancy firm Ernst & Young (EY) was accused of a data breach after a Canadian used-computer dealership purchased old servers that contained sensitive client data.[16] Partner and compliance requirements may also necessitate data disposal, along with proof.

Half Of Enterprises Will Consider Privacy A Competitive Differentiator

From navigating a maze of evolving and conflicting global privacy laws to meeting business partner requirements in today's data economy, privacy discussions are front and center.[17] We are in a golden age of data breaches. Consumer attitudes about privacy are changing in response to the NSA scandal; consumers have a greater awareness about data brokers, privacy tradeoffs, and options for protecting privacy.[18] Companies are sensitive to this and adjusting their strategies and messaging accordingly.[19] Meanwhile, customers — both consumers and businesses — vote with their wallets. Today, about a third of security decision-makers in North America and Europe view privacy as a competitive differentiator for their business.[20] In a digital and always-connected world where buyers have instant access to information at their fingertips, you must establish and maintain customer trust in data collection and handling practices.

- **What it means: Identify a privacy champion.** The EU data protection regulation requires the appointment of a *data protection officer* responsible for applying its provisions.[21] Proposed updates call for organizations that handle EU citizen data, regardless of whether the business is based in the EU, to do the same.[22] In the US, it's more common to see the title of chief privacy officer for this role.[23] A privacy champion for the enterprise, this role is responsible for weighing in not only on customer data security and privacy issues but also on corporate and employee data and agreements with third-party business partners. For example, privacy champions work closely with marketers, who manage personal info, HR pros, who manage employee rights and hiring-related privacy issues, and business partners to determine data-handling requirements.

As Social Media Adoption Grows, S&R Pros Will Become Stronger Privacy Advocates

Since the NSA scandal and recent high-profile data breaches made headlines, more consumers have begun taking proactive measures to protect their personal data, and in particular, their social data. In fact, the most common step consumers now take to protect their personal data is to update their privacy settings on their social profiles.[24] Yet, even with consumers more wary about privacy, they're not abandoning social networks altogether and continue to participate and engage on these channels.[25] Moreover, they're actually interacting with more brands on social media and have growing expectations with the timeliness and result of their social interactions with these brands. Meanwhile, marketing and other business functions will continue to extract greater value from social data with meaningful customer segmentation, affinity mapping, and other valuable customer insights.

- **What it means: Prioritize transparency and trust to keep customers loyal.** Just because consumers will continue to engage on social channels doesn't mean they're ambivalent when it comes to privacy. In fact, the vast majority of consumers are skeptical of how their social data is used even when the information that's accessed is public. Since the business value of this consumer data is likely too great for your firm not to use at least in some manner, S&R's goal should be to act as the internal privacy advocate and develop data strategies that ease consumer skepticism as much as possible. Be open about data initiatives and explain in public communications how and why you use consumer data, as well as the measures you take to actively protect it — and ensure that what is communicated is actually done![26]

A Wearables Health Data Breach Will Spur FTC Action

Wearable health and fitness devices have captured the imagination of health conscious consumers, businesses, and the healthcare industry. Forrester's Consumer Technographics® data shows that US online consumer interest in wrist-worn wearables increased 14%, from 28% to 42%, between 2013 and 2014."[27] Some employers are looking to monitor the personally generated health information from these wearables as a part of corporate-wellness programs.[28] Healthcare insurance providers are exploring how they might use this data as well.[29] Apple's new iPhone 6 is shipping with personal health apps and HealthKit, while Samsung's Galaxy S5 comes with its own health app and sensors to capture heart rate and footsteps taken.[30]

From a regulatory perspective, we are in uncharted waters. Some vendors are looking at various levels of FDA approval for their products. Yet the race to bring health and fitness wearables to market combined with the variety of data that can be collected raises questions about privacy concerns for acceptable data use, permissioning access, and storage.[31] From the perspective of HIPAA, consumer-generated healthcare information (CGHI) is not considered regulated PHI.

- **What it means: Treat consumer-generated healthcare info as if it were your own.** In the US, a breach of this type of data may not put you under fire from HIPAA (yet) but will likely get you the attention of the Federal Trade Commission (FTC) and definitely upset your customers. From a regulatory perspective and with a mandate to protect consumers, it seems like the FTC is the only one with justification to regulate security and privacy in these types of healthcare apps. As the FTC continues to assert its authority as a privacy regulator, the healthcare space is an attractive arena. Healthcare mobile app providers won't be able to address privacy in these apps before data is breached (it's only a matter of time, especially if these apps connect to other PHI or PII) and the FTC steps in to try to regulate these offerings to protect consumer privacy.

State-Sponsored Medical Records Theft Will Rise In 2015

In July 2014, Community Health Systems, an operator of over 200 hospitals in 29 states, was the victim of a security breach in April and June 2014. In its 8-K filing with the SEC, the company stated that Mandiant determined that the breach was state sponsored by China and resulted in the breach of 4.5 million medical records.[32] While electronic medical records can fetch $50 a record on the black market and can be used to get payment information or controlled medications, these breaches are not for financial gain.[33] Mandiant noted that, while this particular intruder usually steals intellectual property, this breach was "non-medical patient identification data related to the company's physician practice operations."[34] Look for healthcare, medical device, oncology, and research data breaches from state-sponsored attacks to increase, as the World Health Organization predicts that the cancer growth rate will grow by 70% worldwide over the next two decades.[35]

- **What it means: The time for healthcare companies to step up their security is now.** To prevent patient and intellectual property loss to state-sponsored hackers, healthcare companies of all types, including research hospitals, should start adopting security controls and capabilities comparable to those of the financial industry.[36] Insider threats are just as great, with one engineer who stole millions of engineering schematics for MRI machines and another convicted of economic espionage for stealing a possible cancer-fighting compound and the research data that led to its creation.[37] All aspects of the healthcare industry must get the basics right. DLP, Zero Trust, security awareness, persistent threat and vulnerability analysis, and security monitoring all need to be implemented and budgets need to increase to address these state-sponsored threats.

Cloud Security Monitoring Will Slowly Improve, But Privacy Remains At Risk

As cloud adoption continues to accelerate, cloud vendors have made good progress in the development of controls for cloud-based workloads, but they must do more. The impact on privacy is real as more sensitive information either explicitly or implicitly moves to the cloud through planned and unplanned expansion.[38] Behavioral monitoring of applications, networks, and people are all in their infancy for cloud environments. However, all of Forrester's research still singles out security as the primary inhibitor of cloud adoption of all types.[39]

Current approaches to cloud security mirror other forms of outsourcing, including colocation. This may not be the best approach overall, as these virtualized environments must use new security controls styled to meet the needs of new flexible environments. What's needed is an effective ability to detect and protect against data loss in cloud environments — especially for data that falls under privacy compliance regulations. This requires effective continuous monitoring. While we see vendors moving forward with improved methods for security monitoring, the pace is not keeping up with the need.

- **What it means: Demand monitoring for your cloud environments.** Organizations are accelerating cloud deployments due to the flexibility of these environments, but privacy could suffer if companies can't properly monitor for potential adversary behavior and data loss. Vendors like Alert Logic, AlienVault, Datapipe, and Elastica can help here, and S&R pros must also push them and demand that their cloud providers and managed security service providers (MSSPs) do a better job of providing monitoring capabilities. Technology providers, service providers, and platform vendors all need to step up capabilities in this space to better support protection of customer privacy.

Political Instability Globally Will Put Privacy In The Cross-Fire

The rise in the number and destructiveness of cyberattacks in no small way can be attributed to two factors: the ability for organized crime to monetize their stolen property and the ability of nation states and their proxies to use cybercrime as a form of defense. The impact to privacy will be pronounced, as many of the record types that these adversaries want are easily monetized or represent a direct path to monetization, such as credit card, healthcare, and PII data. Russian crime groups in 2014, for example, amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses.[40]

This trend will continue. The current adversarial relationship between western nations and Russia over Ukraine will not support cooperation of the arrest and prosecution of these groups. More directly, the US White House had expressed fears that the recent JPMorgan Chase breach of an estimated 76 million names, addresses, phone numbers, and email addresses was actually sponsored by the Russian government in response to Western sanction for Russia's incursion into the Ukraine.[41] This remains unproven, but as of this writing, the investigation continues. In addition, adversarial relationships and global conflicts increasingly have a cyber-element. Militant group ISIS is under watch as its cyber capabilities are being debated.[42]

- **What it means: Protect customer privacy from both adversaries and governments alike.** The ongoing attacks from organizations that operate under the cover, with sanction or in cooperation with organized crime and nation state actors, present unprecedented challenges to privacy protection. Banks and other types of commercial enterprises have astronomically large amounts of sensitive information about their customers, and much of this information is easily monetizable. At the same time, law enforcement and national security counter measures, such as surveillance programs, will expose private information to scrutiny beyond what the owners of the information may feel comfortable with.

