FORRESTER®

For: Security &
Risk Professionals

Understand The State Of Data Security And Privacy: 2013 To 2014

by Heidi Shey, October 1, 2013

KEY TAKEAWAYS

Data Security Budget Allocation Holds Steady; Data Discovery, Classification Gaining

Organizations are allocating, on average, 17% of security technology budget to data security. DLP and database vulnerability assessment, monitoring, and auditing will see the most growth in the next 12 months. And good news: Data discovery and classification are also gaining ground as security priorities.

Insiders Continue To Cause Their Fair Share Of Data Breaches

Inadvertent misuse of data from insiders tops the list of breach causes in 2013, responsible for 36% of breaches seen in Forrester's data. No surprise, given that security awareness training is undervalued; employees have access to data but don't understand data use policies and are using and storing data across a variety of devices today.

Data Privacy And Regulations Responsibility Is Falling More Into Security's Hands

In 2013, the security group is fully responsible for privacy and regulations in 30% of firms, contrary to 2012, when full responsibility began shifting toward a privacy officer. In firms that didn't focus on privacy before, this change is encouraging, but it will be a concern as privacy program needs mature and the security team gets overloaded.

Understand The State Of Data Security And Privacy: 2013 To 2014

Benchmarks: Data Security And Privacy Playbook

by Heidi Shey
with Stephanie Balaouras, Brian Luu, and Kelley Mak

WHY READ THIS REPORT

Throughout the year, Forrester analysts engage in hundreds of discussions with vendors and end users about data security and privacy. Analysis of B2B survey data from Forrester's Forrsights Security Survey, Q2 2013 and additional data from our data partner CyberFactors provides another layer of insight into the state of data security and privacy today and in the future. 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 organizations for 2013 to 2014. 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.

Table Of Contents

Notes & Resources

Forrester analyzed data from Forrester Forrsights Security Survey, Q2 2013 and CyberFactors in this report.

Related Research Documents

Identify And Influence Data Security And Privacy Stakeholders
September 12, 2012

Job Description: Chief Privacy Officer
August 23, 2012

INSIDERS CARRY ON AS A MAJOR SOURCE OF DATA BREACH

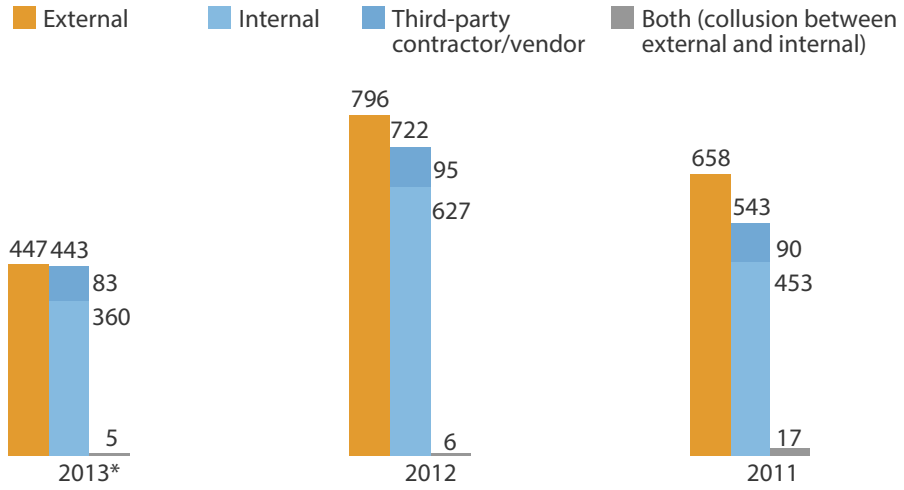
Based on CyberFactors' count of publicly reported cyberincidents in 2013 thus far, cases in which insiders are the cause of breach are on track to make up almost half of incidents this year (see Figure 1). This is in line with the final tallies from the previous two years. Within Forrester's own survey data, roughly 36% of breaches originate from inadvertent misuse of data by insiders, crowning it the top cause of breaches seen during the past 12 months (see Figure 2). It's no surprise that insiders contribute to their fair share of data breaches. Consider that:

- **They have not received any kind of security awareness and training.** In Forrester's recent study of information workers in North America and Europe across SMBs and enterprises, only 42% of the workforce indicated that they had received training on how to stay secure at work, and only 57% say they are aware of their organization's current security policies.[1] Security awareness and training is underappreciated and undervalued in many organizations — and it shows. The goal of an awareness and training effort should not be distribution of information, but driving behavioral change.[2]

- **They have access to the data but don't always know about or understand data use policies.** You've just handed your car keys over to someone who doesn't know about traffic signals — and you're not alone. Today, 56% of information workers are actually aware of or understand the policies in place that are specific to data use and handling inside their company (see Figure 3). Overall, 61% say they actually follow security policies in general. This is not simply about awareness. It's a more deeply rooted issue caused by the organization's basic lack of knowledge about the data in use, overly complex classifications (if they even exist at all), and subsequent ineffective data use policies.[3] Organizations must define their data and roles for data creators, owners, users, and auditors if they hope to protect their data and allow employees to understand how to use the data appropriately.[4]

- **They are using a myriad of devices and regularly store and access files on these devices.** Information workers are rapidly increasing the variety and combination of devices that they use for work. About 10% indicate that they're using a combination of desktop, laptop, tablet, and smartphone for work (see Figure 4). Roughly 61% are using some type of mobile device (laptop, tablet, smartphone) for work today. On average, 26.6% of information workers use at least three or more devices for work.[5] When accessing or storing files on these devices, 66% of the workforce puts these files on a USB flash drive or CD/DVD, while 27% use a file sync, sharing, or online locker service (see Figure 5). Do you know where your data is?

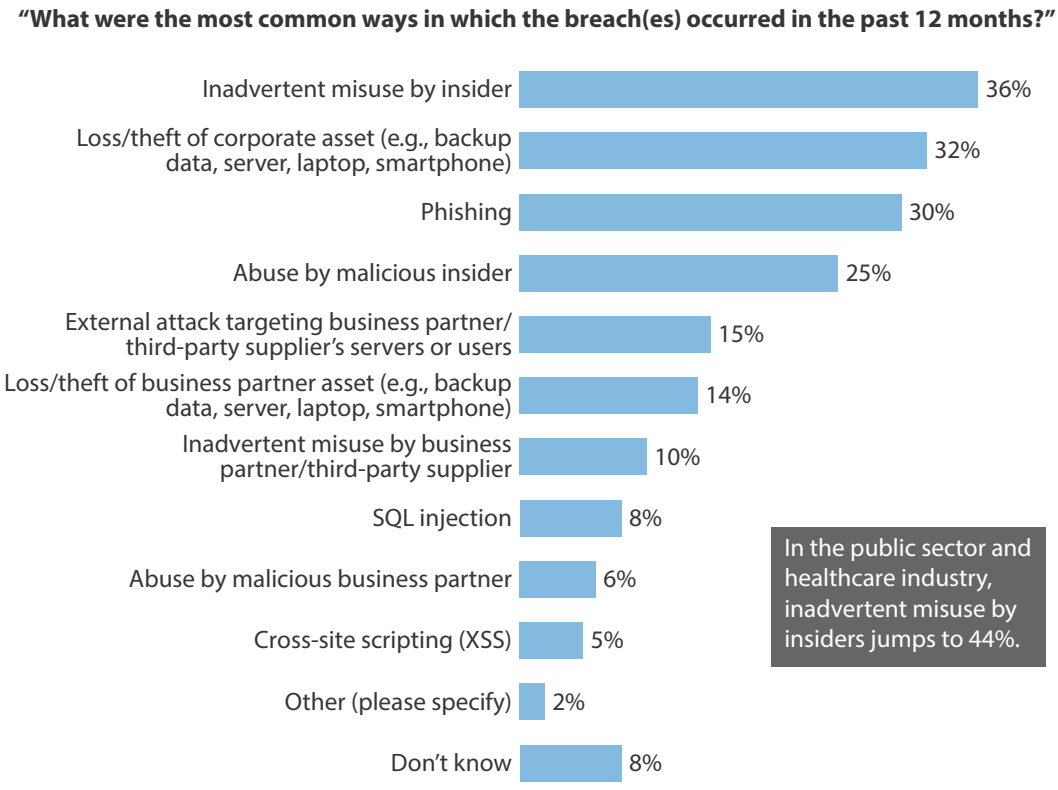
Figure 1 Publicly Reported Sources Of Incidents Remain Consistent Year Over Year



*Note: 2013 data is from January 1, 2013 to August 27, 2013
Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure

82021 Source: Forrester Research, Inc.

Figure 2 Insiders And Lost Or Stolen Devices Continue As Common Sources Of Data Breach

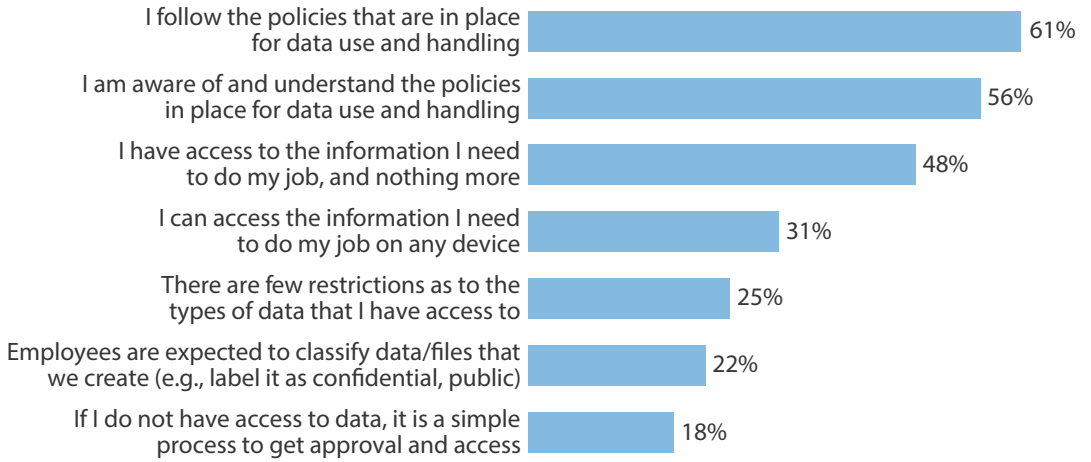


Source: Forrsights Security Survey, Q2 2013

82021 Source: Forrester Research, Inc.

Figure 3 Most Info Workers Follow Data Use Policies, But Awareness Could Be Better

"Select the statements about information use and handling at your company that you agree with."



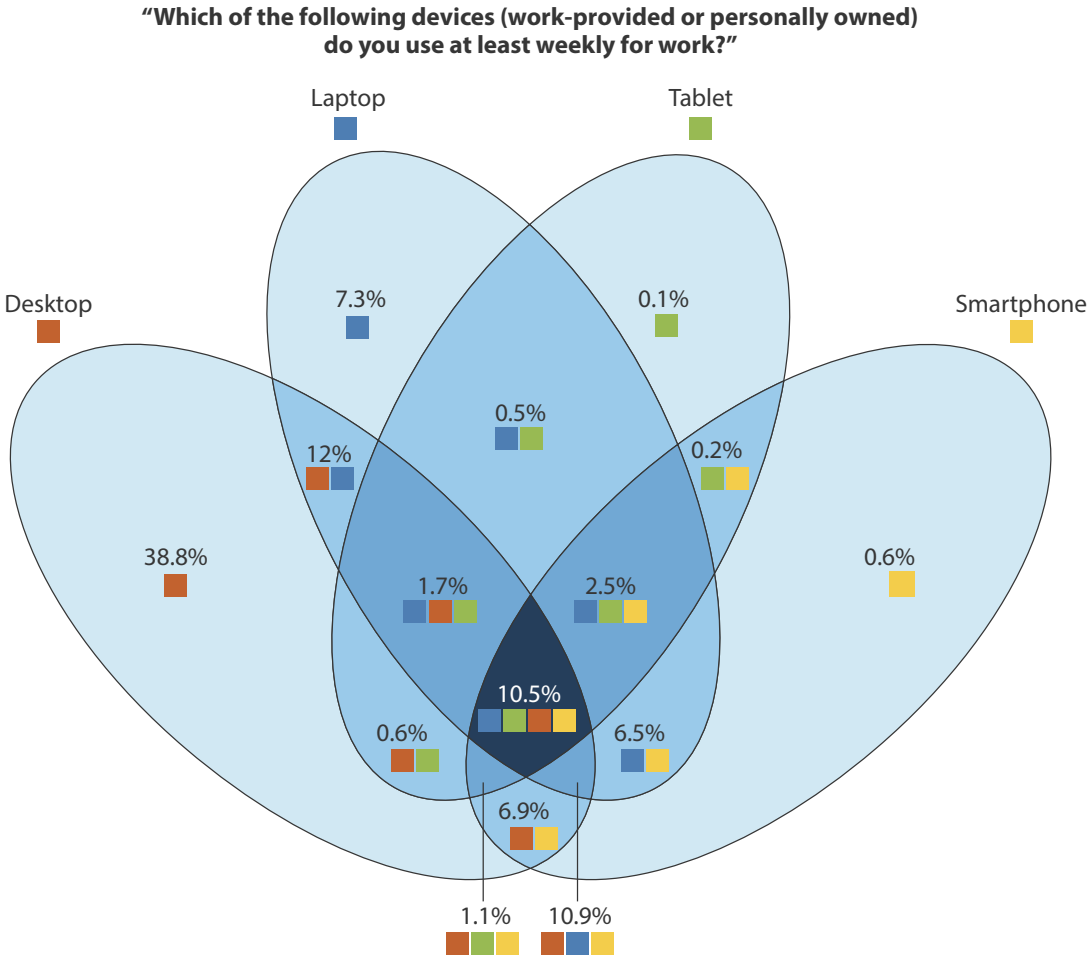
Executives (directors or above) are more likely than managers or individual workers to have access to information on any device, and less aware of policies for data use and handling. Fifty-five percent of executives say they follow policies that are in place for data use and handling.

Base: 4,262 North American and European information workers at SMBs and enterprises

Note: An information worker is an employee who uses a computing device (desktop, laptop, tablet, smartphone) for at least an hour per day for work purposes.
Source: Forrsights Devices And Security Workforce Survey, Q2 2013

82021 Source: Forrester Research, Inc.

Figure 4 Information Workers Use A Variety And Combination Of Devices To Do Their Job



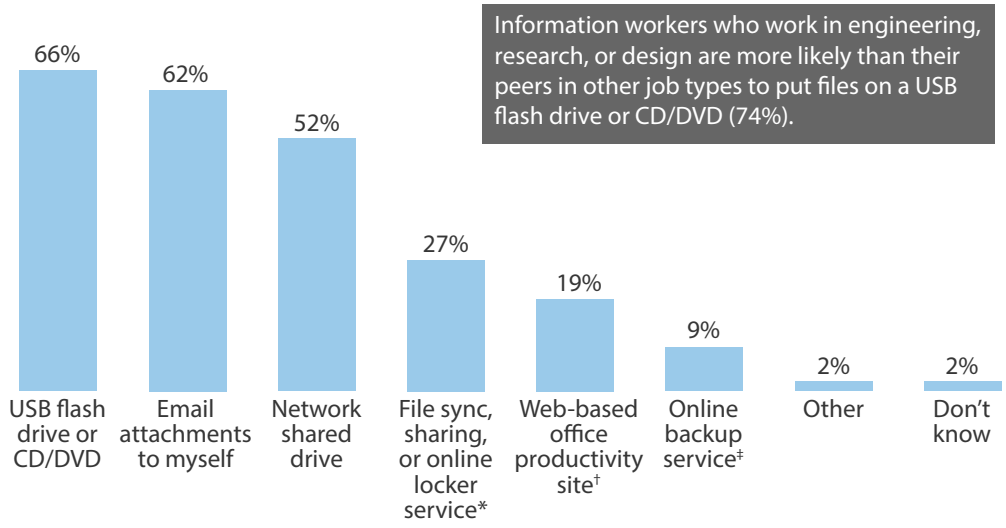
Base: 5,003 information workers

Note: An information worker is an employee who uses a computing device (desktop, laptop, tablet, smartphone) for at least an hour per day for work purposes.
Source: Forrsights Devices And Security Workforce Survey, Q2 2013

82021 Source: Forrester Research, Inc.

Figure 5 Info Workers Rely Most On USB Flash Drives And CD/DVDs For File Storage And Access

"How do you store and access your files on multiple PCs, smartphones, or tablets?"



Base: 1,920 North American and European information workers at SMBs and enterprises who regularly store/access files on multiple devices for work

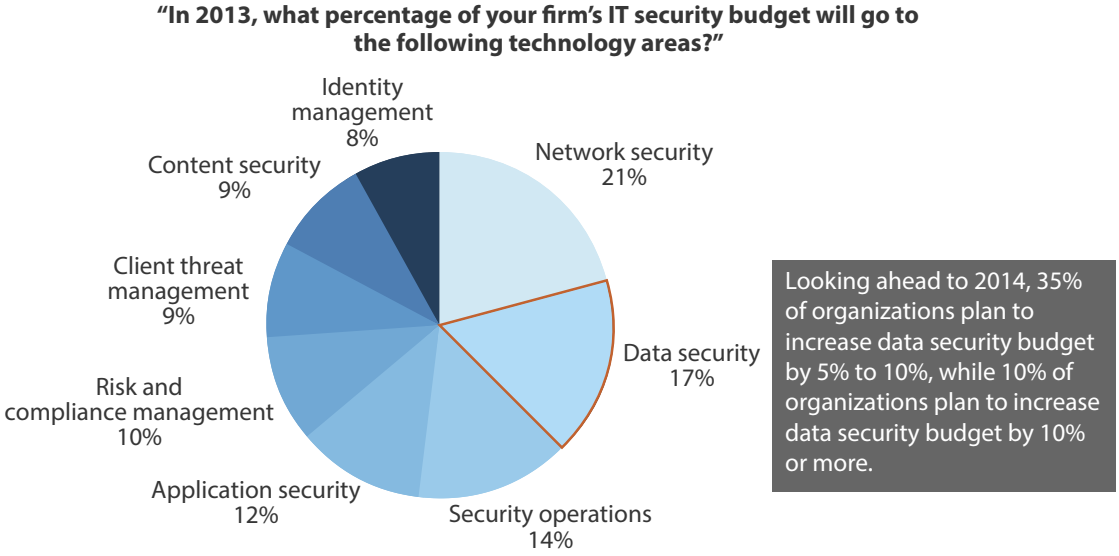
Note: An information worker is an employee who uses a computing device (desktop, laptop, tablet, smartphone) for at least an hour per day for work purposes.
Source: Forrsights Devices And Security Workforce Survey, Q2 2013
*Examples shown to survey respondents: Dropbox, YouSendIt, SkyDrive, Box.net
†Examples shown to survey respondents: Google Docs, Zoho, Office Web Apps
‡Examples shown to survey respondents: Carbonite, Mozy, Norton Online Backup

82021 Source: Forrester Research, Inc.

DATA SECURITY IS TOP OF MIND NOT JUST FOR S&R PROS BUT EXECUTIVES, TOO

Data security takes up the second largest portion of the IT security technology budget (17%) in 2013, and 35% of firms have plans to increase spending here in 2014 (see Figure 6). Data security is not an IT issue, but a business imperative. If conversations about data security were not happening before, they are now. In 55% of organizations, recent high-profile cyberattacks on IT security have raised the awareness of executives.[6] As executives see more and more media coverage of data breaches and security incidents, the inevitable question is: "What are we doing to make sure that doesn't happen to us?" The stakes remain high, as personally identifiable information and intellectual property continue to be the top two data types most likely to be compromised in a breach.[7]

Figure 6 Data Security Takes 17% Of The Security Technology Budget In 2013



Base: 1,417 North American and European enterprise and SMB IT security decision-makers

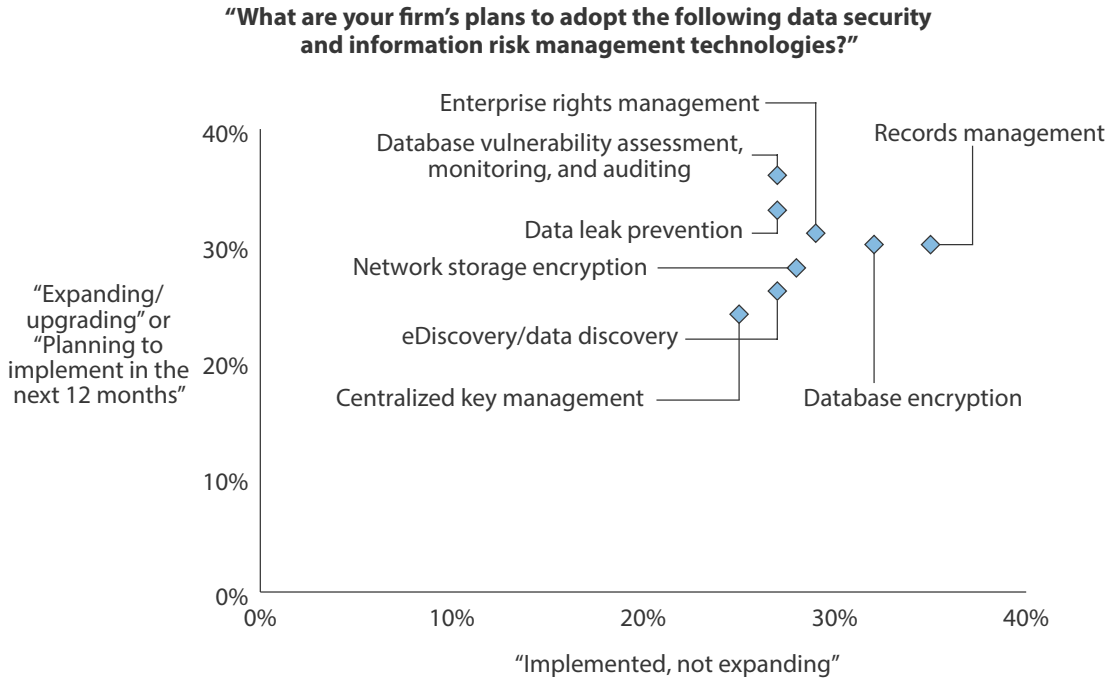
Source: Forrsights Security Survey, Q2 2013

82021 Source: Forrester Research, Inc.

S&R Pros Focus Investments On Data Leak Prevention And Database Security

Data leak prevention (DLP) and database vulnerability assessment, monitoring, and auditing remain on the top of the most wanted technology list for data security and information risk management in 2013 going into 2014. Thirty-six percent of companies are looking to either adopt a new implementation or add investment to a current implementation for database vulnerability technologies, and 33% of companies are looking to do the same with DLP solutions (see Figure 7).

Figure 7 DLP And Database Security Take The Top Spots On The Technology Wish List



Base: 692 North American and European enterprise and SMB IT security decision-makers

Source: Forrsights Security Survey, Q2 2013

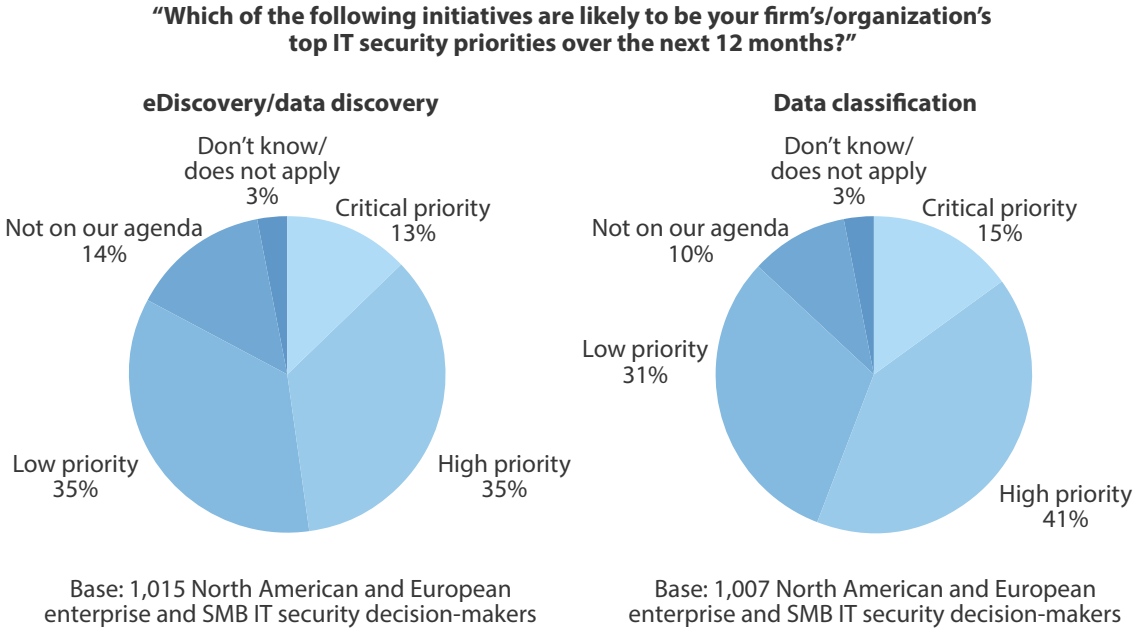
82021 Source: Forrester Research, Inc.

The Basics Of Data Control Strategy (Discovery And Classification) Are Gaining Ground

Data security and privacy challenges comprised 7% of the client inquiries fielded by Forrester's security and risk analysts in 2012, and we are on track to meet or surpass that in 2013.[8] The specific challenges seen across these inquiries revolve around data control processes and technologies such as data discovery, classification, encryption, and DLP in addition to questions about specific privacy regulations. One of the most common technology questions that we receive relating to data security is about DLP. 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 such technology investments. Forrester's Data Security And Control Framework helps to bring together silos of data control and protection (like archiving, DLP, and access control) and moves security controls closer to the data.[9]

However, before data controls and policies are created, organizations must know what they're trying to protect.[10] This is where data discovery and data classification are a critical first step in this framework. Today, 48% of organizations consider data discovery a high or critical priority, a huge jump from 2012 when 20% of companies felt the same (see Figure 8). Data classification is a high or critical priority for 56% of organizations, and also an increasingly popular inquiry topic — and one that brings stakeholders from both the security group and privacy office to the table.

Figure 8 Roughly Half Of Organizations Consider Defining Their Data As A High Or Critical Priority



Data discovery gains momentum in 2013. In 2012, only 20% of organizations considered it a high or critical priority.

Source: Forrsights Security Survey, Q2 2013

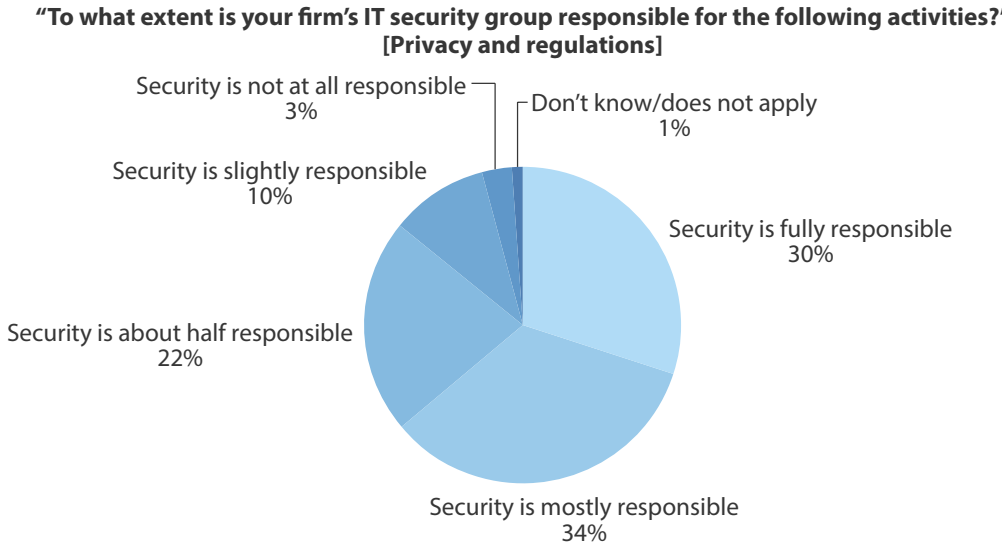
82021 Source: Forrester Research, Inc.

DATA PRIVACY COMMANDS MORE ATTENTION FROM S&R PROS

Contrary to 2012 when privacy responsibility was shifting to an organizationwide accountability, in 2013 it's falling more onto the security group within enterprises (see Figure 9). 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 more widespread pain and have requirements that necessitate the hiring of a privacy officer (or several!) to take the lead on privacy. Smaller-sized enterprises may be feeling the pinch but opting instead to have the security group take on privacy responsibility as a first step toward privacy program maturity.

In general, this overall shift is not entirely surprising given the amount of public attention and debate that privacy receives today. However, it's a matter of concern if more and more enterprises deem the security group fully responsible for privacy and regulations. After all, privacy does not begin and end with security; security is only one aspect of privacy.[11] Ensuring privacy requires a union of technology, policy, and culture, and a 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 in an increasingly complex world, it's only a matter of time before privacy and regulations require the full attention of a dedicated privacy officer and group.

Figure 9 In 30% Of Organizations, Security Is Fully Responsible For Privacy And Regulations



In North America, the larger the enterprise, the less likely security is fully responsible. In North American enterprises with 20,000 or more employees, 24% say that security is fully responsible for privacy and regulations.

