Understand The State Of Data Security And Privacy: 2015 To 2016

Benchmarks: Data Security And Privacy Playbook

by Heidi Shey

January 8, 2016

Why Read This Report

Throughout the year, Forrester analysts engage in hundreds of discussions about data security and privacy. This data-driven report outlines budgeting and spending, technology adoption plans, and other key breach, data protection, and privacy trends in North American and European firms for 2015 through 2016. Understanding these trends and their implications will help security and risk (S&R) executives examine, and adjust as necessary, their own resource allocation for data security and privacy.

Key Takeaways

Insiders Continue To Cause And Contribute To Data Breaches

Internal incidents top the list of breach causes in 2015. Even with external attacks, a common link is attackers targeting and taking advantage of insiders.

Old And New Data Security Technologies Will See Growth In 2016

Data security consumes the third largest portion of the security technology budget, behind network security and client threat management. DLP, cloud encryption, key management, archiving, managed file transfer, and email encryption are notable technologies on S&R pros' agendas.

Focus On People, Not Just Technology, For Data Security And Privacy

There is an arsenal of tools and technologies available today that can help protect data. S&R pros must look beyond technology to focus on people and their behaviors: the board, security staff, employees, third-party partners, and customers. Re-engage the human firewall to uplift data security and privacy efforts.

Understand The State Of Data Security And Privacy: 2015 To 2016

Benchmarks: Data Security And Privacy Playbook

by Heidi Shey
with Stephanie Balaouras, Alex Spiliotes, and Peggy Dostie

January 8, 2016

Table Of Contents

Notes & Resources

Forrester analyzed data from Forrester's Global Business Technographics® Security Survey, 2015 for this report.

Related Research Documents

The Cybercriminal's Prize: Your Customer Data And Intellectual Property

The Future Of Data Security And Privacy: Growth And Competitive Differentiation

FORRESTER®

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

Human Behaviors And Motivations Render Data Loss Inevitable

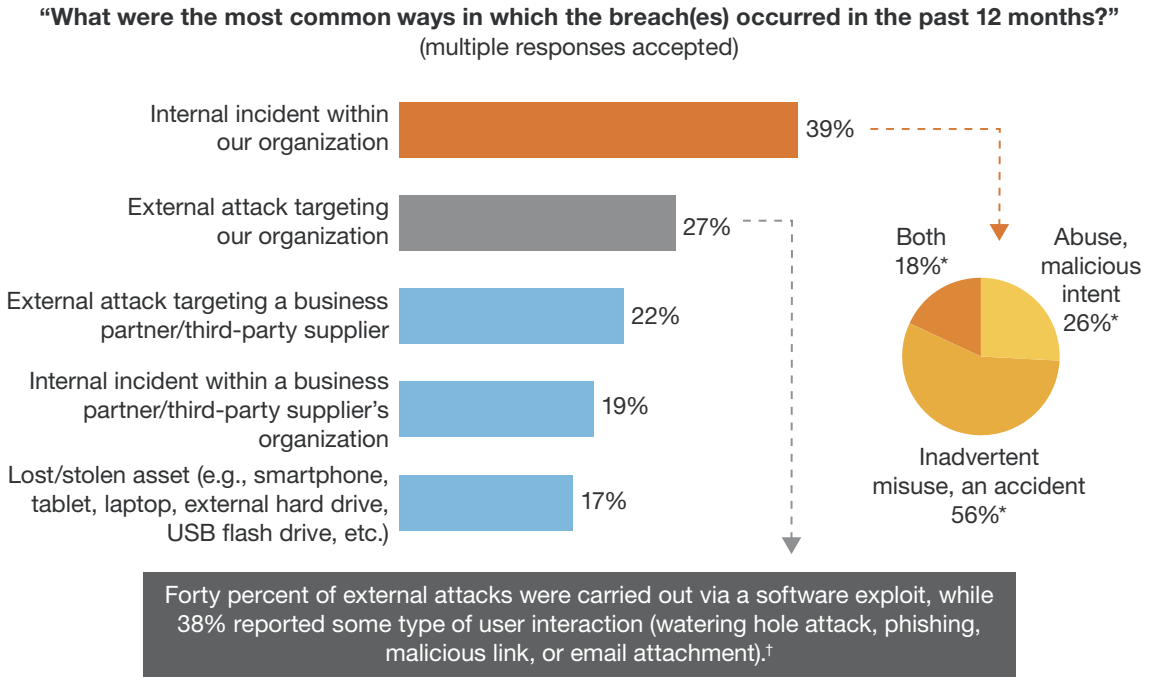
Data breaches continue to plague organizations and feed news headlines. Anthem, Ashley Madison, Sony Pictures, The Republic of Turkey, Topface, and the US OPM are a few among many that have disclosed breaches in the past year. Chances are there are many more compromised organizations that are also leaking data unknowingly. Forrester's Global Business Technographics Security Survey, 2015, shows that in firms had experienced a breach in the past 12 months, the top three most common ways in which breaches occurred were internal incident within their organization (39%), external attack targeting their organization (27%), and external attack targeting a business partner/third-party supplier (22%) (see Figure 1).[1] These numbers aren't surprising given that:

- **Cybercriminals and nation-state-sponsored attackers see your data as a goldmine.** In 2015, the top two data types compromised in a breach were personally identifiable information (PII) and authentication credentials (see Figure 2).[2] For cybercriminals, authentication credentials provide the keys to the kingdom. The underground market for cardholder data, PII, personal health information (PHI), and intellectual property (IP) provide huge incentives with low barriers to entry.[3] Cybercriminals are increasingly extorting firms and individuals by taking data hostage via ransomware in broad, opportunistic attacks.[4] State-sponsored attackers value sensitive corporate and government data.
- **Fraudsters will take advantage of employees trying to do their jobs.** Fraudsters are breathing new life into business email compromise and wire transfer scams, also known as CEO fraud, in which a fraudster poses as an executive and directs employees to transfer funds.[5] Many firms don't implement user security awareness and training adequately or effectively, making themselves susceptible to scams like this one.[6] In Forrester's 2015 study of information workers across SMBs and enterprises, only 39% of the North American and European workforce indicated that they had received training on how to stay secure at work, and only 53% say they are aware of their organization's current security policies.[7]
- **Hacktivists see your data as a pawn for their protest.** Everything from customer data to sensitive corporate information (hello email) is fair game for hacktivists intent on making a statement. Whether they're protesting your business practices or indirectly linking your firm to a larger cause, this is an opportunity to expose data and embarrass your organization.
- **Employees have access to data but don't always know or understand use policies.** In 2015, 56% of internal incidents were due to inadvertent misuse or an accident.[8] Today, 51% of North American and European information workers are aware of or understand the policies that are specific to data use and handling inside their company. This is not simply about awareness. It's a more deeply rooted issue: the firm's basic lack of knowledge about the data in use, overly complex classifications (if they even exist at all), and subsequent ineffective (or unenforceable) data-use policies.[9]

› **Third parties and contractors widen the attack surface.** Third parties and trusted business partners can maneuver into systems undetected and without setting off any alarms. Cybercriminals also use third parties as stepping stones into a targeted company. By infiltrating and infecting a trusted partner's network or compromising its credentials, cybercriminals can move laterally through the environment, wreaking havoc.[10]

› **S&R pros lack confidence in their own programs.** Less than half of S&R pros are confident in their organization's ability to protect data today.[11] There are just too many vectors and issues for S&R pros to keep up with. Confronting the sprawling threat landscape with limited resources can be a harrowing task. As the business pushes on with the motivation to use all types of technologies to further their organization's position, S&R pros are left to wonder, "What can and should I protect first?"

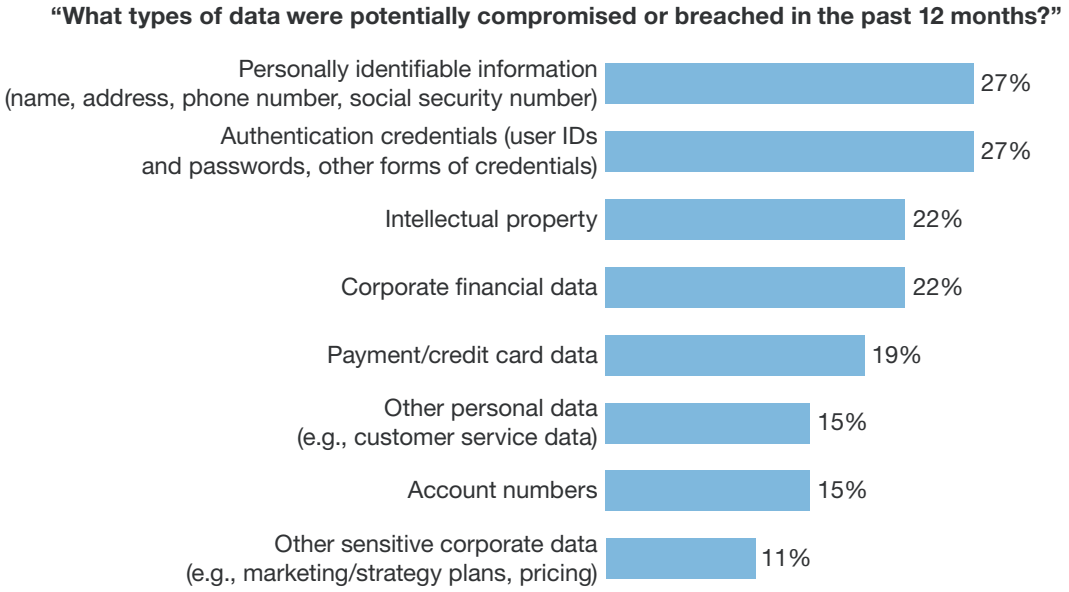
FIGURE 1 Internal Incidents Are A Common Cause Of Breach



Base: 358 North American and European network security decision-makers who have experienced data breaches in the past 12 months (20+ employees)
*Base: 184 North American and European network security decision-makers who have experienced the specified breaches (20+ employees)
†Base: 156 North American and European network security decision-makers who have experienced the specified breaches (20+ employees)

Source: Forrester's Business Technographics® Global Security Survey, 2015

FIGURE 2 PII And Authentication Credentials Are The Top Two Targets



Base: 358 North American and European network security decision-makers who have experienced data breaches in the past 12 months (20+ employees)

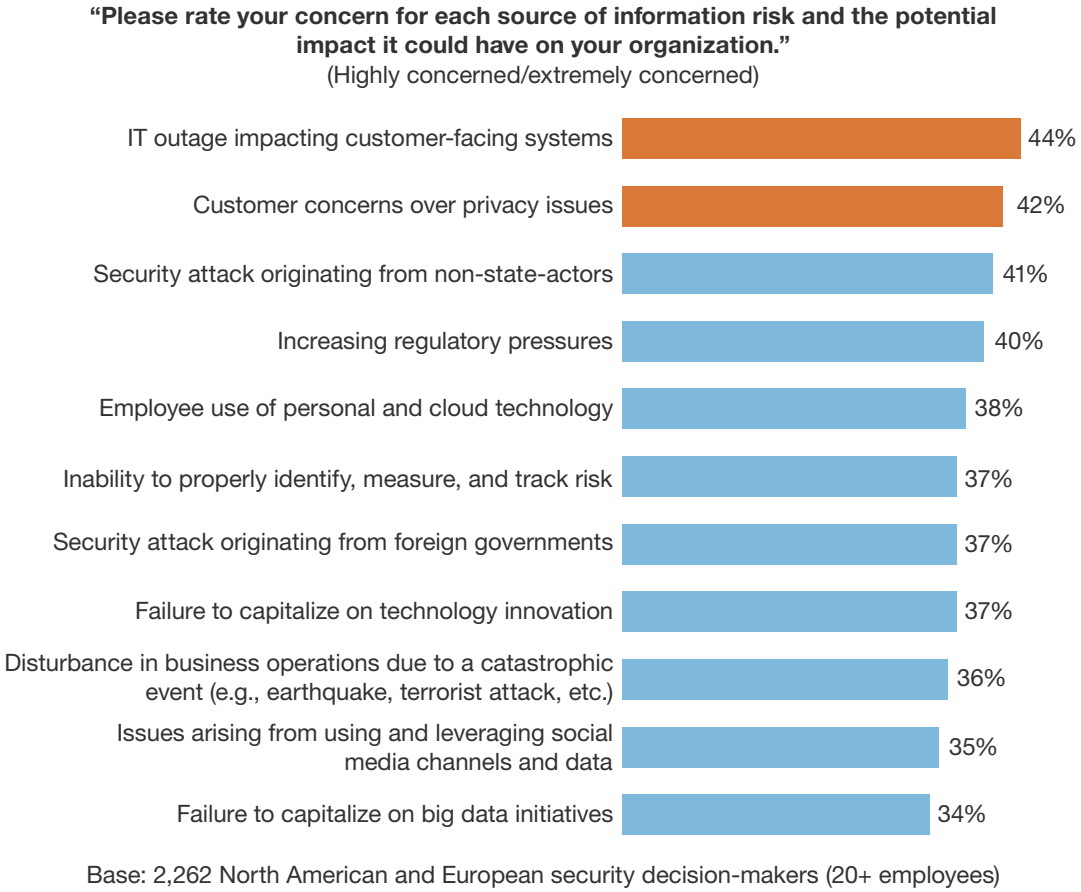
Note: 11% of those who have experienced a breach did not know what types of data were compromised in the incident.
Source: Forrester's Business Technographics® Global Security Survey, 2015

Safeguarding The Customer Experience Is Essential For Building Trust

In the age of the customer, S&R pros are expected to be active in helping the business meet customer demands and expectations. This customer-first focus is essential to building trust. A recent study on the future of data-sharing from the Columbia Business School and Aimia demonstrated that consumers' trust in a brand influences the types of data they're willing to share.[12] As businesses strive to turn data into action via digital insights (finding meaning in customer, product, and business environment information), S&R pros must help protect the brand's reputation and safeguard the customer experience.[13]

IT outages impacting customer-facing systems and customer concerns over privacy issues are at the top of the list of concerns for S&R pros today (see Figure 3). S&R pros have a direct impact on customer experience when it comes to: 1) protecting customer data; 2) enforcing data privacy policies; and 3) creating and regularly testing incident response plans (which include many customer-facing aspects like communications and breach notification, too).

FIGURE 3 Customer Experience And Concerns Are Top Of Mind Alongside Regulatory Pressures



Base: 2,262 North American and European security decision-makers (20+ employees)

Source: Forrester's Business Technographics® Global Security Survey, 2015

Privacy Is A Business Differentiator And A Challenge

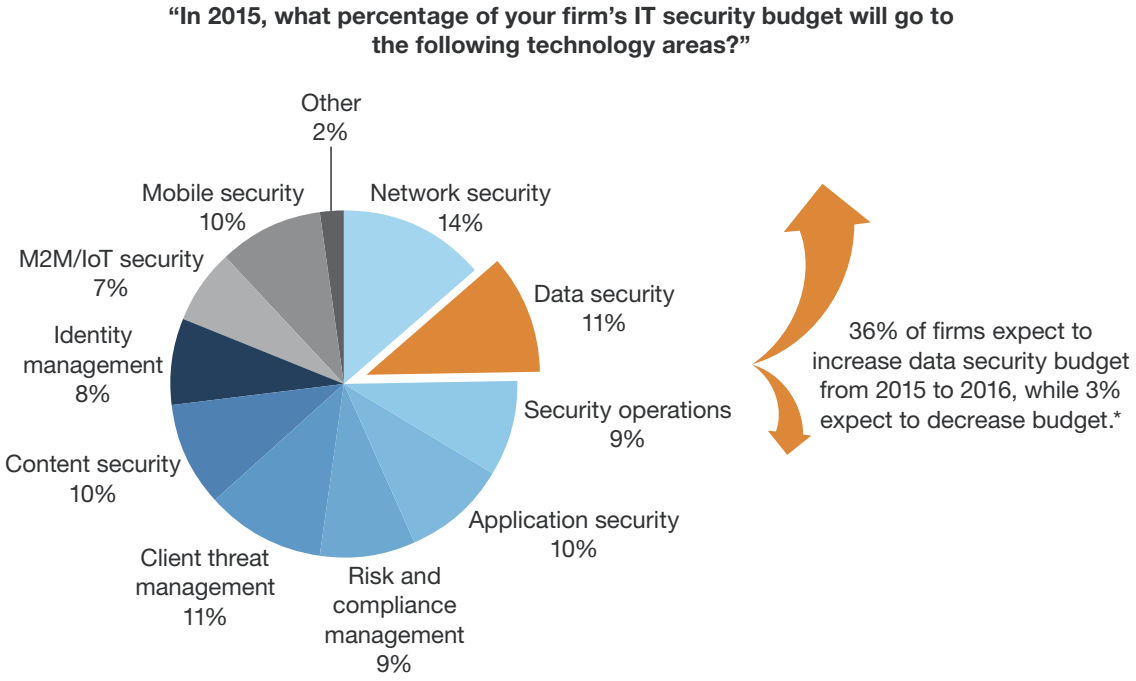
Today, 23% of security decision-makers agree that privacy is a competitive differentiator, and 69% of enterprise security technology decision-makers say that their security group is mostly or fully responsible for privacy in their organizations.[14] The shouldering of privacy and regulatory responsibility by the security group is more pronounced in smaller enterprises in North America. Larger organizations are more likely to face widespread pain and have requirements that necessitate the hiring of a privacy officer (or several!) to take the lead on privacy. However, breaches of trust from privacy infringements or data leakage can severely damage the brand, lead to customer backlash, and incur regulatory scrutiny and hefty fines. In the end, S&R pros must deal with privacy whether they like it or not because the blame will often fall on them; 68% of security decision-makers say they are at least partly responsible for protecting customers' personal information from privacy abuses.[15] The privacy picture gets ugly when a firm:

- **Attempts to align with the patchwork of privacy regulations.** The global privacy legal landscape is a bumpy and thorny one due to the plethora of privacy laws and the lack of harmonization within and across countries.[16] It is one (major) step to first understand how the rules work, and another (much larger) step to implement and align an organization's business practices with often conflicting laws.[17]
- **Uses cloud services.** The use of cloud has many benefits, such as reduced cost and increased efficiency. But handing over application and data assets to a cloud provider introduces a range of risks to data location, data handling, eDiscovery, the shared multitenant environment, and security breach response policies.[18] Firms increasingly turn to third-party cloud security solutions for help. Today, Forrester sees solutions converging around four categories: cloud data protection, cloud governance, cloud access security intelligence, and centralized cloud workload security management.[19]
- **Transfers data between partners.** Data is the lifeblood of business in today's digital economy. Companies must provide access to data to those who need it in order to do their jobs as well as do business with their organization. It's paramount to insure that the data is accessed by the right people, moves and flows to where it's required, and is used appropriately while it is protected. Today, 66% of security decision-makers say they are at least partly responsible for ensuring the security and privacy of customer data sold to or exchanged with partners.[20]
- **Assumes that good security equates to good privacy.** Privacy does not begin and end with security; security is only one aspect of privacy.[21] Ensuring good privacy practices requires a union of technology, policy, and corporate culture; it also requires harmony between many business units, from security to legal to HR to employees. As an organization's data use, privacy considerations, and regulatory requirements collide — resulting in a war between such business requirements as advancing big data initiatives, changing consumer attitudes about data privacy, and evolving privacy laws —a dedicated privacy officer and support staff will need to give the privacy program their full attention.

Data-Centric Security Is A Business Imperative

Data security takes up the third largest portion of the security technology budget (11%) in 2015, and 36% of firms have plans to increase spending here from 2015 to 2016 (see Figure 4). Currently, 54% of security decision-makers say adopting a data-centric approach to security is a high or critical IT security priority over the next 12 months.[22] Data security is a business imperative, and one that now has the attention of the board of directors. If conversations about data security were not happening before, they are now. Forty-seven percent of security decision-makers indicate that recent high-profile cyberattacks on IT security have raised the awareness of their executives.[23] As executives see more and more media coverage of data breaches and security incidents, the big question they'll be asking is: "What are we doing to make sure that doesn't happen to us?"

FIGURE 4 Data Security Takes 11% Of The Security Tech Budget In 2015



Base: 1,036 North American and European security technology decision-makers with budget authority (20+ employees)
*Base: 2,262 North American and European security decision-makers (20+ employees)
(percentages do not total 100 because of rounding)

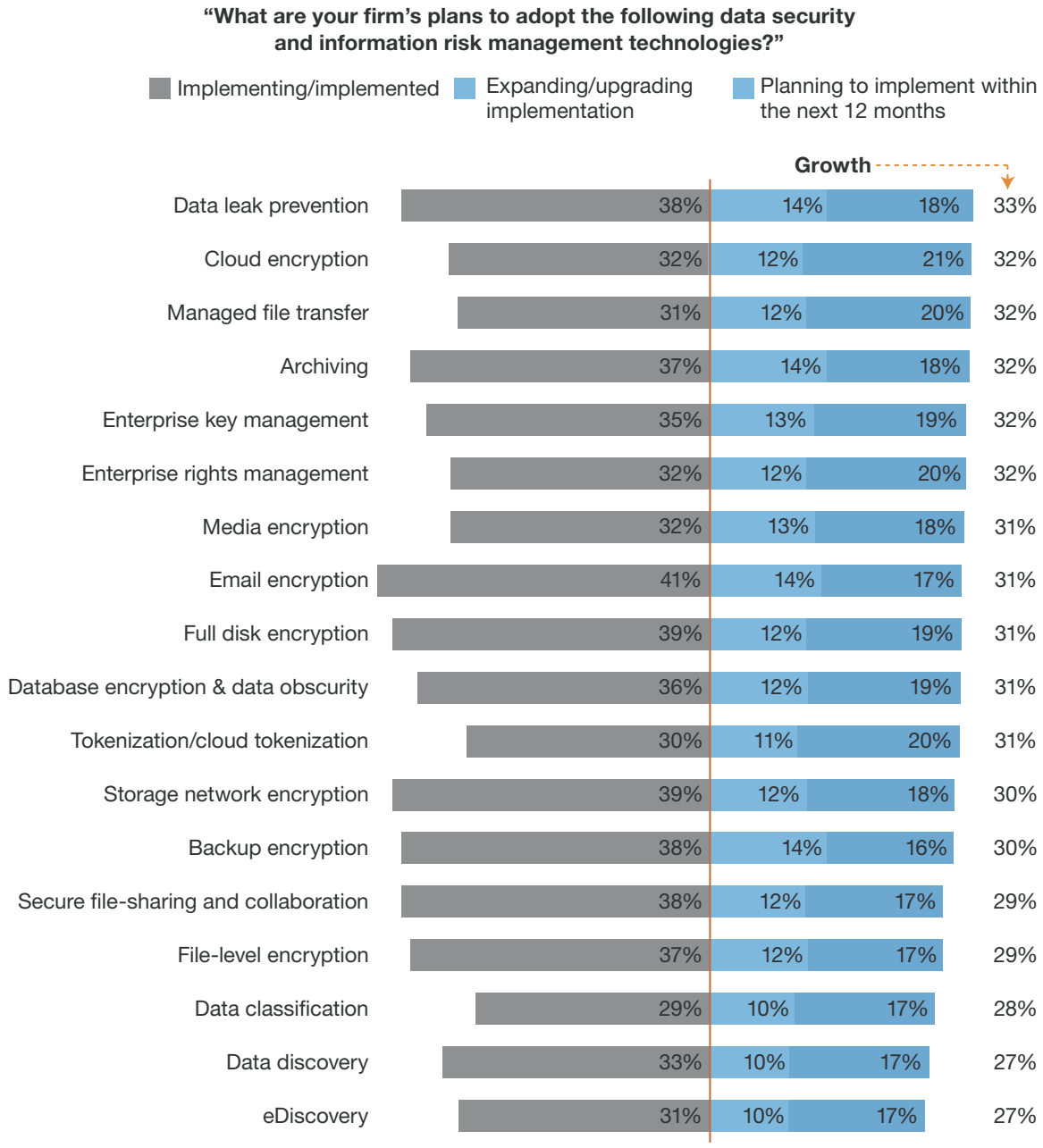
Source: Forrester's Business Technographics® Global Security Survey, 2015

Core Data Security Technologies Are All In Demand In 2016

Data security technologies that apply protections *directly* to the data itself or to the application that stores and provides access to the data, or that enable the critical processes that we have outlined in Forrester's data security and control framework, are in healthy demand today.[24] Few differences exist when we consider the overall picture of implemented solutions versus future plans to implement or expand and upgrade current implementations. There is growth to come across these technologies, and no one solution type stands head and shoulders above the rest. However, when we take a closer look, the very minor differences in demand that do emerge illustrate several hot technologies that S&R pros have their eyes on for 2016 (see Figure 5):