SUPPLEMENTAL MATERIAL

Methodology

Forrester collaborated with CyberFactors to obtain the data in this report. The data may contain publicly available information and/or proprietary data collected by CyberFactors. The analysis of the data is exclusively Forrester's. More information about CyberFactors is available at www.cyberfactors.com.

ENDNOTES

[1] Source: Mandiant, "APT 1" (http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) and "Kaspersky Lab Uncovers 'The Mask': One of the Most Advanced Global Cyber-espionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers," Kaspersky Lab, February 11, 2014 (http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Uncovers-The-Mask-One-of-the-Most-Advanced-Global-Cyber-espionage-Operations-to-Date-Due-to-the-Complexity-of-the-Toolset-Used-by-the-Attackers).

[2] Hackers who gained access to the emergency broadcast system issued an alert to the public about a zombie attack. Source: Zack Whittaker, "US Emergency Alert System open to more 'zombie' hackers after accidental SSH key disclosure," Zero Day, July 9, 2013 (http://www.zdnet.com/u-s-emergency-alert-system-open-to-more-zombie-hackers-after-accidental-ssh-key-disclosure-7000017811).

[3] Source: Megan Geuss, "Private crypto keys are accessible to Heartbleed hackers, new data shows," Ars Technica, April 13, 2014 (http://arstechnica.com/security/2014/04/private-crypto-keys-are-accessible-to-heartbleed-hackers-new-data-shows).

[4] The PCI Council has proposed seven possible topics for 2015 special interest groups (SIGs) to put up for vote. Final results will be announced in November 2014 and commence in January 2015. Source: "Special Interest Groups," PCI Security Standards Council (https://www.pcisecuritystandards.org/get_involved/special_interest_groups.php).

[5] Source: Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, "Recommendation for Key Management – Part 1: General (Revision 3)," US Department of Commerce, July 2012 (http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf) and ISO (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53456 and https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmi).

[6] Source: Fahmida Y. Rashid, "Trust-Based Attacks Against SSH, SSL Cost Firms Big Money: Report," Security Week, February 20, 2013 (http://www.securityweek.com/trust-based-attacks-against-ssh-ssl-cost-firms-big-money-report).

[7] In the publishing, media and entertainment, and services industries, and across many other verticals, fewer and fewer companies deliver their products as physical assets such as printed reports, books, or magazines. Instead, these assets are created, stored, and accessed as digital content. In the following report, Forrester guides security and risk professionals through governance best practices and tools and vendors' solutions to combat digital asset overuse. For more information, see the June 30, 2014, "Protect Your Digital Assets — Without Driving Customers Away" report.

[8] Every day, vendors introduce a new product or service that claims to be the silver bullet to data security challenges. To avoid the hype and take a holistic and long-lasting approach to data security that encompasses people, processes, and technology, we developed Forrester's Data Security And Control Framework. The following TechRadar™ assesses 20 of the key traditional and emerging data security technologies that S&R leaders and their staff can use to underpin the best practices and recommendations of our framework. For more information, see the April 22, 2014, "TechRadar™: Data Security, Q2 2014" report.

[9] S&R pros must work in a complex ecosystem of powerful customers increasingly concerned about their privacy, digitally native employees, and potentially hundreds of demanding partners and suppliers — all perpetually connected by new systems of engagement and cloud services. In this new reality, traditional perimeter-based approaches to security are insufficient. S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model. For more information, see the June 5, 2014, "The Future Of Data Security: A Zero Trust Approach" report.

[10] Intralinks acquired docTrackr in 2014 for this purpose. Box points to IRM as one of its strategic advanced security investments. IRM capabilities have been a key differentiator for WatchDox as well. Source: Romain Dillet, "Intralinks Acquires Document Security Service docTrackr," TechCrunch, April 24, 2014 (http://techcrunch.com/2014/04/24/intralinks-acquires-document-security-service-doctrackr/) and Whitney Bouck, "#BoxWorks: True Enterprise Collaboration Needs a Next-Gen Content Platform," Box blog, September 4, 2014 (https://blog.box.com/2014/09/boxworks-true-enterprise-collaboration-needs-a-next-gen-content-platform/).

[11] Content Raven announced new marketing analytics capabilities in 2014 to complement its existing secure content sharing and distribution business. Vobile acquired Blayze Consulting for video analytics capabilities to enter the YouTube content management space. Source: Nathan Eddy, "Content Raven Lauches Marketing Analytics Tool," eWeek, September 5, 2014 (http://www.eweek.com/small-business/content-raven-launches-marketing-analytics-tool.html) and Alan Van, "Vobile Set to Enter Youtube Content Rights Management Market with Acquisition of Blayze," New Media Rockstars, March 6, 2014 (http://newmediarockstars.com/2014/03/vobile-set-to-enter-youtube-content-rights-management-market-with-acquisition-of-blayze/).

[12] Source: "Data Disposal Laws," National Conference of State Legislatures, December 26, 2013 (http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx).

[13] Source: CyberFactors (http://cyberfactors.com/).

[14] Source: CyberFactors (http://cyberfactors.com/).

[15] Source: Micheal Mahoney, "Medical records found blowing in wind near health clinic," KMBC-TV, May 20, 2014 (http://www.kmbc.com/news/patient-records-found-outside-research-medical-center/26071174).

[16] The individual who purchased the servers attempted to ransom the data in addition to putting it up for sale (and receiving bids supposedly of over $1 million) before an agreement was made where Ernst & Young would pay him $1,500 per day to cooperate with data inspection. Source: Lisa Vaas, "Man buys old servers, accuses Ernst & Young of data breach," Naked Security, September 16, 2014 (http://nakedsecurity.sophos.com/2014/09/16/man-buys-old-servers-accuses-ernst-young-of-data-breach/).

[17] To help security and risk professionals navigate the complex landscape of privacy laws around the world, Forrester created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. For more information, see the August 6, 2014, "Forrester's 2014 Data Privacy Heat Map" report.

[18] Forrester combined three data sources to capture a comprehensive, 360-degree view of US online adults' evolving attitudes on privacy. By blending Consumer Technographics® survey data, qualitative insights from our ConsumerVoices market research online community (MROC), and social listening data, the following report tracks the changes in consumer perceptions and provides firsthand accounts of how individuals expect their data to be used by the firms with which they do business. For more information, see the July 28, 2014, "Evolving Consumer Attitudes On Privacy" report.

[19] Like other tech giants, Apple wants to assure concerned customers around the world that it doesn't willingly participate in or condone widespread government surveillance efforts. For more information, see the October 1, 2014, "Brief: Apple Throws Down The Privacy Gauntlet" report.

[20] Today, 30% of security decision-makers agree that privacy is a competitive differentiator and 66% of security decision-makers say they are mostly or fully responsible for privacy in their organizations. For more information, look for our upcoming "Understand The State Of Data Security And Privacy: 2014 To 2015" report.

[21] Source: European Data Protection Supervisor (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/DPO).

[22] Source: Ellen Messmer, "Does your business need a 'Data Protection Officer?'" Network World, August 8, 2014 (http://www.networkworld.com/article/2462855/security0/does-your-business-need-a-data-protection-officer.html).

[23] Since the chief information security officer (CISO) must work hand in hand with the CPO, S&R executives must help define the role responsibilities and job description and play a major role in candidate selection.

[24] Since the revelations from news of the NSA scandal, more consumers feel more empowered when it comes to protecting their privacy and are increasingly taking privacy matters into their own hands. To protect their personal data, the three most common steps consumers now take are the following: 1) changing the privacy settings on their social network account; 2) installing privacy protection tools (e.g., AdBlock); and 3) changing their mobile phone provider. For more information, see the July 28, 2014, "Evolving Consumer Attitudes On Privacy" report.

[25] Ultimately, consumers are willing to accept a certain level of risk for a perceived benefit. For example, while privacy and security are concerns, usability and reliability are better indicators for successful adoption of mobile authentication technologies. For more information, see the September 17, 2014, "Transform And Protect Your Customers' Mobile Moments With Seamless Authentication" report.

[26] Source: In 2013, TrendNet settled with the FTC after it was found that the company's consumer home surveillance cameras were susceptible to attack due to improper authentication measures. Source: Federal Trade Commission (http://www.ftc.gov/).

[27] The wearables market suffers from a hype bubble: The ratio of released products to product sales is currently very high. But wearables are for real. Forrester surveyed 4,566 US online consumers and interviewed 25 companies to understand the demand — today and tomorrow — for wearable devices. For more information, see the October 21, 2014, "Wearables Drive Innovation By Addressing Fundamental Human Needs" report.

[28] Fitness wearables enjoy the lion's share of publicity for their consumer market offerings today, but they're coming soon to an enterprise near you. Employee wellness factors into business success via multiple dimensions — with even CEOs playing a role. Companies will be investigating the role that health and fitness wearable technology can play in driving worker productivity up and health insurance rates down. For more information, see the January 6, 2014, "Building A Fitter Business With Wearable Technology" report.

[29] Source: Parmy Olson, "Wearable Tech Is Plugging Into Health Insurance," Forbes, June 19, 2014 (http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance).

[30] Source: Ben Heubl, "When Wearable Health Trackers Meet Your Doctor," TechCrunch, August 6, 2014 (http://techcrunch.com/2014/08/06/wearable-health-trackers-should-you-show-your-doctor/).

[31] Whether you're thinking about wearables for use by customers or employees, infrastructure and operations professionals must plan for the privacy ramifications. In the following report, we assess the state of wearables privacy using quantitative data from Forrester's Consumer Technographics® surveys, then lay out five steps you can take when beginning to pilot wearable solutions. For more information, see the August 1, 2014, "Five Ways To Navigate Privacy Issues In Wearable Computing" report.

[32] Source: “Current Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934,” US Securities and Exchange Commission, August 18, 2014 (http://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm).

[33] Source: Robert Lowes, “Stolen HER Charts Sell For $50 Each On Black Market,” Medcape Medical News, April 28, 2014 (http://www.medscape.com/viewarticle/8241).

[34] For the past few years, China’s health costs have been outpacing its GDP growth rates and, along with the growing environmental problems in the country, the government is vastly behind the times when it comes to treatments for diseases like lung cancer, stomach cancer, and asthma. Cyber breaches may be one way to leapfrog ahead of their current capabilities for a population whose health problems are costing the government tens of billions of dollars.

[35] Source: Jason Beaubien, “Cancer Cases Rising At An Alarming Rate Worldwide,” National Public Radio, February 4, 2014 (http://www.npr.org/blogs/health/2014/02/04/271519414/global-cancer-cases-rising-at-an-alarming-rate-worldwide).

[36] As the threat landscape continues to evolve, S&R leaders must adjust their risk management strategies to also counter the next frontier: intellectual property theft. For more information, see the August 6, 2014, “The Cybercriminal’s Prize: Your Customer Data And Competitive Advantage” report.

[37] Source: US District Court Criminal Complaint United States of America versus Jun Xie (http://media.jrn.com/documents/gecomplaint.pdf).

[38] Currently there is significant growth in unplanned cloud deployments. Business leaders with spending authority are short-circuiting the information technology procurement cycle and purchased cloud-based solutions at a record rate without necessary due diligence on the security of these environments.

[39] A perceived lack of security has been one of the more prominent reasons organizations cite for not adopting cloud services. However, this attitude is changing rapidly as cloud service providers (CSPs) begin to offer comprehensive security capabilities. For more information, see the August 2, 2013, “Security’s Cloud Revolution Is Upon Us” report.

[40] Source: Nicole Perlroth and David Gelles, “Russian Hackers Amass Over A Billion Internet Passwords,” The New York Times, August 5, 2014 (http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0).

[41] Source: Michael Corkery, David E. Sanger, and Jessica Silver-Greenberg, “Obama Had Security Fears on JPMorgan Data Breach,” The New York Times, October 8, 2014 (http://dealbook.nytimes.com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/).

[42] Source: Kelly Jackson Higgins, “ISIS Cyber Threat To US Under Debate,” Dark Reading, September 23, 2014 (http://www.darkreading.com/vulnerabilities—-threats/advanced-threats/isis-cyber-threat-to-us-under-debate/d/d-id/1316004).

Forrester Research (Nasdaq: FORR) is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Our clients face progressively complex business and technology decisions every day. To help them understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. We guide leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow.