Know Your Data To Create Actionable Policy

Policy And Procedures: The Data Security And Privacy Playbook

by Heidi Shey and John Kindervag
February 18, 2016

Why Read This Report

Too often, security and risk (S&R) leaders 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 policies are ineffective and can even hinder business processes. In today’s evolving data economy, data identity is the missing link that S&R leaders must define to create actionable policy. We designed this report to help S&R leaders develop effective policies using our Data Security And Control Framework as a guideline.

Key Takeaways

Use Forrester’s Data Security And Control Framework For Policy Creation
This framework breaks data protection into three areas: 1) defining data; 2) dissecting and analyzing data; and 3) defending data. A policy overlay can be applied where: 1) data identification stems from defining data; 2) data implications and audit mechanisms arise from dissecting and analyzing data; and 3) policies are created to defend data.

Data Identity Is A Key Concept For Actionable Data Security Policy
Applying identity and tagging data packets with identity attributes allows us to determine the business criticality of any piece of data and thereby protect it more effectively. Data identification must address three elements: data identity, data handling roles, and data control tools.

The Chief Data Officer Will Drive Data Security Policy Initiatives In The Future
The chief data officer, chief information security officer, chief marketing officer, and chief privacy officer each have a key contributing role in data security policy. However, Forrester believes that to properly protect data from the dramatic and disastrous consequences of a data breach, the chief data officer position must be incentivized to objectively oversee data protection mandates.
Know Your Data To Create Actionable Policy

Policy And Procedures: The Data Security And Privacy Playbook

by Heidi Shey and John Kindervag
with Michele Goetz, Stephanie Balaouras, Kelley Mak, Alexander Spiliotes, and Peggy Dostie
February 18, 2016

Table Of Contents

2 Data Security And Privacy Policies Today
   Have More Bark Than Bite
2 Get Some Policy Teeth With The Data
   Security And Control Framework
11 Chief Data Officers Will Drive Data Security
   Policy Initiatives

What It Means

13 Know Your Data To Meet Evolving Privacy/
   Data Sovereignty Demands

14 Supplemental Material

Notes & Resources

In developing this report, Forrester drew from
insight and research through advisory and
discussions with end users and vendors.

Related Research Documents

Build A Privacy Organization For Consumer Data
Management

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

Top Performers Appoint Chief Data Officers
Data Security And Privacy Policies Today Have More Bark Than Bite

Data defense is the fundamental purpose of information security. To defend your data, there are only four levers you can pull: 1) controlling access; 2) inspecting data usage patterns for abuse; 3) disposing of data when it no longer has value; and 4) obfuscating or “killing” data to render it unreadable in the event that it is stolen. Policy addresses when and how much to pull the levers. Sadly, today’s security policies are habitually static documents that sit on a shelf gathering dust. More often than not, data security policies are a checkbox item rather than a well-thought-out schema that ties data with security and privacy policy, enforcement, and auditing activities. This primarily stems from:

› **Organizations’ lack of knowledge about their own data.** Organizations now measure their data storage in petabytes, and capacities continue to skyrocket. As a result, S&R pros have preconceived notions and fears about data classification; they believe that trying to get to know the data contributes to the problem of ineffective data security policy: “It’s like trying to boil the ocean!”

› **Overly complex and impractical classification schemes.** Those who attempt to get to know their data and classify it through traditional confidentiality or integrity frameworks such as Bell-LaPadula and Biba for access control struggle to apply these academic frameworks in a big data world and end up with overly complex classifications. As a result, such policies look good on paper but are not necessarily practical or useful.

› **A siloed approach to privacy.** Privacy is a business discipline that requires the involvement of stakeholders from across the organization. Organizations that operate in silos run the risk of creating public-facing privacy policies created by legal or compliance without the involvement of their technology management counterparts — and thus lack confirmation that these policies are enforceable.

Get Some Policy Teeth With The Data Security And Control Framework

To help security professionals adapt to the new data economy, Forrester has created our Data Security And Control Framework. This framework breaks data protection into three key areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending the data. Security pros can build a policy layer on top of this control framework where: 1) defining the data leads to identifying the data; 2) dissecting and analyzing the data leads to understanding data implications and creating audit mechanisms; and 3) defending and protecting the data leads to creating data security and control policies (see Figure 1).
Identify Data And Roles To Create A Foundation For Actionable Policy

There are only two types of data that exist in your organization: 1) data that someone wants to steal and 2) everything else. The first type is sensitive or toxic data, which can be easily identified with the equation 3P + IP = TD. The three P’s stand for personally identifiable information (PII), personal health information (PHI), and personal cardholder information (PCI); IP is intellectual property; and TD is toxic data (see Figure 2).

The premise of defining your data is that if you don’t know what toxic data exists and where it resides, you can’t expect to adequately secure and protect it. Typically, we think of identity as an idea that one can only apply to network users. But users merely assert an identity on the network that is contained in the packet that flows across the network. By re-applying identity to all the packets traversing a network, we can tag data packets with identity attributes that will allow us to determine the business criticality of any piece of data and thereby protect it more effectively. Data identification is the first step toward creating actionable policy; it must address four key components:

- **Data identity.** As users and systems create data and it moves around the network, it picks up attributes in much the way users and applications generate traffic and have identities (see Figure 3). Data identity encompasses attributes such as: 1) who created it; 2) who owns it in the business; 3) where it’s located; 4) what its toxicity level is; and 5) who can consume it (read versus write). Over time, data can acquire various attributes that provide value to the business from both a security and operations perspective.
› **Data-handling roles.** Identify data-handling roles to set and clarify expectations for behavior and access. Understand how employees work (e.g., are they primarily mobile?), why they need access to this data, and what data they need to access for their role. Forty-five percent of information workers in North America and Europe say they only have access to information needed to do their job and nothing more.⁴ Remember to account for your privileged users, too.⁵

› **Data control tools.** Identify tools that can help with policy automation and enforcement. Manual data discovery and classification can quickly turn into a futile and unenforceable policy exercise. Data discovery and classification tools can help streamline processes and automate enforcement.⁶ Network analysis and visibility (NAV) and data loss prevention (DLP) tools can help discover data so that it can be properly identified and classified.⁷ The data from NAV and DLP tools can also feed into security analytics to help the enterprise know where to look for toxic data.⁸

› **Data stewards and business analysts.** Data governance teams implementing data quality, master data management, and metadata management programs regularly assess and manage data policies aligned to operational and analytics data use. Often reporting into chief data officers (CDOs), they are responsible for also considering data security in their data management solutions. Additionally, their understanding of data flow provides broad context to connect activities and processes of various data-handling roles.⁹

---

**FIGURE 2** Identify Sensitive Data With The Toxic Data Equation

```
3P + IP = TD
```

<table>
<thead>
<tr>
<th>The 3 P’s</th>
<th>Intellectual property</th>
<th>Toxic data</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>PHI</td>
<td>PII</td>
</tr>
</tbody>
</table>

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378
Understand Implications For Data Handling To Develop Practical Policies

Data is a valuable asset that morphs into a liability when improperly handled. Organizations must understand the implications of data handling, from use to storage and disposal, in order to develop sound policies. S&R pros can’t do this alone. This is where the chief privacy officer (CPO), or equivalent privacy official, legal, compliance, and marketing team members, will have a vital role in decoding regulatory complexity and customer expectations. You will need to help your enterprise consider:

› **State-specific legislation in the US.** State-specific legislation covers a variety of considerations ranging from privacy practices, data encryption mandates, and breach notification rules to acceptable use of data such as social security numbers (SSNs). California, for example, passed state laws in October 2015 that address almost all of the aforementioned considerations.10

› **Country-specific laws.** These will vary by country.11 Canada’s PIPEDA requires organizations to meet specific conditions when they collect, use, or disclose PII data without an individual’s knowledge and consent.12 Upcoming changes to the EU Data Protection Directive will create new requirements for firms to meet, such as an individual’s right to erasure of his or her data.13 South Korea’s recent amendment to its Personal Information Privacy Act (PIPA) provides that companies that leak personal information “because of a deliberate act or serious error” could suffer court-awarded damages up to three times the damage caused by the loss.14

› **Industry-specific regulations.** In the US, the Gramm-Leach-Bliley Act requires that financial institutions explain privacy practices to customers and safeguard their sensitive data.15 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology
for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act (2009) address protections for personal health information. In South Korea, the Act on Promotion of Information and Communications Networks Utilization and Information Protection, Etc. requires data control measures for telecoms, web portals, and website operators, while the Financial Holding Companies Act restricts data sharing among financial holding company affiliates.

Other policy influencers. Reports and plans from governments and other sources such as think tanks also influence data-handling decisions. For example, in the US, the Obama administration’s “Consumer Privacy Bill of Rights” is a public document available to consumers, businesses, and lawmakers alike. In Europe, the Article 29 Working Party, an independent entity with advisory status, issues publicly available opinions and guidance on topics related to processing of personal data. The International Association of Privacy Professionals (IAPP) Westin Research Center also works to produce practical and applicable research relating to privacy issues and concerns.

Respect Consumer Concerns When Creating And Communicating Policies

Given that, in many cases, much of the sensitive data that organizations handle is about consumers and their PII, organizations can’t overlook consumer security and privacy perceptions. A variety of interactions with your organization cause concern among consumers (see Figure 4). Most of these involve the sharing of information. Even if your organization is primarily a B2B company, remember that your business customers are consumers, too. S&R pros must consider:

Consumer perceptions. Be aware of consumer perceptions to better align data priorities and justify needed investments for security. Security and privacy considerations are a major component of the customer relationship, and they require collaboration between business and security stakeholders alike. Consumer concern is notable when it relates to financial transactions and purchases. For example, 53% of US online adults who are worried about the security of their financial data are concerned about their security and privacy when purchasing products online.

Consumer behavior. Evaluate critical customer touchpoints and experiences that can generate security and privacy concerns. Consider that 38% of US online adults express concern with using mobile payments. Know what types of data are collected in a purchase transaction, and identify where unnecessary data collection — and potential liability — can be reduced. With 31% of US online adults expressing security and privacy concerns about downloading mobile apps, application security and app privacy policies must be taken seriously.
**FIGURE 4** Consumers Have Security And Privacy Concerns When Interacting With Your Business

“How concerned are you about personal data privacy and security when doing each of the following?”

(Respondents who selected 4 or 5 on a scale of 1 [not concerned at all] to 5 [very concerned])

- **Share personal info online**: 54%
- **Using free Wi-Fi provided by retail stores, malls, or restaurants**: 43%
- **Sharing personal information with your social network**: 43%
- **Use social networking login info to access other sites**: 40%
- **Making payments with your mobile phone (e.g., with ApplePay)**: 38%
- **Using mobile apps that know your location**: 37%
- **Purchase products online**: 34%
- **Download apps to a mobile phone or tablet**: 31%
- **Using a search engine**: 29%


---

**Establish Audit Mechanisms To Prove Policy Enforcement**

The existence of a policy in and of itself does not guarantee enforcement. This is where technology has a role to help enforce policy, provide an audit trail, and meet compliance requirements. Tools and processes to assist in this effort include:

- **Data discovery.** Data discovery tools not only identify where data resides but also show how the data is being used and handled within the organization. Data discovery capabilities are available in a variety of tools today, from standalone discovery tools to discovery capabilities embedded within other tools like DLP, eDiscovery, or data governance tools. Vendors such as AccessData, Active Navigation, Digital Guardian, Ground Labs, Guidance Software, Identity Finder, McAfee (Intel Security), Nuix, Recommind, RSA (Dell/EMC company), StoredIQ (an IBM company), Vontu (Symantec), Websense, Zylab, and others can help discover how data is handled.
› **Data classification.** Data creators can use classification tools to tag data by toxicity level, which helps identify and map to appropriate data use, handling, and access. Classification tools also help provide metadata that feeds into DLP tools. Vendors such as Boldon James, Concept Searching, Digital Guardian, IBM, Identity Finder, Imperva, Secure Islands (Microsoft), NextLabs, Titus, Varonis Systems, and Whitebox Security (SailPoint) can help with data classification.

› **Data loss prevention (DLP).** DLP tools can help control data by enforcing predetermined policies once the upfront work of defining the data is done. However, think of DLP itself not as a single product but as a process and an embedded function. DLP tools can also provide data discovery capabilities. Vendors such as Clearswift, Digital Guardian, Forcepoint, Intel Security (McAfee), Symantec, and Trend Micro can help with DLP.

› **Network analysis and visibility (NAV).** NAV tools provide situational awareness and visibility into happenings on the network to show what users and data are doing. NAV tools are not a single tool but a collection of diverse tools. These can include network discovery tools from such vendors as Lumeta, SolarWinds, Spiceworks, and 10-Strike Software; flow data analysis tools from Arbor Networks, Lancope (Cisco), Flowtraq, and Vitria; packet capture and analysis tools from NetScout and Niksun; network metadata analysis tools from BlueCoat Systems, Fidelis Cybersecurity, and RSA NetWitness (Dell/EMC); and network forensics tools from Guidance Software.

› **Data management tools.** Enterprise data management solutions such as data quality, master data management, and data profiling come with data security capabilities built in. IBM, Informatica, and SAP leverage their existing data security tools to establish access and controls in developer and stewardship user groups as well as for data consumers. Metadata repositories provide rich data connecting data use and access to security policies as an additional alert mechanism for breaches and misuse. Intelligent semantic catalogs such as Cambridge Semantics, Novetta, and Verato are also emerging that establish relationships between identities, business objects, and behavior to improve fraud detection and manage PII at big data scale.

› **Intelligent forensics.** This analysis provides organizations the ability to find perpetrators and investigate breach methods. Vendors like SparkCognition leverage cognitive agents to scan developer and hacker communities for discussions on hacks and breaches.

---

**Create Data Security Policies Without Reinventing The Wheel**

Defending data boils down to addressing four key components: access, inspect, dispose, and kill. Data security and use activities and corresponding policies can thus be created for each defense component. To simplify policy creation, use accepted security standards as a starting point to identify necessary data security and control activities and systematically create corresponding policies for each component of defense (see Figure 5). ISO/IEC 27002 can surface high-level considerations and provide an idea of scope for each defense piece. Tactically, PCI DSS can provide more detailed and prescriptive guidance. Specifically, look for:
› **Access policies.** Policies must ensure that the right users can access the right data at the right time (see Figure 6). Sections 6.2 and 9 of ISO/IEC 27002 detail access control considerations for business requirements to mobile devices and teleworking. PCI DSS requirements 7, 8, and 9 provide additional specific guidance for access control.

› **Inspection policies.** Policies should be in place that ensure the inspection of data usage patterns, so that suspicious activity can be identified (see Figure 7). Section 12.4 of ISO/IEC 27002 addresses monitoring, specifically audit logging, monitoring system use, and protection of log information. PCI DSS Requirement 10 addresses the tracking and monitoring of access to network resources and cardholder data.

› **Disposal policies.** S&R pros need to create policies to address data disposal to decrease liability when the organization no longer needs the data for business purposes (see Figure 8). Relevant aspects of ISO/IEC 27002 include secure disposal or reuse of equipment (Section 11.2.7), disposal of media (Section 8.3.2), and compliance for protection of organizational records (Section 18.1.3). PCI DSS Requirement 3 addresses data protection, while Requirement 3.1 directly addresses the implementation of data retention and disposal policies, procedures, and processes. Requirement 9 addresses restrictions for physical access to the data.