- **DLP is one of the most-wanted technologies.** Thirty-three percent of companies are looking to either adopt a new implementation or add investment to a current implementation of DLP. While DLP remains an important tool for defense, organizations run into trouble when they think of DLP as a product instead of a function and don't have a process or holistic data protection strategy in place before they start making investments here.[25]
- **Email encryption has a solid user base that will continue to grow.** Email encryption is one of the more popular data security technologies, thanks to compliance requirements: 41% of client security decision-makers say their firms have implemented or are implementing email encryption. In 2016, another 31% have plans to implement or invest more in their existing implementation.[26] The onus to protect sensitive email and corporate communications will continue to contribute to email encryption's popularity beyond compliance-driven mandates.
- **Stalwarts like archiving and managed file transfer see renewed interest.** Exploding data volumes, renewed focus on the data life cycle, and defensible data deletion, along with legal data retention requirements, spur firms to take a closer look at their data archiving strategy and supporting tools. Thirty-two percent of client security decision-makers have plans in 2016 to take action here.[27] Managed file transfer, the backbone for secure and automated B2B data transfer, sees renewed interest as companies enter a cycle of upgrading and replacement for existing solutions to better meet current (and anticipated future) business needs.
- **Cloud encryption and enterprise key management shine due to privacy concerns.** The cloud is here and it's not going away. Cloud encryption and control over encryption keys are on the agenda for S&R pros concerned about unauthorized third-party (government as well as vendor) access to their data in the cloud. Close to a third of organizations plan to implement or invest more in cloud encryption and key management in 2016.

FIGURE 5 DLP, Cloud, And Email Encryption Solutions Are High On The Wish List



Base: 770 North American and European client security decision-makers (20+ employees)
Source: Forrester's Business Technographics® Global Security Survey, 2015

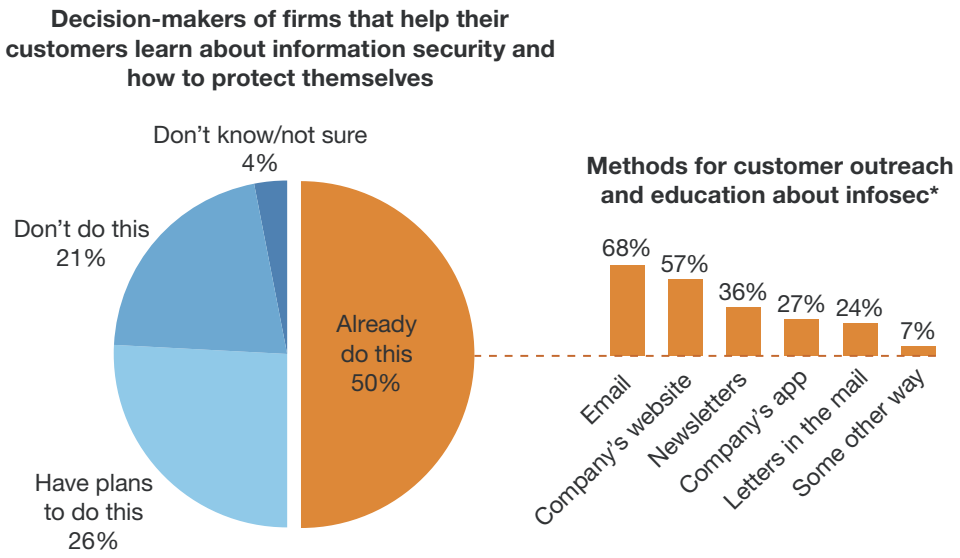
Your Efforts Depend On People, Not Just Technology

Investing in people is just as important as investing in technology and tools for data security and privacy. We're all human and will make mistakes, as clearly evidenced by the volume of breaches caused by accident or uninformed data-handling. All the training in the world can't entirely eliminate human error, but it can at least help reduce the number of incidents that human error causes. Focus on:

- **The board of directors.** Cybersecurity and data protection are top of mind for corporate boards across all industries today, but that doesn't necessarily mean that the board understands security. If anything, they're eager to learn and eager for answers. S&R pros must take the opportunity to educate and rally the board's support for data security and privacy initiatives for both funding the budget and for setting the tone for cybersecurity efforts in the organization.[28]
- **Security staff.** What's being done to prevent burnout and create growth opportunities for security staff?[29] Currently, 40% of security technology decision-makers say that their organization plans to increase opportunities for security skills training over the next 12 months to attract and retain talent.[30] Attrition is a concern for a number of reasons. Best case scenario: A skilled security employee finds a growth opportunity elsewhere and your organization is faced with the time and cost of hiring a replacement. Worst case scenario: Security staff leave because they're fed up with organizational roadblocks that prevent them from applying their skills, and they want out before a breach inevitably occurs and they become the scapegoats.
- **Employees.** They create, collect, and handle sensitive data as a part of their job. It's imperative that employees understand the implications of improper data use and collection practices, as well as what constitutes appropriate and secure data-handling and online behavior. Rolling out effective security training and awareness for employees across the organization is a critical or high priority for 57% of security technology decision-makers today.[31] As the resident experts, S&R pros must lead the charge when it comes to instilling basic security and privacy concepts and behaviors in employees. The goal is not simply security awareness, but a change toward security-minded behavior.[32]
- **Third-party partners and suppliers.** Businesses don't operate in a vacuum, and third-party partners and suppliers are insiders, too, given their ties and access to the organization. Clearly outline the security and breach response responsibilities for each party in advance, and identify your organization's security requirements that must be met as a condition of the business relationship. Carefully control and monitor all third-party access to data and systems. Ask what your partners and suppliers do to ensure that their staff understand how to handle data and access, and know when and whom they should alert in the event that they suspect something is awry.
- **Customers.** Customers that do business with your organization share their data with the expectation that you will protect it. But there's more that S&R pros can do here for customers too. Today, 50% of security decision-makers indicate that their organizations help educate their customers about information security and how to protect themselves (see Figure 6). Email (68%) is the most common way of customer outreach, followed by messages on the website (57%) and

newsletters (36%). Identify the outreach medium that best suits your customers as a channel to engage about security- and privacy-minded behaviors. Help them help themselves — and your organization in the process — and use these educational opportunities as additional touchpoints for customer engagement.

FIGURE 6 Half Of Organizations Are Helping To Educate Customers About Infosec



Base: 2,262 North American and European security decision-makers (20+ employees);
*Base: 1,127 North American and European security decision-makers who educate their customers about informations security
(percentages do not total 100 because of rounding)

Source: Forrester's Business Technographics® Global Security Survey, 2015

What It Means

Use Benchmarks As A Starting Point For Your Own Analysis

The data shown in this report provides a view of what North American and European SMBs and enterprises are spending and doing today for data security. However, each organization is unique due to its size, industry, long-term business objectives, and tolerance for risk. While it's helpful to see what other firms may be spending and doing, it's critical that you don't become a slave to the data. Consider this benchmark a guide, where the key trends and takeaways seen can serve as a starting point for analysis of your own budget and technology adoption plans for data security and privacy.

Based on what Forrester sees as data security trends for 2015 to 2016, S&R pros must:

- **Evaluate how S&R is increasingly a customer-facing, people-oriented role.** S&R helps to enable a secure customer experience, addresses and assuages customer concerns in a timely manner with clear communication as a part of incident response, and assists with engaging and educating customers about security- and privacy-minded behaviors. It's now more important than ever to focus on people: the board, security staff, employees, third-party partners and suppliers, and customers.
- **Balance your investments to address upcoming concerns in addition to the basics.** DLP remains a hot must-have security technology across many organizations. S&R pros are also trying to balance addressing pressing cloud and email security and privacy concerns with reevaluating the basics for a data-centric approach to security and securing the data life cycle.
- **Reassess S&R responsibilities for privacy.** It's encouraging that S&R pros continue to pay attention to creating a holistic data control strategy. An area of caution, and one to watch, will be privacy responsibility. Although the security group should undoubtedly be a core stakeholder and contributor to privacy initiatives and responsibility within organizations, it may not necessarily be in the best position — in terms of focus and resources — to lead and take full responsibility for privacy.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

Supplemental Material

Survey Methodology

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. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Endnotes

[1] For the purposes of this report, Forrester analyzed the Global Business Technographics Security Survey, 2015 responses of only North American and European network security decision-makers at companies with 20 or more employees.

[2] And, unfortunately, 11% of security decision-makers simply do not know what types of data were compromised from incidents at their organization. This is problematic for many reasons. Was intellectual property stolen? What about customer data? In case of the latter, companies may find themselves running up against breach notification laws as a result. Source: Forrester's Global Business Technographics Security Survey, 2015.

[3] For more information on cybercriminals and the cost of stolen data, see the "The Cybercriminal's Prize: Your Customer Data And Intellectual Property" Forrester report.

[4] Source: Kim Zetter, "Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise," Wired, September 17, 2015 (http://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/).

[5] This type of scam has been reported in all 50 US states and 70 countries. The US Federal Bureau of Investigation estimates that fraudsters have stolen $1.2 billion from this type of scam between October 2013 and December 2014. Source: Brian Krebs, "FBI: $1.2B Lost to Business Email Scams," Krebs on Security, August 27, 2015 (http://krebsonsecurity.com/2015/08/fbi-1-2b-lost-to-business-email-scams/).

[6] The goal of an awareness and training effort should not be distribution of information, but driving behavioral change. Three factors play a role in behavioral change: motivation, ability, and triggers. You shouldn't be thinking about simply creating an "awareness campaign" but an ongoing behavioral program that continues throughout every employee's time with the organization. This report takes lessons from CISOs who have both failed and succeeded, and from a variety of marketers and vendors, to outline a new way to approach what has for too long been a stale and stagnant practice; a new way to engage the human firewall. See the "Reinvent Security Awareness To Engage The Human Firewall" Forrester report.

Focus metrics on core elements of behavior — motivation, ability, and triggers — to assess environmental indicators to measure results. This report takes lessons from CISOs, marketers, and vendors, to propose a new way of measuring the human firewall, one that focuses on behavioral change as the cornerstone of a successful security program. See the "Measuring Security Awareness To Enhance The Human Firewall" Forrester report.

[7] Source: Forrester's Global Business Technographics Devices And Security Workforce Survey, 2015.

[8] Source: Forrester's Global Business Technographics Security Survey, 2015.

[9] Too often, organizations create data policies without a clear understanding of feasibility and purpose within their business because they themselves are in the dark about their data — from what data they have to where it resides. As a result, many data security policies are ineffective and can even hinder business processes. In today's evolving data economy, data identity is the missing link that security and risk (S&R) leaders must define in order to create actionable data security and control policy. We designed this report to help S&R leaders develop effective policies using our data security and control framework as a guideline. See the "Know Your Data To Create Actionable Policy" Forrester report.

[10] We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily bypass current security protections. To help S&R professionals eliminate the soft chewy center that exposes the organization, Forrester has developed the Zero Trust Model of information security. For more information, see the "No More Chewy Centers: The Zero Trust Model Of Information Security" Forrester report.

[11] Source: Forrester's Global Business Technographics Security Survey, 2015.

[12] Source: "What Is the Future of Data Sharing?" Columbia Business School, October 2015 (https://www8.gsb.columbia.edu/globalbrands/research/future-of-data-sharing).

[13] Demanding customers and competitive pressures require firms to treat insights — not just data — as a business asset. Forrester's research into incumbents like Ford Motor, General Electric (GE), and USAA as well as digital insurgents like Netflix and LinkedIn found that these leaders are fusing a new business discipline with technology to create "systems of insight." See the "Digital Insights Are The New Currency Of Business" Forrester report.

[14] Source: Forrester's Global Business Technographics Security Survey, 2015.

[15] Source: Forrester's Global Business Technographics Security Survey, 2015.

[16] 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. Due to the dynamic nature of data protection legislation, information within the interactive tool is kept up-to-date with an annual update cycle. See the "Forrester's 2015 Data Privacy Heat Map" Forrester report.

[17] How companies handle and protect consumer data privacy is much more than a compliance issue. Privacy is a competitive differentiator, and firms that fail to have a cohesive privacy strategy and program will struggle to succeed at best and be a ticking time bomb for customer outrage at worst. This requires oversight and clear lines of privacy responsibility and accountability; S&R pros can't tackle this alone and must partner with their business peers. See the "Build A Privacy Organization For Consumer Data Management" Forrester report.

[18] Security and risk professionals need to provide a way of securely connecting to cloud services and infrastructure (security to the cloud); they need to validate the security posture of their cloud providers' environment (security in the cloud); and they need to apply effective controls for on-premises applications using cloud services (security from the cloud). And because empowered business owners can procure their own services without IT's involvement, it's critical that you build strong relationships with the business to ensure they consult you during cloud service procurement decisions and negotiations. This report explains the process and technology challenges as well as best practices for implementing security to, in, and from in the cloud. See the "An S&R Pro's Guide To Security To, In, And From The Cloud" Forrester report.

[19] As enterprises embrace a diverse cloud ecosystem, a new generation of software is emerging to address the security requirements of highly distributed IT infrastructure. These new offerings make up for the missing features of perimeter-based security solutions in their ability to discover, analyze, and control corporate data across bare metal, virtual machines, IaaS, PaaS, and SaaS, and are rapidly maturing into an independent category Forrester calls cloud security solutions. See the "Sizing The Cloud Security Market" Forrester report.

[20] Source: Forrester's Global Business Technographics Security Survey, 2015.

[21] The Organisation for Economic Co-operation and Development (OECD) developed a set of guidelines to help "harmonize" the disparities in national privacy regulations being enacted across the EU. Source: "The OECD Privacy Framework," OECD (http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf).

[22] Source: Forrester's Global Business Technographics Security Survey, 2015.

[23] Source: Forrester's Global Business Technographics Security Survey, 2015.

[24] Forrester has created a framework to help security and risk professionals control big data. We break the problem of securing and controlling big data down into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data. See the "The Future Of Data Security And Privacy: Growth And Competitive Differentiation" Forrester report.

[25] DLP is a key tool to help prevent the leakage and exfiltration of toxic data: personal cardholder data, personal healthcare data, personally identifiable information, and intellectual property. It is also an important tool for enforcing privacy policies. Understand how to address common pitfalls and implementation challenges, and assess your DLP process maturity. See the "Rethinking DLP: Introducing The Forrester DLP Maturity Grid" Forrester report.

[26] Source: Forrester's Global Business Technographics Security Survey, 2015.

[27] Source: Forrester's Global Business Technographics Security Survey, 2015.

[28] A good working relationship with the board will ensure that the CISO is seen not only as the security expert but as a strategic business executive who is essential to the performance, growth, and ongoing success of the business. This report explains how security leaders can transform the risk conversation and develop their personal brand as a key corporate player. See the "Security Leaders, Earn Your Seat At The Table" Forrester report.

[29] As organizations have become too hung up and reliant on technology, the human aspect doesn't get the attention it deserves. Over time, outdated skills; stagnated thinking; and complacency in security personnel, the security group, and the organization itself become a threat to the business. It's time for S&R leaders to invest in themselves, their staff, and all employees because employees — not technologies — are the ones responsible for security strategy design, implementation, and behavioral change. See the "Maintain Your Security Edge" Forrester report.

[30] Source: Forrester's Global Business Technographics Security Survey, 2015.

[31] Source: Forrester's Global Business Technographics Security Survey, 2015.

[32] For too long, creating security awareness has been an afterthought, something CISOs did in their spare time after putting out the operational fires that sprang up around them with alarming regularity. S&R professionals are coming to realize, however, that their neglect of the human aspect is actually one of the reasons that incident numbers are not declining despite increased adoption of technological controls. This report takes lessons from CISOs who have both failed and succeeded, and from a variety of marketers and vendors, to outline a new way to approach what has too long been a stale and stagnant practice; a new way to engage the human firewall. See the "Reinvent Security Awareness To Engage The Human Firewall" 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.