A Forrester Consulting
Thought Leadership Paper
Commissioned By IBM

September 2014

Implement A Proactive Strategy For Data Security

Data Security And Privacy Are Critical Business Imperatives In The Data Economy

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Hardly a week goes by without headlines about a breach of customer data. Less frequent, but just as alarming, are the publicly reported examples and allegations of intellectual property theft. Data security and privacy — and by extension, brand reputation — are front and center today and will quickly become a business differentiator for tomorrow. The question remains: How will organizations respond?

IBM commissioned Forrester Consulting to evaluate data security decision-making by security buyers and influencers, and what it means to engage in proactive data security and privacy efforts in order to address threats today and in the future. This study began in May 2014 and was completed in June 2014. Forrester developed a hypothesis that tested the assertion that enterprises today have many more stakeholders involved in data control, data governance, security, and privacy. However, despite this involvement, organizations approach data security in a very reactive fashion and often do not have a clear understanding about the value of their data.

Security teams have the attention of executives who are increasingly aware of and concerned about data security.

In conducting surveys with 200 security decision-makers in the US, UK, and Germany, and having five in-depth follow-up phone interviews for additional context, Forrester found that while these companies' data security efforts are primarily driven by compliance and tactical in nature, security teams have the attention of executives who are increasingly aware of and concerned about data security. These security decision-makers also place a high priority on helping securely enable big data and data quality initiatives — both of which have implications for revenue growth and customer experience.

KEY FINDINGS

Forrester's study yielded five key findings:

- **Data security efforts are policy- and compliance-driven.** Compliance is necessary, and policies are an important part of data security. However, organizations that drive data security efforts based on policy and compliance put the business at risk by neglecting to take a more holistic and proactive approach to data security strategy. Remember: Compliance does not equal security.
- **Firms do not understand what is sensitive data.** What is sensitive data to the organization? And does the entire organization share a common understanding of what constitutes sensitive data? In order to protect data, we must first understand (or know) our data.
- **Proactive data security goes beyond technology implementation.** Technology is only one part of the equation. People and processes matter. Data privacy and security are conjoined concepts that require coordination between people and processes to successfully address these concerns.
- **Many firms struggle with data security and are not mature in measuring the success of data security initiatives.** The transition from network and device-centric security to data-centric security is new to most enterprises. There is a significant cultural shift that must take place in order for organizations to mature their data security practices.
- **For better or worse, breaches are an organizational catalyst.** As a direct result of a data breach, 45% of firms implemented new security controls and policies, and 42% said that security and privacy have become bigger topics of discussion. However, 35% also indicated that the breach caused a lot of disruption in the organization, with 18% of companies laying off employees as a direct result of a breach.

Data Security Is On The Executive Agenda, But Investment Is Stalling

Data security today has catapulted into the board room as a serious topic of business discussion. The relentless pursuit of customer data and intellectual property by cybercriminals and other attackers like state-sponsored actors has painted bright targets on the backs of businesses of all shapes and sizes. An organization's data security posture — or lack thereof — has implications for brand reputation, revenue growth, and long-term competitiveness in a digital world. Following a customer data breach in late 2013, a major retailing company laid off 475 employees, saw the departure of its CIO and CEO, and watched profits drop 46% in the fourth quarter over the same period the year.[1] In the final months of 2013, an estimated $61 million was spent dealing with the breach, with an additional $168 million spent in Q2 2014.[2] As of May 2014, the retailing company is wrestling with more than 140 lawsuits.[3] Executives see on a near daily basis news and reports of data breaches in other companies, and naturally, ask, "Could this happen to us?" Business leaders are:

› **Increasing attention and focus on data security.** Data security and privacy is now an organization-wide discussion and not just limited to IT. In response to awareness of high-profile cyberattacks that have happened to other organizations, executives today are asking questions and increasing the organization's focus on IT security and data protection (see Figure 1).

› **Pausing when it comes to funding or investment.** Unfortunately for many firms, the increased attention and focus hasn't translated into action in the form of earmarking adequate funding or investment to make meaningful changes or provide the ability to enforce policy. Ten percent of firms haven't changed anything, and about 34% of organizations today have increased security funding as a result. Executives often think in terms of ROI on investment. Yet, IT security faces challenges with articulating value — not just about data security investments but also about what constitutes sensitive data and the value of this data — and providing a business case and metrics that resonate with executives.

FIGURE 1
High-Profile Cyber Attacks Have Raised Executives' Awareness Of IT Security

Base: 200 security decision-makers in the US, UK, and Germany

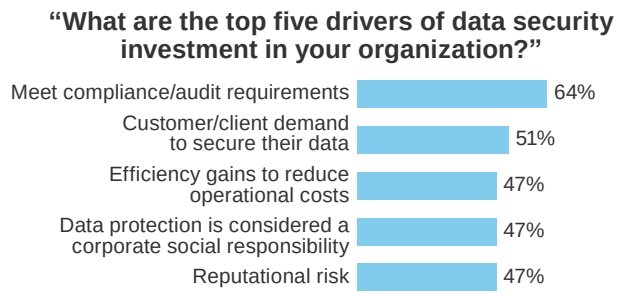
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

Compliance And Breaches Remain Primary Drivers For Tactical Action

Organizations are in a constant struggle to keep up amid challenges surrounding security budget, skills, and staffing, and the changing nature of threats. This is not news to many security professionals. However, combined with the dual challenge of articulating security value and value of sensitive data, firms have gravitated toward continuously operating in a responsive fashion with regards to data security where:

› **Compliance is the path of least resistance.** Compliance is non-negotiable; it simply must be done. Executives understand this, view it as a cost of doing business, and budget accordingly — making it easier for IT and security to justify investments here, especially in industries where there are strong compliance regulations. Compliance remains by far the top driver for security investment today (see Figure 2).

FIGURE 2
Top Five Drivers Of Data Security Investment



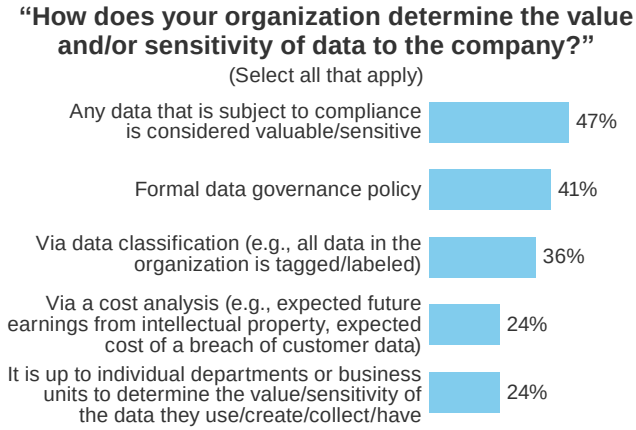
Base: 200 security decision-makers in the US, UK, and Germany

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

- **Firms mistakenly equate compliance with security.** Both executives and IT and security professionals alike get caught up in efforts to meet compliance and easily forget that merely being compliant with requirements does not mean the organization's data is secure. Compliance is the bare minimum and not a substitute for a robust security strategy. Compliance standards also take time to change, whereas threats and technology are constantly evolving.[4] As a result, it's not unusual to see compliant companies still getting breached.[5] Meeting compliance requirements and fulfilling a checklist puts more of the attention on ensuring a good snapshot at one point in time rather than sustained focus on implementing and maintaining a continuous program.

- **Companies are unclear about what constitutes sensitive data.** What is considered sensitive data in your organization? And is this understanding consistent across departments in the company? Often the answer is no, and that in itself is a problem. Organizations cannot expect to protect something if they don't know what they are trying to protect. Many firms typically consider any data subject to compliance initiatives as sensitive, rather than rely on other means like data classification, cost analysis, or involvement from the rest of the business (see Figure 3). Companies that take this approach are more likely to leave other sensitive data like intellectual property exposed to a breach as a result. Study participants provided a wide spread and range of responses. When asked about how much of their organization's data is considered sensitive, some indicated that all of the data in the organization (100% of it) is sensitive data, while others indicated that only 10% of their data is sensitive. This suggests a lack of awareness about what data is actually sensitive (see Figure 4). If 100% of the data in an organization is sensitive, can we assume that a company believes public-facing information, such as copies of their public SEC filings and product information fact sheets, is sensitive and in need of protection?

FIGURE 3
Companies Lack Awareness And Clear Understanding About What Data Is Sensitive



Base: 200 security decision-makers in the US, UK, and Germany

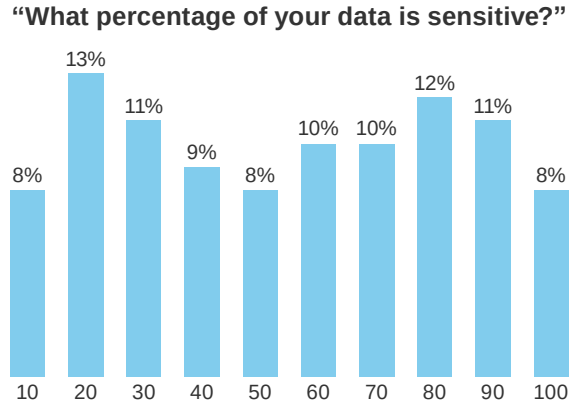
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

"We are driven by regulators, compliance, risk, and also reputation — that's high up in the management side."

— Head of IT at a UK-based financial company

FIGURE 4

Spread And Range Of Response Suggest Lack Of Awareness About What Data Is Sensitive



Base: 200 security decision-makers in the US, UK, and Germany

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

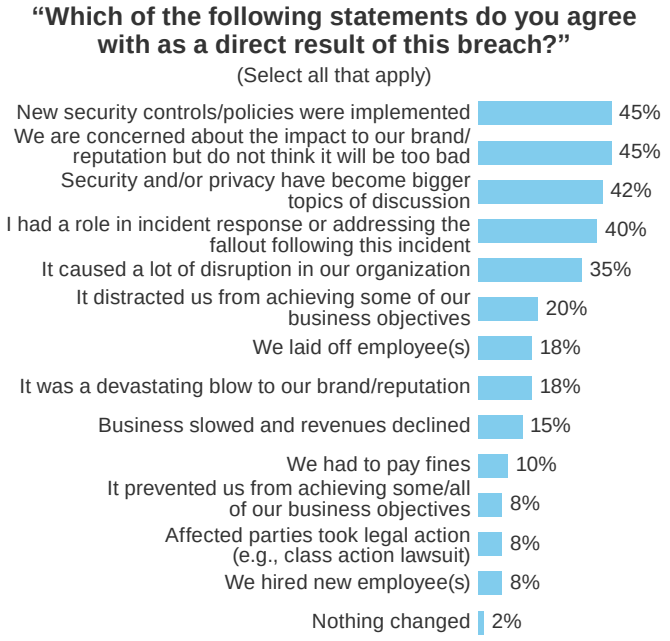
› **For many, a data breach is the only wake-up call — and a costly one.** Following a breach, 35% of firms said they experienced a lot of disruption, and 45% indicated that they implemented new security controls and policies as a result (see Figure 5). Jobs are also on the line — 18% of organizations told us that layoffs followed a data breach. More often than not, firms are simply taking action as issues crop up and hoping for the best. This focus on tactical measures misses the important goal of executing on a more holistic and strategic plan for data security. In addition, this reactive tactical approach disrupts efforts to measure ROI on security investments.

"To what degree those risks are articulated to the bottom line or quantitative perspective, I don't know. But from a qualitative perspective, these things significantly affect reputation and bottom line."

— Head of innovation and knowledge management at a Germany-based manufacturing company

FIGURE 5

Companies Are Most Likely To Put In Place New Security Controls Following A Data Breach



Base: 40 security decision-makers in the US, UK, and Germany

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

Proactive Data Security Requires A Strategic Approach

Good data security and control is more than just doing what is needed to stop bad things from happening, whether it's a data breach, a failed audit, or files and penalties for noncompliance. Realize that there are real business opportunities for proactive data security. Identify how the business wants to use data, what data is required, and how to source this data. In a digital and data-driven economy where big data analytics gains momentum and the race to better understand and anticipate customer demands and preferences intensifies, data security and privacy — and data quality — will be key enablers. Lines of business like marketing and sales see this more clearly today compared with technology decision-makers. In a world where always connected consumers can quickly and easily share their views and hear about other consumers' experiences with a company or service, business reputations can either garner and sustain goodwill or quickly crumble. About a third of firms

in this study that have experienced a breach indicated that the breach affected both their reputation and bottom line.[6] Don't wait until after a breach to take action to protect the brand.

Proactive businesses view data security and privacy today as a cost of doing business; business partners and customers implicitly expect and in some cases have specific requirements for it. This is evidenced by security requirements set out in service-level agreements (SLAs) and contracts, in addition to the flurry of lawsuits that follow a customer data breach. It will not be long before we see data security and privacy emerge as a business differentiator. Companies that are proactive in their efforts will have a competitive edge in this digital and data-driven economy.

"To be proactive means not waiting until an issue arises, [and taking action] before security breaches."

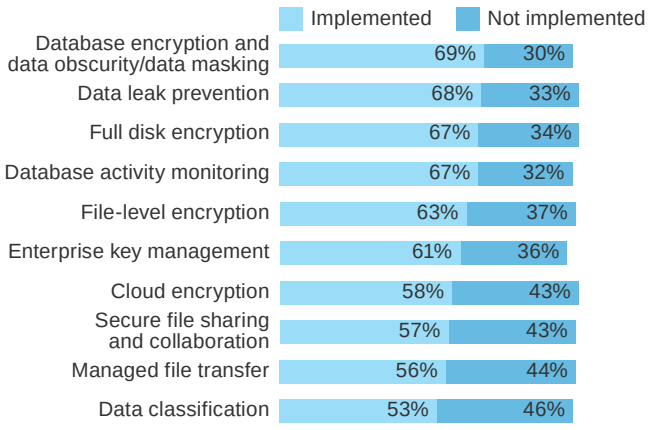
— AVP information security at a US-based financial company

Companies that already have security policies in place tend to want to jump straight to implementing technologies to help enforce policies for data protection. For example, encryption and data leak prevention (DLP) are among the top technology tools in use today (see Figure 6). While necessary, this is only one part of a data protection strategy. Firms must approach data security in a more holistic manner. Doing so not only paves a more secure route to achieving other technology and business initiatives like adopting cloud services or creating more engaging interactions with your customers, but it also encourages more efficient security investment (in terms of both time and effort). Forrester's data security and control framework breaks data protection strategy down into three main phases:

- **Define your data.** This involves data discovery (inventory) and classification. Understand where the organization's data is located and its sensitivity. Know what you are trying to protect in order to better identify the appropriate policies and technologies required for data security and privacy.
- **Dissect your data.** This effort comprises a combination of security data analytics and intelligence. Use your security data (information collected via security technologies like security information management tools or network analysis and visibility tools) to help protect your sensitive data. Get as close as you can to a near-time view of what goes on in the corporate network, and understand how data flows through the organization. Data activity monitoring can help uncover anomalous behaviors indicative of security and privacy violations. Does sensitive data traverse to — or originate from — any surprising or strange places?
- **Defend your data.** Last but not least, this phase is about four key data protection technologies and techniques: 1) access control to ensure only authorized users have access; 2) inspection of data usage patterns to spot suspicious activity, not taking access controls for granted; 3) data disposal for data that is no longer needed for business purposes; and 4) encryption, tokenization, and data masking to hinder use of the sensitive data in the event it is stolen or compromised.

FIGURE 6

Encryption And DLP Are Among The Top Data Security Technologies Implemented Today



Base: 200 security decision-makers in the US, UK, and Germany

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

Key Recommendations

In a world where deperimeterization has loosened our control of our networks and the rise of personally owned mobile devices and cloud has made device security largely irrelevant, it is important that the future of security lies in data-centric security. Protect the data. Data is the thing that gets organizations in trouble with legal entities and regulatory organizations. But data security is about a program and not a product. It is a way of doing business. In a world ever more dominated by mobility and cloud services, data security is just good business. An organization's data assets — including customer data, customer analytics and insights, business analytics, and intellectual property — are a critical resource that supports revenue growth and competitive advantage. In the data economy, organizations will implement and find new ways to value and monetize their data assets. Firms that fail to protect these crown jewels will struggle to grow, garner customer trust, and successfully respond to market demands.

In order to achieve a more data-centric security posture, you should:

- **Appoint a data champion.** A data champion is someone who is responsible for overseeing the organization's use of data — everything from data collected from customers to data created by the company (intellectual property) to data that the firm may monetize. This data champion has a vested interest in ensuring not just data quality, but data security as well. Understand that IT is not a data owner; the business owns the data. Organizations need data users to give context about the data and help in defining data (what it is, how sensitive the data is, and what it is used for). A data champion can help to rally data users and owners to provide input for technology decisions and influence internal resources for data protection.
- **Rethink your existing approach.** The use of a data security and control framework is just one component of a holistic approach that looks at people, processes, and technology, albeit an important one. A key consequence of disappearing perimeters is that traditional models of information security are now woefully inadequate. Perimeter-based security and the longstanding adage of "trust, but verify" is no longer sufficient. Today's data economy requires a new approach: the Zero Trust Model of information security.[7] The Zero Trust approach eliminates the concept of a "trusted" network (usually the corporate network) and "untrusted" network; in Zero Trust, all networks are untrusted and organizations must: 1) verify and secure all resources regardless of location; 2) limit and strictly enforce access control across all user populations, devices/channels, and hosting models; and 3) log and inspect all traffic, both internal and external.
- **Focus on your people.** A hyper-focus on external threats and attackers makes it easy to neglect internal threats — your employees. Many data loss events caused by internal sources might have been preventable. Proactive data security is more than just policies and technologies that detect suspicious behavior or attacks. An uninformed workforce and declining security staff are detrimental to data security efforts. Make sure employees are aware of how to securely handle data and the consequences of data loss. Pay attention to your security staff too to prevent burnout. Create opportunities for skills and career development to keep security staff engaged and reduce turnover. Also, be cognizant of the personnel and management requirements that security technologies and tools can require, and look to automate functions and reduce tool management burdens where possible to free up security staff time from handling more tactical issues to more strategic ones.
- **Expand the concept of compliance.** Compliance is not going away, but good security practices make it easier for firms to meet compliance requirements. Plus, by looking at security and compliance more holistically, compliance initiatives can unlock security budgets. The dissecting data phase of the data security and control framework is more than just about technology. In this phase, compliance and proactive data security can converge. Apply the concept of dissecting to develop a better understanding of data security strategy inputs like compliance requirements and privacy principles. And develop privacy legislation, consumer perceptions, and response toward data breaches. Use this knowledge to further inform your data security policies and processes. Continue to invest in compliance, but minimize cost (and therefore increase ROI) by implementing the flexibility

necessary to address new regulations before they happen. Remember that compliance requirements take time for standards bodies to change. Plan to get ahead of the risk.

- **Make sure you track business-relevant metrics.** Is there any report or dashboard to show how the organization is doing? And more importantly, what does that reporting enable in terms of actions? Security data gathered from security technologies and tools can provide useful information for the security team but not the business. The board is unlikely to care about the number of intrusions detected or variants of malware identified. Pinpoint the key questions — the things that the security team is accountable for — from the board and the business. Develop and track key business-relevant security metrics to help answer those questions. At the top of your list should be a metric on data exfiltration to help answer the question: Did sensitive data leave the organization?

Appendix A: Methodology

In this study, Forrester conducted five in-depth interviews and an online survey of 200 organizations in the US, UK, and Germany to evaluate the benefits of proactive effort in data security and privacy. Survey participants included security decision-makers in IT and line of business. Questions provided to the participants asked about their current data security measures and their investments in it. Respondents were offered incentives as a thank you for time spent on the survey. The study began in May 2014 and was completed in June 2014.

Appendix B: Endnotes

[1] Source: Elizabeth A. Harris, "Target Executive Resigns After Breach," The New York Times, March 5, 2014 (http://www.nytimes.com/2014/03/06/business/a-top-target-executive-resigns.html) and Meagan Clark, "Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer," International Business Times, May 5, 2014 (http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056).

[2] Source: Elizabeth A. Harris, "Target Executive Resigns After Breach," The New York Times, March 5, 2014 (http://www.nytimes.com/2014/03/06/business/a-top-target-executive-resigns.html).

[3] Source: Jeffrey Roman, "Target Breach Lawsuits Consolidated," BankInfoSecurity, May 15, 2014 (http://www.bankinfosecurity.com/target-breach-lawsuits-consolidated-a-6845/op-1).

[4] For example, the definition of personal healthcare data in HIPAA currently does not consider consumer-generated healthcare information (such as data from a fitness tracking device or a health score). Yet, this is data that can be sensitive in nature and used by businesses (e.g., insurance providers, hospitals, pharmaceuticals) in ways that consumers find objectionable and in violation of their privacy. Source: Katie Wike, "HIPAA Doesn't Cover All Personal Health Data," Health IT Outcomes, July 25, 2014 (http://www.healthitoutcomes.com/doc/hipaa-doesn-t-cover-all-personal-health-data-0001).

[5] Target was certified as compliant with PCI-DSS in September 2013, before a data breach occurred in the following months. Source: John P. Mello Jr., "Target Breach Lesson: PCI Compliance Isn't Enough," TechNewsWorld, March 18, 2014 (http://www.technewsworld.com/story/80160.html).

[6] Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014.

[7] Source: Brian Robinson, "'Trust but verify' is so last year," GCN, January 21, 2014 (http://gcn.com/Articles/2014/01/21/zero-trust.aspx).