› **Kill policies.** Kill data using data abstraction techniques such as encryption, tokenization, and masking (see Figure 9). Killing data devalues it so that cybercriminals cannot use or profit from it, which can help protect the organization from compliance penalties in the event of a breach. ISO/IEC 27002 Section 10 addresses policy on the use of cryptographic controls, including key management. Other sections of ISO/IEC 27002 relevant to killing data include 12.3.1 for information backup and 18.1.5 for regulation of cryptographic controls. PCI DSS requirements 3 and 4 address encryption as well, where Requirement 3 approaches it from a data security perspective and Requirement 4 from a network security perspective.

**FIGURE 5** Mapping Policy To Defensive Components Of The Security And Control Framework

<table>
<thead>
<tr>
<th>Defend</th>
<th>Access</th>
<th>Inspect</th>
<th>Dispose</th>
<th>Kill</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI DSS Reqs 7, 8, 9</td>
<td>PCI DSS Req 10</td>
<td>PCI DSS Req 3, 9</td>
<td>PCI DSS Reqs 3, 4</td>
<td></td>
</tr>
</tbody>
</table>
FIGURE 6 Mapping Policies For Access Control

Defend
Access | Inspect | Dispose | Kill

PCI DSS  
Req 7: Restrict access to cardholder data by business need-to-know.  
Req 8: Identify and authenticate access to system components.  
Req 9: Restrict physical access to cardholder data.

ISO/IEC 27002  
Section 6.2: Mobile devices and teleworking  
Section 9: Access control

FIGURE 7 Mapping Policies For Data Inspection

Defend
Access | Inspect | Dispose | Kill

PCI DSS  
Req 10: Track and monitor all access to network resources and cardholder data.

ISO/IEC 27002  
Section 12.4: Logging and monitoring

FIGURE 8 Mapping Policies For Data Disposal

Defend
Access | Inspect | Dispose | Kill

PCI DSS  
Req 3: Protect stored cardholder data.  
Req 9: Restrict physical access to cardholder data.

ISO/IEC 27002  
Section 8.3.2: Disposal of media  
Section 11.2.7: Secure disposal or re-use of equipment  
Section 18.1.3: Protection of records
Chief Data Officers Will Drive Data Security Policy Initiatives

Organizations must now derive actionable business insights from more data than ever before in order to win, serve, and retain customers. To navigate the morass of information available internally and externally, companies need senior data leaders. Enter the CDO. More than 50% of data and analytics decision-makers at companies with greater than 10% revenue growth have appointed CDOs, and businesses with CDOs are 60% more likely to report increased business agility as a result of big data solutions than those without CDOs. Businesses with CDOs are also 70% more likely to report compliance and reduced risks as benefits of big data solutions than those without CDOs.27

The CDO doesn’t necessarily have ultimate authority over a company’s data, however; the CDO, CISO, CPO, and CMO each has a different mandate and relationship when it comes to company data (see Figure 10). Forrester believes that to properly protect data from the dramatic and disastrous consequences of a data breach, the CDO position must be incentivized to objectively oversee data protection mandates. The CISO and CDO need each other, and the CDO will drive security policy initiatives because:

- **CDOs can directly tie business value to data assets.** CDOs whose aim is to maximize the use of business data for better data-driven business decision-making can help the firm save time and costs in addition to driving productivity and revenue. Data quality becomes essential, because shoddy data erodes business value. When data is the product, data quality is paramount and produces an even more explicit value in the form of direct sales revenue. The CDO’s ability to demonstrate the business value of data assets will help the CISO when it comes to financially modeling information security risk and prioritizing expenditures for security.28

- **CDOs have the greatest understanding of data identity and purpose.** Responsibility for data strategy involves knowing the organization’s data — what data assets exist, where they are, what the organization uses these assets for, and how the organization should correctly use these assets. The CDO has the answers to the key questions that the CISO asks about the organization’s data in order to protect it.
› **CDOs possess the greatest incentive to protect the data.** In the event of a breach, the CISO takes the heat because, ultimately, security is the CISO’s responsibility. But responsibility and incentive are not the same thing. Because security is the CISO’s primary responsibility, the CISO surely has the incentive to protect the data. Yet, the CDO possesses the greatest incentive of all to protect the data because leveraging data assets as a strategic business asset is the CDO’s primary responsibility. If the organization does not protect these data assets from theft or misuse, it compromises the CDO’s data strategy itself.

**FIGURE 10 The Roles Of The CDO, CISO, CPO, And CMO**

<table>
<thead>
<tr>
<th>Role</th>
<th>Primary data mandate(s)</th>
<th>Relationship with data</th>
<th>Data security policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief officer</td>
<td>Data quality, data strategy, and governance</td>
<td>Treats data as a business asset and revenue stream.</td>
<td>Driver</td>
</tr>
<tr>
<td>Chief information security officer</td>
<td>Data security, access, and control</td>
<td>Understands the security risks and threats to data assets and the necessary controls to protect data.</td>
<td>Enforcer</td>
</tr>
<tr>
<td>Chief privacy officer</td>
<td>Data privacy, compliance</td>
<td>Ensures that the organization adheres to privacy principles in data collection, use, and handling practices.</td>
<td>Advisor</td>
</tr>
<tr>
<td>Chief marketing officer</td>
<td>Data usage for business purposes</td>
<td>Business and marketing intelligence to get more revenue and profitability</td>
<td>User</td>
</tr>
</tbody>
</table>

**But The CISO Will Architect Data Security And Privacy Control Strategy**

There is a distinction between policy and enforcement responsibilities. Much in the way the CPO works with the CISO to implement privacy policies and controls, the CDO will work with the CISO (and CPO) to implement data security and data use policies. There may be overlap along with collaboration when it comes to policy creation among the roles of the CDO, CPO, and CISO, but the CISO will hold the sole responsibility for architecting the necessary security and privacy controls to enforce policy and ensure that these controls are aligned with the organization’s overarching security strategy. S&R pros must also recognize that the CDO can come in many forms today. While the role is not always recognized in the C-suite, many organizations are appointing designated data stewards or data champions with CDO-like responsibilities.29
What It Means

Know Your Data To Meet Evolving Privacy/Data Sovereignty Demands

Updates to privacy laws in countries like Russia and the European Court of Justice’s ruling that Safe Harbor is invalid are forcing organizations to re-evaluate how they will legally store, process, and transfer both customer and employee data. Business, security, and privacy leaders are just now beginning to understand the issues around data residency — or sovereignty and localization — requirements. Recognize that:

› **It’s extremely difficult to secure data using traditional geographic paradigms.** There are no geographical borders on the Internet. The policies and approaches to governing the storage and transport of nation-specific data are critical for organizations to meet evolving privacy and data sovereignty requirements. Knowing your data will help to offer greater flexibility in your approaches to meeting regulatory, business partner, and customer requirements.

› **S&R pros cannot tackle these requirements alone.** For example, to meet requirements, a firm may opt for a policy to encrypt — during transport and storage — all PII of residents from countries with data residency requirements and mandate that the organization manage the associated encryption keys. In addition, the firm may call for a review of business use policies for this data. The policies and technology controls required to meet privacy requirements will impact both business and technology strategy. As a result, the CDO, CISO, CPO, CMO, and other business stakeholders like legal counsel will each take a seat at the data security and privacy table.

› **Staying in the dark about your data will impact your firm’s bottom line.** Penalties for security and privacy violations have been handed out at a healthy clip in the US thanks to bodies like the Federal Trade Commission. Countries like South Korea in the Asia Pacific region have also added teeth to privacy laws. With the European Union finalizing a top level fine of 4% of global turnover for a violation of the new General Data Protection Regulation, data sovereignty could become one of the biggest policy challenges of our time — and one with steep financial penalties for missteps.
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’s North American Consumer Technographics Consumer Technology Survey, 2015 was an online survey conducted in March 2015 of 6,743 US and Canadian individuals ages 18 to 88. For results based on a randomly chosen sample of this size, there is 95% confidence that the results have a statistical precision of plus or minus 1.2% of what they would be if the entire population of US and Canadian online adults (defined as those online weekly or more often) had been surveyed. Forrester weighted the data by age, gender, income, broadband adoption, and region to demographically represent the adult US and Canadian online population. The survey sample size, when weighted, was 6,697. (Note: Weighted sample sizes can be different from the actual number of respondents to account for individuals generally underrepresented in online panels.) Please note that respondents who participate in online surveys generally have more experience with the Internet and feel more comfortable transacting online.

Forrester’s Global Business Technographics Devices And Security Workforce Survey, 2015 was an online survey fielded in June and July of 2015 of 7,267 information workers 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.

Forrester’s Global Business Technographics® Data And Analytics Survey, 2015 was an online survey fielded in January through March 2015 of 3,005 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the United Kingdom, and the United States from companies with 100 or more employees.

Endnotes

1 Introduced in 1973, the Bell-LaPadula model primarily focuses on confidentiality for access control. Under this model, subjects are assigned clearance levels based on the objects they’re allowed to access. The simple security property prevents users from reading information above their clearance level but allows them to read down. The star property allows users to write up and create documents equal to or above their clearance level but prevents them from writing down to lower clearance levels, and the strong start property only allows users to read and write at their own level. Introduced in 1977, the Biba model primarily focuses on data integrity. In Biba, the simple security property does not allow users to read down to a lower level of classification, while the star property prevents users from writing up to a higher level of classification. Source: The CISSP Open Study Guide Web Site (https://www.cccure.org/Documents/HISM/087-089.html).

2 S&R pros can’t tackle this alone and must partner with their business peers. This report outlines the key capabilities necessary to build a privacy program that effectively manages consumer data privacy. See the “Build A Privacy Organization For Consumer Data Management” Forrester report.

3 Forrester breaks down the problem of securing and controlling data 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.


5 S&R pros recognize the imperative to manage privileged accounts properly. The current breach climate coupled with the migration of company data to cloud infrastructures means that privileged identities within the organization can become either security enablers, if assigned and monitored appropriately, or key vulnerabilities for hackers to exploit. For more information about challenges in privileged identity management and current vendor solutions, see the “Critical Questions To Ask Your Privileged Identity Management Solution Provider” Forrester report and see the “Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14” Forrester report.

6 Defining data via data discovery and classification is an often overlooked, yet critical, component of data security and control. See the “Rethinking Data Discovery And Data Classification” Forrester report.

7 Network analysis and visibility (NAV) is comprised of a diverse tool set designed to provide situational awareness for networking and information security professionals. See the “Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility” Forrester report.
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. This 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. Read the forthcoming “TechRadar™: Data Security, Q1 2016” Forrester report.

New roles will emerge to consider data risk and value. See the “Consider New Data Governance Software To Support Business-Led Efforts” Forrester report.

In October 2015, California Governor Jerry Brown signed into law five bills that: 1) force the government to obtain a warrant before requiring a company to produce user communications and metadata; 2) refine the definition of encryption to exclude some noncompliant, less effective technologies; and 3) add license plate information gleaned through motion-sensing cameras to the list of information that requires a breach notification letter if compromised. Source: David Navetta, Boris Segalis, Andrew Hoffman, Kimberly Gold, and Kathryn Linsky, “Five new privacy laws on tap in California,” Norton Rose Fulbright, October 23, 2015 (http://www.dataprotectionreport.com/2015/10/five-new-privacy-laws-on-tap-in-california/).

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.


Forrester clients frequently ask about European Union (EU) privacy regulations. This Q&A report addresses common data privacy questions and highlights upcoming changes in the regulations that have the most impact on organizations operating on a global scale. See the “Q&A: EU Privacy Regulations” Forrester report.

The American Recovery and Reinvestment Act of 2009 (ARRA) includes a section that expands the reach of the Health Insurance Portability and Accountability Act (HIPAA). This section, also known as the Health Information Technology for Economic and Clinical Health (HITECH) Act, expands the reach of HIPAA to include “business associates,” also known as service providers to HIPAA-covered entities. Under the HITECH Act, the business associates are now directly subject to HIPAA security and privacy requirements. Source: “One Hundred Eleventh Congress of the United States of America,” United States Government Printing Office (http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf).

Source: Cynthia O’Donoghue, “South Korea introduces further data protection breach penalties to encourage compliance, and issues mobile app guidance,” JD Supra Business Advisor, August 21, 2015 (http://www.jdsupra.com/legalnews/south-korea-introduces-further-data-93957/).

The Gramm-Leach-Bliley Act requires financial institutions — companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance — to explain their information-sharing practices to their customers and to safeguard sensitive data. Source: “Gramm-Leach-Bliley Act,” Federal Trade Commission (http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act).


Source: IAPP Westin Research Center (https://privacyassociation.org/westin-research-center/).


“Privacy is dead”: It’s a trope so often repeated you might actually think it’s true. But in the age of smartphones and sensors, privacy is not only possible, it's essential for building trust, the foundational currency of social, mobile, and local services. Context is key: Businesses crave insight into the context in which consumers are using their products, and consumers want businesses to deliver contextually relevant services. Contextual privacy is a framework for negotiating the collection and use of personal data that ensures a fair value exchange for both the customer and the business. See the “The New Privacy: It's All About Context” Forrester report.


S&R pros need to approach DLP as an ongoing process, not a product or even a one-time project. We designed this report to help you assess the current state of your DLP efforts against data loss vectors and process maturity. See the “Rethinking DLP: Introducing The Forrester DLP Maturity Grid” Forrester report.

Forrester’s Zero Trust Model of information security demands that organizations know what types of activities take place on their internal network as well as their external network. To provide this type of deep insight into internal and external networks, Forrester has defined a new functional space called network analysis and visibility (NAV). NAV is comprised of a diverse tool set designed to provide situational awareness for networking and information security professionals. See the “Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility” Forrester report.

The constantly mutating threat landscape requires new defensive measures, one of which is the pervasive use of data encryption technologies. In the future, you will encrypt data — both in motion and at rest — by default. This data-centric approach to security is a much more effective way to keep up with determined cybercriminals. By encrypting, and thereby devaluing, your sensitive data, you can make cybercriminals bypass your networks and look for less robustly protected targets. Encryption will become a strategic cornerstone for security and risk (S&R) executives responsible for their organization's data security and privacy efforts. We designed this report to help you understand how to use encryption, tokenization, and other technologies to “kill your data.” See the “Kill Your Data To Protect It From Cybercriminals” Forrester report.

There's a new kid in town, and it's the chief data officer (CDO). The new position arose from a growing awareness of the value of data and recognition of an inability to take advantage of the opportunities that it provides — either due to technology, business, or basic cultural barriers. This new role, however, varies significantly across organizations in terms of where it sits and what it does. These differences depend on the data legacy and current needs of the organization. See the “Top Performers Appoint Chief Data Officers” Forrester report.

In today’s seemingly never-ending cycle of new technologies, cyberthreats, and regulations, it’s almost impossible for CISOs to meet all of the modern organization’s security demands. In this difficult environment, senior leadership will evaluate the CISO not only on technical performance but also on how he or she manages information security as a business — prioritizing expenditures and making tough financial calls. Forrester presents the Information Security Value Model, which you can use to calculate the financial value that information security provides to the business in terms your executive colleagues will understand. With this approach, you’ll be able to make tough and effective financial decisions and demonstrate appropriate use of resources. See the “Determine The Business Value Of An Effective Security Program — Information Security Economics 101” Forrester report.
In anticipation of the increasing adoption of personal identity and data management (PIDM) tools and services, customer insights (CI) leaders will be held increasingly accountable for their organizations’ data collection, management, and use practices — including those of the vendors they hire to augment their CI teams. This practice, which Forrester calls “data stewardship,” is an imperative that organizations must plan for and enact today. See the “Building Data Stewardship Is A New Customer Insights Imperative” Forrester report.
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.