Base: 995 North American and European enterprise IT security decision-makers

Source: Forrsights Security Survey, Q2 2013

82021 Source: Forrester Research, Inc.

WHAT IT MEANS

USE BENCHMARKS AS A STARTING POINT FOR YOUR OWN ANALYSIS

Based on what Forrester sees as data security trends for 2013 to 2014, organizations continue to falter when it comes to addressing internal and employee-related risks. However, there are bright spots. While DLP is hands down still the hottest must-have security technology across many organizations, there is greater attention paid today to creating a holistic data control strategy. Firms are starting by building a strong foundation and defining their data with data discovery and data classification. 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 to lead and take full responsibility for privacy.

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 as 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.

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.

Forrester's Forrsights Security Survey, Q2 2013, was fielded to 2,134 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester's Forrsights for Business Technology and was fielded from March 2013 to June 2013. ResearchNow fielded this survey online on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates. We have provided exact sample sizes in this report on a question-by-question basis.

Each calendar year, Forrester's Forrsights for Business Technology fields business-to-business technology studies in more than 17 countries spanning North America, Latin America, Europe, and developed and emerging Asia. For quality control, we carefully screen respondents according to job title and function. Forrester's Forrsights for Business Technology ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of IT products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Forrsights uses only superior data sources and advanced data cleaning techniques to ensure the highest data quality.

ENDNOTES

[1] An information worker is an individual who uses a computing device (desktop, laptop, tablet, smartphone) for at least an hour a day for work. Source: Forrsights Devices And Security Workforce Survey, Q2 2013.

[2] 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 too long been a stale and stagnant practice; a new way to engage the human firewall. See the April 12, 2013, "Reinvent Security Awareness To Engage The Human Firewall" 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 August 14, 2013, "Measuring Security Awareness To Enhance The Human Firewall" report.

[3] 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 January 15, 2013, "Know Your Data To Create Actionable Policy" report.

[4] Defining data via data discovery and classification is an often overlooked, yet critical, component of data security and control. Security and risk (S&R) pros can't expect to adequately protect data if they don't have knowledge about what data exists, where it resides, its value to the organization, and who can use it. Data classification also helps to create data identity (data-ID), the missing link for creating actionable data security and control policies. Yet, organizations that attempt to classify their data are thwarted by their own efforts with overly complex classification schemes and haphazard approaches. As a result, many see data discovery and classification as a Sisyphean task. This report aims to help S&R pros rethink and simplify their strategy to define their data. See the April 5, 2013, "Strategy Deep Dive: Define Your Data" report.

[5] Source: Forrsights Devices And Security Workforce Survey, Q2 2013.

[6] Source: Forrsights Security Survey, Q2 2013.

[7] In organizations that have been breached in the past 12 months, 32% indicated that personally identifiable information was compromised, and 30% indicated that intellectual property was compromised. The third most likely to be compromised data type was authentication credentials (25%). Source: Forrsights Security Survey, Q2 2013.

[8] Forrester's security and risk (S&R) team fields hundreds of inquiries every month. We use these inquiries as a barometer to track client challenges and to gauge client interest in the various topics we cover; this is a key source of input as we plan our future research agenda. As we sift through the 2012 inquiries, we're sharing this data so that you can see exactly what's keeping your peers up at night and what they're doing about it. See the June 26, 2013, "Inquiry Spotlight: Security And Risk, Q1 To Q4 2012" report.

[9] Now is the time to bring together separate silos of data control and protection such as archiving, DLP, and access control. This also involves moving data security controls closer to the data itself, instead of at the edges (perimeters) of networks. 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 July 12, 2012, "Control And Protect Sensitive Information In The Era Of Big Data" report.

[10] Defining data via data discovery and classification is an often overlooked, yet critical, component of data security and control. Security and risk (S&R) pros can't expect to adequately protect data if they don't have knowledge about what data exists, where it resides, its value to the organization, and who can use it. Data classification also helps to create data identity (data-ID), the missing link for creating actionable data security and control policies. Yet, organizations that attempt to classify their data are thwarted by their own efforts with overly complex classification schemes and haphazard approaches. As a result, many see data discovery and classification as a Sisyphean task. This report aims to help S&R pros rethink and simplify their strategy to define their data. See the April 5, 2013, "Strategy Deep Dive: Define Your Data" report.

[11] 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: "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD (http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html).

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

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.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals