A Forrester Consulting Thought Leadership Paper Commissioned By Microsoft And RSA, The Security Division Of EMC

# The Value Of Corporate Secrets

How Compliance And Collaboration Affect Enterprise Perceptions Of Risk

March 2010

**Headquarters | Forrester Research, Inc.**
400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | www.forrester.com

Forrester Consulting
Making Leaders Successful Every Day

## 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 www.forrester.com/consulting.

## Executive Summary

In November 2009, Microsoft and RSA, the security division of EMC, commissioned Forrester Consulting to assess the data security practices of North American, European, and Australian enterprises. We sought to understand: 1) the value of sensitive information contained in enterprise portfolios; 2) the security controls used to protect this information; 3) the drivers of information security programs; and finally, 4) the cost and impact of enterprise data security incidents. For this report, Forrester conducted 305 in-depth surveys with IT security decision-makers to understand how enterprises value and protect their enterprise information portfolios.

### Key Findings

Enterprises' chief information security officers (CISOs) face increasing demands from their business units, regulators, and business partners to safeguard their information assets. Security programs protect two types of data: *secrets* that confer long-term competitive advantage and *custodial data* assets that they are compelled to protect. Secrets include product plans, earnings forecasts, and trade secrets; custodial data includes customer, medical, and payment card information that becomes "toxic" when spilled or stolen. We found that enterprises are overly focused on compliance and not focused enough on protecting their secrets. Our key findings are the following:

- **Secrets comprise two-thirds of the value of firms' information portfolios.** Despite the increasing mandates enterprises face, custodial data assets aren't the most valuable assets in enterprise information portfolios. Proprietary knowledge and company secrets, by contrast, are twice as valuable as the custodial data. And as recent company attacks illustrate, secrets are targets for theft.

- **Compliance, not security, drives security budgets.** Enterprises devote 80% of their security budgets to two priorities: compliance and securing sensitive corporate information, with the same percentage (about 40%) devoted to each. But secrets comprise 62% of the overall information portfolio's total value while compliance-related custodial data comprises just 38%, a much smaller proportion. This strongly suggests that investments are overweighed toward compliance.

- **Firms focus on preventing accidents, but theft is where the money is.** Data security incidents related to accidental losses and mistakes are common but cause little quantifiable damage. By contrast, employee theft of sensitive information is 10 times costlier on a per-incident basis than any single incident caused by accidents: hundreds of thousands of dollars versus tens of thousands.

- **The more valuable a firm's information, the more incidents it will have.** The "portfolio value" of the information managed by the top quartile of enterprises was 20 times higher than the bottom quartile. These high-value enterprises had four times as many security incidents as low-value firms. High-value firms are not sufficiently protecting data from theft and abuse by third parties. They had six times more data security incidents due to outside parties than low-value firms, even though the number of third parties they work with is only 60% greater.

- **CISOs do not know how effective their security controls actually are.** Regardless of information asset value, spending, or number of incidents observed, nearly every company rated its security controls to be equally effective — even though the number and cost of incidents varied widely. Even enterprises with a high number of incidents are still likely to imagine that their programs are "very effective." We concluded that most enterprises do not actually know whether their data security programs work or not.

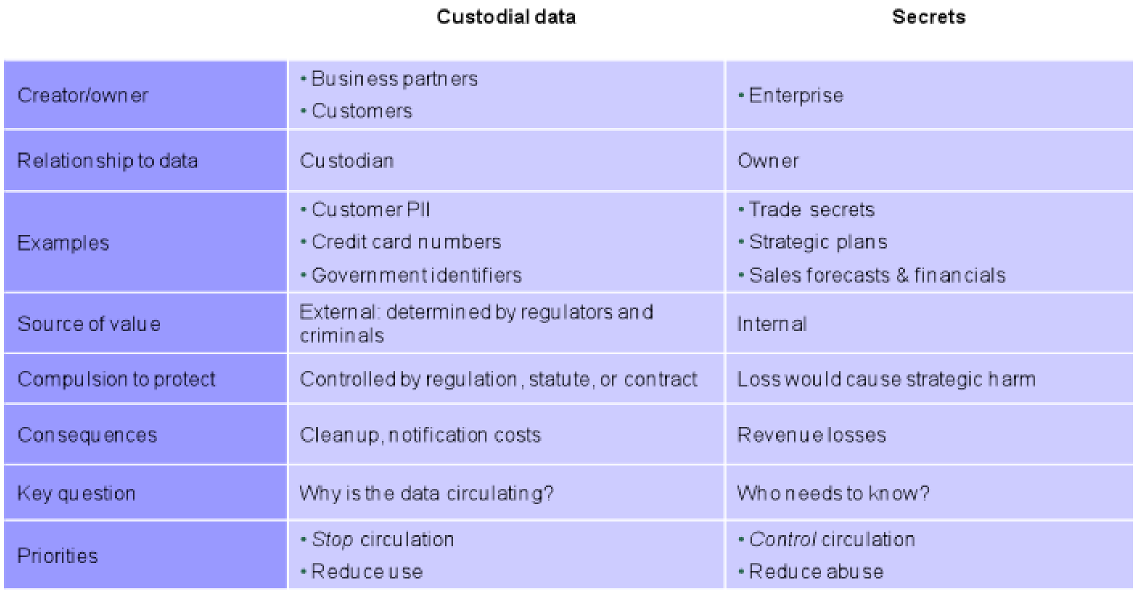
The sections that follow explain our findings in detail.

## Secrets Comprise Two-Thirds Of The Value Of Firms' Information Portfolios

Enterprise information portfolios contain everything from cardholder details and customer records to unstructured documents that contain intellectual property. We identified two kinds of information that have clear and tangible value. Proprietary company *secrets* generate revenue, increase profits, and maintain competitive advantage. In addition, *custodial data* such as customer, medical, and payment card information has value because regulation or contracts make it toxic when spilled and costly to clean up. We explain each below.

*Secrets* refer to information that the enterprise creates and wishes to keep under wraps. Secrets tend to be messily and abstractly described in Word documents, embedded in presentations, and enshrined in application-specific formats like CAD. Secrets that have intrinsic value to the firm are always specific to the enterprise's business context. An interested party could cause long-term competitive harm if it obtains these secrets. Keeping proprietary knowledge away from competitors is essential to maintaining market advantage (see Figure 1).

**Figure 1**
Secrets Versus Custodial Data



| | Custodial data | Secrets |
|---|---|---|
| Creator/owner | • Business partners<br>• Customers | • Enterprise |
| Relationship to data | Custodian | Owner |
| Examples | • Customer PII<br>• Credit card numbers<br>• Government identifiers | • Trade secrets<br>• Strategic plans<br>• Sales forecasts & financials |
| Source of value | External: determined by regulators and criminals | Internal |
| Compulsion to protect | Controlled by regulation, statute, or contract | Loss would cause strategic harm |
| Consequences | Cleanup, notification costs | Revenue losses |
| Key question | Why is the data circulating? | Who needs to know? |
| Priorities | • *Stop* circulation<br>• Reduce use | • *Control* circulation<br>• Reduce abuse |

Source: Forrester Research, "Selecting Data Security Technologies," December 2009.

Companies in knowledge-intensive industries such as aerospace and defense, electronics, and consulting generate large amounts of confidential intellectual property that present barriers to entry for competitors. Unlike with toxic data spills, failures to protect secrets are almost never made public. And in January 2010, a major search engine revealed that Chinese attackers compromised its computers and stole valuable intellectual property.[1]

By contrast, legislation, regulation, and contracts compel enterprises to protect *custodial data*. Mandates that oblige enterprises to be good custodians include contractual obligations like the Payment Card Industry Data Security Standard (PCI-DSS) and data breach and privacy laws.

Custodial data has little intrinsic value in and of itself. But when it is obtained by an unauthorized party, misused, lost, or stolen, it changes state. Data that is ordinarily benign transforms into something harmful. When custodial data is spilled, it becomes "toxic" and poisons the enterprise's air in terms of press headlines, fines, and customer complaints. Outsiders, such as organized criminals, value custodial data because they can make money with it. Custodial data also accrues indirect value to the enterprise based on the costs of fines, lawsuits, and adverse publicity.

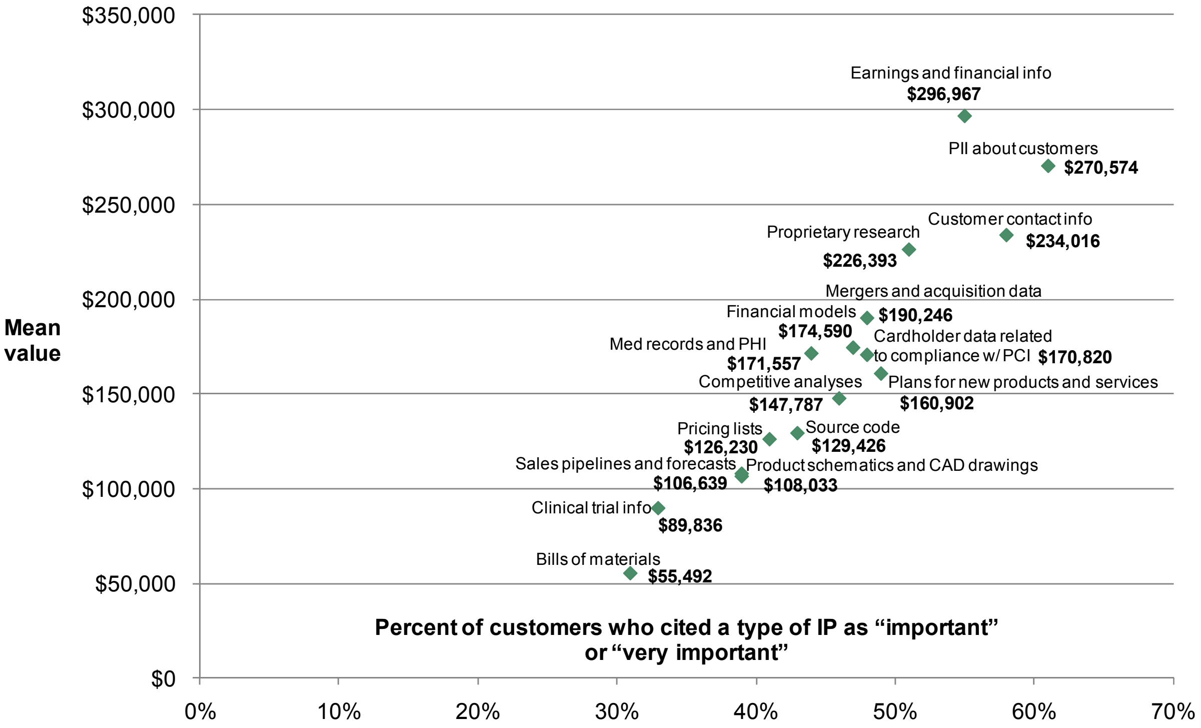
Examples of custodial data include customer personally identifiable information (PII) attributes like name, address, email, and phone number; government identifiers; payment card details like credit card numbers and expiration dates; and medical records and government identifiers like passport number and Social Security Number. Many well-known firms have graced the front pages of major newspapers with toxic data spills.

## Secrets Are Much More Valuable Than Custodial Data

Catastrophic toxic data spills are dramatic and expensive, and they garner the most headlines. But for most enterprises, secrets are more valuable than custodial data. For this survey, we asked respondents to identify the five most valuable assets in their information portfolios out of 17 possible types of information ranging from sales forecasts to cardholder data. For purposes of simplicity, we constrained the maximum value to $1 million. On average, enterprises valued their top five assets at $2.7 million in aggregate. Significantly, two-thirds of the value comes from secrets, not custodial data (see Figure 2).

**Figure 2**

Enterprises' Information Portfolios Are Worth $2.7 Million, 62% Of Which Derives From Secrets



Base: 305 senior-level IT security decision-makers

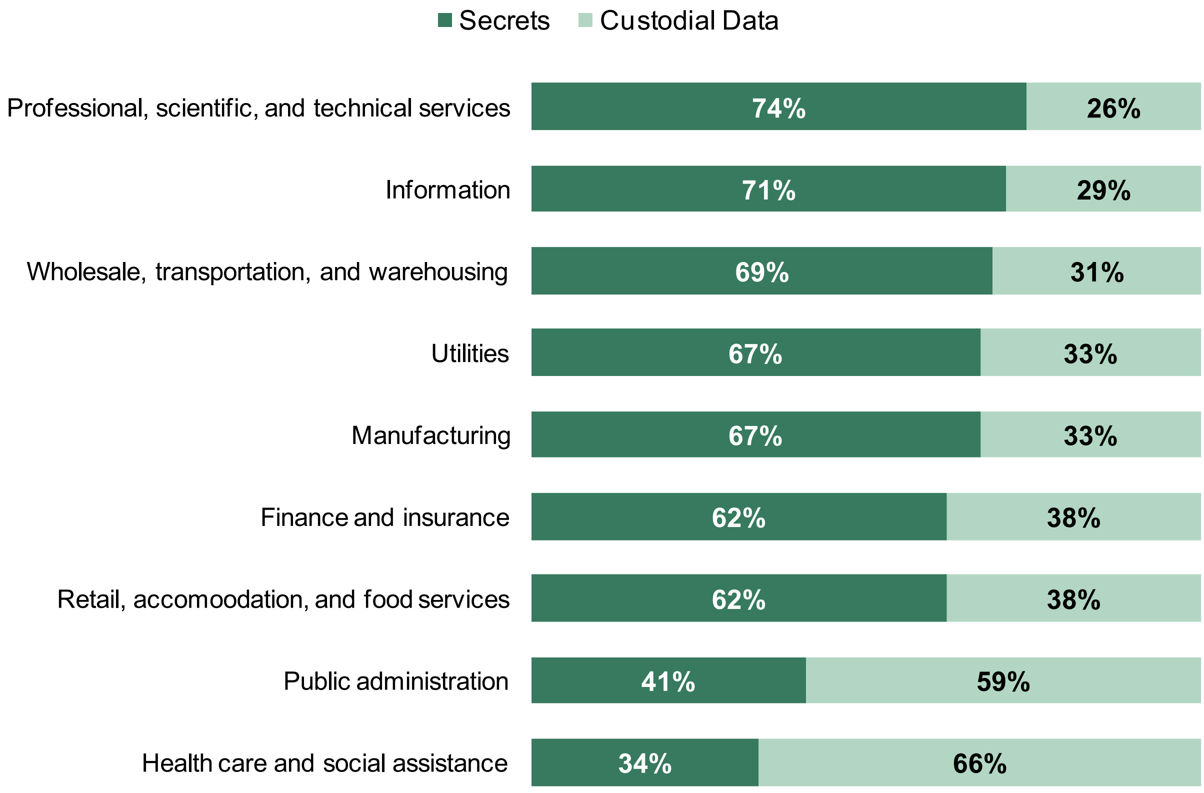
Source: A commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

Earnings and financial information is the most valuable single data type, worth $297,000 on average against a maximum possible value of $1 million. Bills of materials are valued lowest, at $55,492 (see Figure 2).

We found significant differences between verticals. Enterprises in highly knowledge-intensive industries like manufacturing, information services, professional, scientific and technical services, and transportation accrue between 70% and 80% of their information portfolio value from secrets. By contrast, healthcare firms and governmental entities are nearly exactly the opposite. Three-fifths or more of the value of their information assets are custodial data assets (see Figure 3).

**Figure 3**

Knowledge Industries Derive 70% Of Their Information Value From Secrets



Base: 305 senior-level IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

**Conclusion:** Enterprise secrets are an underappreciated and underprotected information asset. Poor custodianship of customer and cardholder data by companies results in high-profile toxic data spills. But in most industries, this is only one-third of the value at risk. Two-thirds of enterprises' information portfolio value comes from the secrets they create. As the recent industrial espionage attack on a large search engine company illustrates, the threat landscape has not changed, but our perception of it has.[2] Targeted zero-day attacks are routine, particularly against government agencies and in the aerospace and defense sectors. What is new is that we are now seeing headlines about it. This search engine's admission that it lost some of its secrets in the recent attack shows that securing trade secrets deserves just as much attention as the toxic stuff.

## Compliance, Not Security, Drives Security Budgets

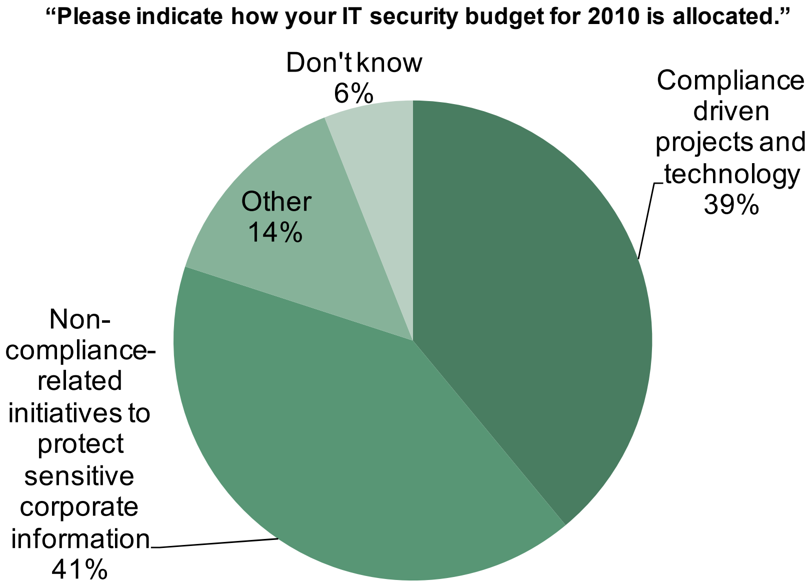
In the past five years, "compliance" of all types has become the primary driver of data security programs. Nearly 90% of enterprises we surveyed agreed that compliance with PCI-DSS, data privacy laws, data breach regulations, and existing data security policies is the primary driver of their data security programs.[3]

A significant percentage of enterprise budgets (39%) is devoted to compliance-related data security programs (see Figure 4). When we dug deeper, Forrester found that while all types of compliance have an influence on budgets, compliance with internal security policies is slightly more likely to move budgets than the statutory and regulatory kind. Nearly 70% of enterprises said that compliance with internal security policies had caused them to spend more time, money, or effort protecting their data. Slightly lower percentages cited compliance with statutes and regulations (62%) and contractual obligations like PCI-DSS (60%). No doubt all of these factors are mutually reinforcing.[4]

**Conclusion:** Companies are underinvesting in programs for protecting their secrets. Interestingly, the percentage of budget spent on compliance programs is nearly identical to the percentage of enterprise information value that can be attributed to custodial data (38%). Only 41% of enterprise data security budgets were spent on securing non-compliance-related types of sensitive corporate information, compared with 62% of the overall information portfolio's total value.

**Figure 4**

Compliance Drives Budgets, But Enterprises Underinvest In Other Data Security Areas



Base: 305 senior-level IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

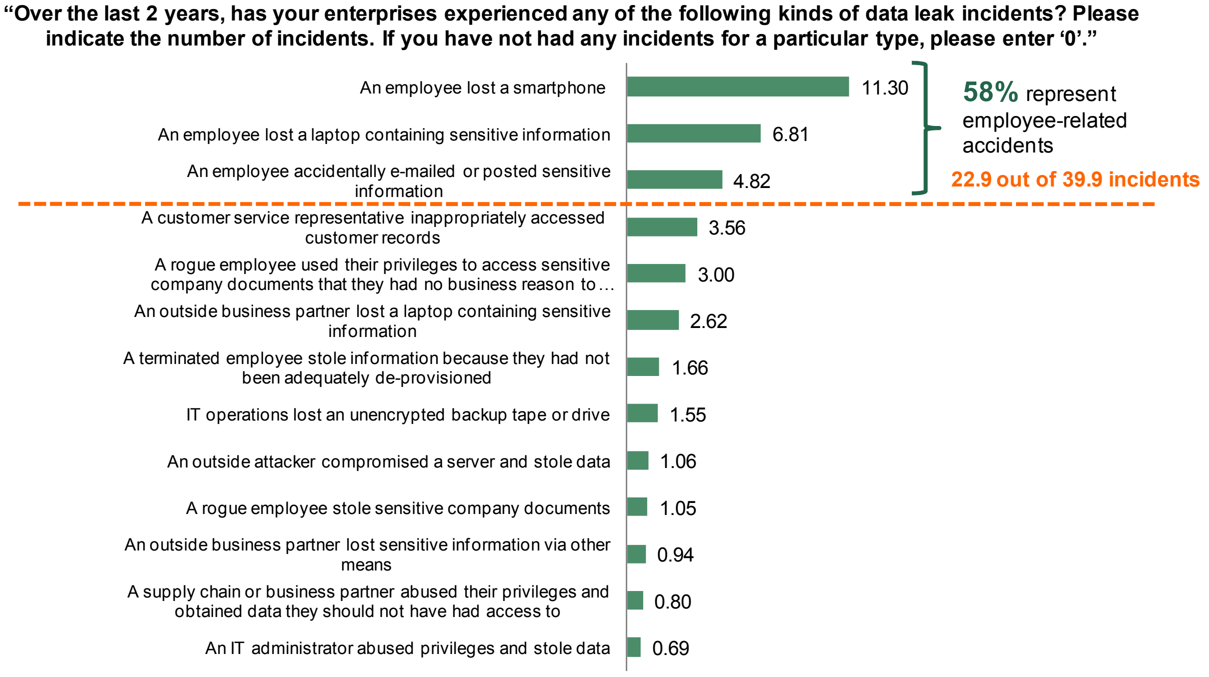
## Firms Focus On Preventing Accidents, But Theft Is Where The Money Is

Enterprise perceptions of *risk* — the types of data security incidents that are most likely, and their magnitude — show that enterprise perceptions are oriented toward preventing accidents. We asked security decision-makers to identify the likelihood of 13 specific sources of data security incidents, such as misplacement of an employee device, theft by a privileged insider, an outsourced call center, and a variety of other sources. We also asked respondents to count the number of incidents they had actually experienced in the past two years.

Enterprise perceptions of incident likelihood were backed up by the incidents they experienced. A majority of enterprises felt that employee-related accidents were the most likely sources. Theft or misplacement of an employee device was seen as likely or extremely likely by 58% of respondents, while the risk of accidental leakage by an employee was seen as nearly as risky (57%). And indeed, the top three actual incidents reported *were* all employee-related accidents. Enterprises lost, on average, 11 company-owned smartphones and seven laptops during the past two years. Employees accidentally emailed or posted sensitive information five times. Of the roughly 40 incidents, these three types comprised two-thirds of the total count (see Figure 5).

**Figure 5**

Employee Toxic Data Accidents Represent 57% Of Incidents . . .



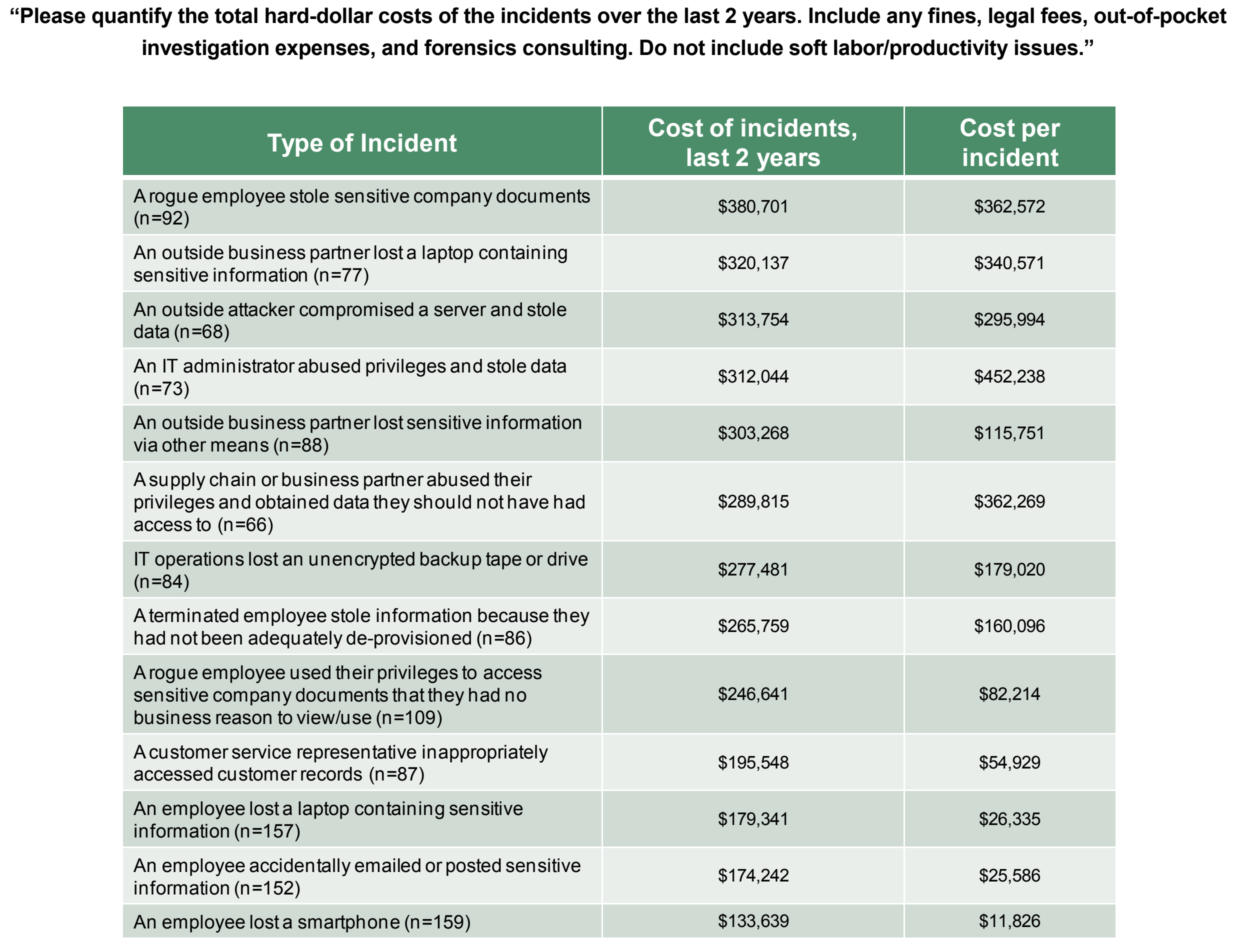
Base: 305 senior-level IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

However, the amount of *damage* that employee-related accidents caused was quite low relative to other types. When we asked enterprises to quantify the hard-dollar costs of the incidents they experienced, the most common incidents were also shown to be the *least costly*. The total cost for all lost smartphone incidents was $134,000, with about half incurring minimal or no costs. The average cost per incident was $12,000 (see Figure 6). Lost laptop incidents incurred slightly more cost and were slightly more serious, with a total cost of $179,000 and a per-incident cost of $26,000. Accidental leakages incurred just $174,000 in total cost and had a per-incident cost of $26,000.

**Figure 6**

. . . But Insider Theft Of Secrets And Other Unstructured Documents Was The Most Costly Type Of Incident



**“Please quantify the total hard-dollar costs of the incidents over the last 2 years. Include any fines, legal fees, out-of-pocket investigation expenses, and forensics consulting. Do not include soft labor/productivity issues.”**

| Type of Incident | Cost of incidents, last 2 years | Cost per incident |
|---|---|---|
| A rogue employee stole sensitive company documents (n=92) | $380,701 | $362,572 |
| An outside business partner lost a laptop containing sensitive information (n=77) | $320,137 | $340,571 |
| An outside attacker compromised a server and stole data (n=68) | $313,754 | $295,994 |
| An IT administrator abused privileges and stole data (n=73) | $312,044 | $452,238 |
| An outside business partner lost sensitive information via other means (n=88) | $303,268 | $115,751 |
| A supply chain or business partner abused their privileges and obtained data they should not have had access to (n=66) | $289,815 | $362,269 |
| IT operations lost an unencrypted backup tape or drive (n=84) | $277,481 | $179,020 |
| A terminated employee stole information because they had not been adequately de-provisioned (n=86) | $265,759 | $160,096 |
| A rogue employee used their privileges to access sensitive company documents that they had no business reason to view/use (n=109) | $246,641 | $82,214 |
| A customer service representative inappropriately accessed customer records (n=87) | $195,548 | $54,929 |
| An employee lost a laptop containing sensitive information (n=157) | $179,341 | $26,335 |
| An employee accidentally emailed or posted sensitive information (n=152) | $174,242 | $25,586 |
| An employee lost a smartphone (n=159) | $133,639 | $11,826 |

Base: 305 senior-level IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

By contrast, malicious theft by insiders and third parties was much costlier. Although enterprises reported, on average, only one incident where a rogue employee stole sensitive company documents, that one incident was the most costly of incident types: $380,000 in absolute terms, or roughly $363,000 per incident. Damage caused by a rogue IT administrator was even more costly on a per-incident basis, at $452,000. To put this in perspective, this means that employee theft of sensitive information is 10 times costlier on a per-incident basis than any single incident caused by employee accidents.

**Conclusions:** Enterprise security investments are overly biased toward preventing employee mistakes rather than securing the critical secrets that confer long-term competitive advantage. Many of the security controls that are believed to be "best practices" — full-disk encryption on laptops, data leak prevention (DLP) policies for detecting protected health information (PHI) or PII, and device control software — are designed to reduce the impact of employee accidents. Today, these controls are most commonly used to reduce the frequency of toxic data spills of custodial data. But they are used less often to prevent theft. Enterprises should focus more of their resources on stopping the most damaging incidents: deliberate theft by insiders and abuse by outsiders.

## The More Valuable A Firm's Information, The More Incidents It Will Have

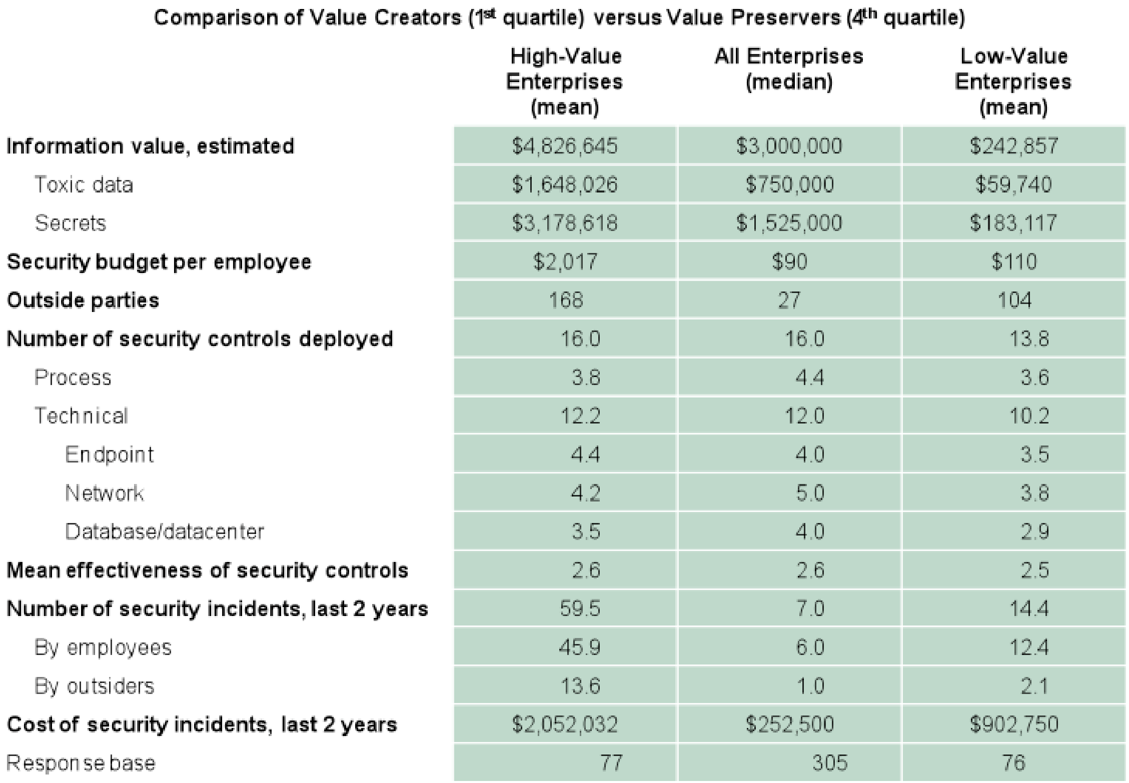
For 90% of enterprises, collaboration tools that cross company lines are essential to the success of their businesses.[5] The average enterprise in our survey works with more than 100 third parties. Nearly three-quarters of this total comes from links with contract professionals (30, on average), supply chain partners (29), and contract manufacturers (16). Regulatory agencies, CPAs, healthcare providers, and other organizations make up the rest.[6]

Forrester hypothesized that enterprises with the most valuable and widely shared information would incur far higher incident costs than others. To test this hypothesis, we divided the enterprises we surveyed into quartiles based on the value of their enterprise information portfolios. The top quartile based on enterprise information value, which we call the high-value quartile, manages information worth $4.8 million out of a maximum possible value of $5 million, of which $3.1 million is secrets and $1.6 million is toxic data (see Figure 7).[7] The bottom quartile, called the low-value quartile, manages just $243,000 in information assets. In other words: High-value enterprises' information is worth at least 20 times that of the low-value enterprises.

We noticed important differences in several key characteristics of high-value enterprises compared with the low-value enterprises. First, the number of connections with outside parties was much higher. High-value enterprises had 60% more relationships with outside third parties than low-value firms (168 parties versus 104). Second, high-value firms used more security controls than low-value firms. High-value firms have deployed approximately 16 process, endpoint, network, and data center controls to protect sensitive data, compared with 13.8 for low-value firms. Most of the difference is explained by technology (12.2 technical controls versus 10.2).[8]

Third, we noticed a striking difference in the number and kind of data security incidents that each group experienced. High-value firms reported four times as many data security incidents as low-value firms — about 60 (59.5) over a two-year period compared with about 15 (14.4). The roughly 4:1 proportion of incidents was true not just overall but with respect to incidents due to employees also. But with the difference in the number of outsider incidents, it was six times higher with high-value versus low-value firms. The more third-party connections an enterprise has, the more incidents it will have that come from outsiders.

**Figure 7**
Firms With High-Value Information Portfolios Gain More, And Spend More, Than Low-Value Firms



Comparison of Value Creators (1st quartile) versus Value Preservers (4th quartile)

| | High-Value Enterprises (mean) | All Enterprises (median) | Low-Value Enterprises (mean) |
|---|---|---|---|
| **Information value, estimated** | $4,826,645 | $3,000,000 | $242,857 |
| Toxic data | $1,648,026 | $750,000 | $59,740 |
| Secrets | $3,178,618 | $1,525,000 | $183,117 |
| **Security budget per employee** | $2,017 | $90 | $110 |
| **Outside parties** | 168 | 27 | 104 |
| **Number of security controls deployed** | 16.0 | 16.0 | 13.8 |
| Process | 3.8 | 4.4 | 3.6 |
| Technical | 12.2 | 12.0 | 10.2 |
| Endpoint | 4.4 | 4.0 | 3.5 |
| Network | 4.2 | 5.0 | 3.8 |
| Database/datacenter | 3.5 | 4.0 | 2.9 |
| **Mean effectiveness of security controls** | 2.6 | 2.6 | 2.5 |
| **Number of security incidents, last 2 years** | 59.5 | 7.0 | 14.4 |
| By employees | 45.9 | 6.0 | 12.4 |
| By outsiders | 13.6 | 1.0 | 2.1 |
| **Cost of security incidents, last 2 years** | $2,052,032 | $252,500 | $902,750 |
| Response base | 77 | 305 | 76 |

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009

Moreover, high-value firms incurred much higher incident costs than the low-value firms. A typical high-value firm's cost of incidents, at $2.05 million over two years, was 50% more than the mean for all enterprises ($1.3 million). The high-value firms' per-incident costs, at $35,000 per incident, are comparable with the mean for all companies ($33,000). High-value incidents are not necessarily more serious on a per-incident basis than those at other companies — but there are a lot more of them.

**Conclusions:** Enterprises with more valuable information portfolios must spend more time and effort securing them. Higher-value portfolios lead to more incidents. Our data shows that enterprises are not spending enough effort protecting data from theft and abuse by outside parties. High-value firms suffer six times more data security incidents due to outside parties than low-value firms, and the number of outside parties they work with is 60% greater. This shows that the combination of more valuable information and more widespread collaboration leads directly to higher security exposure.

## CISOs Do Not Know How Effective Their Security Controls Are

Enterprises implement a range of security controls to protect their sensitive data. Some of these are process controls, such as access controls on file shares, data classification procedures, or data breach reporting. Others are technical controls for the endpoint, network, or data center. Endpoint controls include full-disk encryption, device wipe software for mobile devices, and DLP. Network controls include DLP software for the network and email encryption software. Data center controls include DLP software, access control remediation, database monitoring, database encryption, and security information management (SIM).

When asked to rate the effectiveness of their security controls, respondents rated nearly every one highly. Sixty percent or more rated every single technical control we asked about as "highly effective." A huge majority (95%) expressed high confidence that they know where their most sensitive information flows from and to.[9]

But enterprise confidence in the effectiveness of their controls is overstated. For example, both high-value and low-value firms rated their security programs equally effective — scoring 2.5 and 2.6, respectively, on a 3-point scale. But as we discussed in the previous section, the high-value firms had four times as many incidents as low-value firms. One of them must be wrong. We observed the same pattern when we compared the top and bottom quartiles for security spending and security incidents. In other words, no matter how we cut our data — by information asset value, spending, or number of incidents — the top and bottom quartiles all rated their program effectiveness between 2.5 and 2.6, even though the number and cost of incidents varied widely. We find this implausible.

**Conclusion:** Most enterprises do not actually know whether their data security programs work or not, other than by raw incident counting. Even then, an enterprise with a high number of incidents is still likely to imagine that its programs are "very effective." To understand more objectively how well their security programs perform, enterprises will need better ways of generating key performance indicators and metrics — and we (Forrester) will need to ask more pointed questions to better understand the incidents they missed.

## Conclusions And Recommendations

In analyzing the security practices of more than 300 North American, European, and Australian enterprises, Forrester Consulting confirmed several long-standing hypotheses about data security programs in large companies. We confirmed that, indeed, increased collaboration increases data security's importance, and that compliance pressures continue to be the motor that turns the IT security budget wheel. We also confirmed the conventional wisdom that, 75% of the time, data security incidents are attributed to insiders.

However, we also reached some surprising conclusions. Forrester concluded that not all enterprises are created equally. High-value firms manage information that is 20 times more valuable than low-value firms. And they are much more eager collaborators. As a result, the number and type of data security incidents experienced by high-value firms were four times higher, and the costs are nearly twice as high.

## KEY RECOMMENDATIONS

CISOs invest significant time and money protecting their sensitive information. But their priorities are not always the right ones. Security investments are too often aimed at preventing accidents, such as when employees accidentally lose laptops or inadvertently send emails containing customer information. Enterprises are sensitive to these concerns because compliance with regulations, customer pressures, criminals, and contractual mandates make toxic data spills expensive.

"Compliance" in all its forms has helped CISOs buy more gear. But it has distracted IT security from its traditional focus: keeping company secrets secure. Forrester recommends that enterprises examine their current data security strategies to ensure that they are balanced and appropriate for the portfolios they are protecting. In the next 60 days, you should:

- **Identify the most valuable information assets in your portfolio.** As we have demonstrated in this report, some information assets are more valuable than others. Ask your organization's asset owners to assign coarse-grained monetary values to their custodial data and secrets. Stack-rank the top five most valuable assets, and calculate the proportion that is "secrets" versus "custodial data." Use the broad ratios in Figure 4 as a guideline to determine whether your enterprise contains more — or less — secrets than other enterprises in your vertical.

- **Create a "risk register" of data security risks.** Divide the risks your firm faces into two categories: compliance risks and misuse of secrets. For compliance, review the history of "toxic data spills" involving mobile devices and media. For misuse of secrets, review cases of abuse by users with access to valuable information. Examine the types of information given to third parties, especially the extent to which they are stored on non-company-owned assets. Create a risk register documenting the specific threat scenarios: what data is at risk and from whom, and the likeliest threat vectors the threat agents might exploit.

- **Assess your program's balance between compliance and protecting secrets.** Your organization's senior management has a set of principles that shapes what the security program does and the impulses it responds to. Requests to "protect our patients' medical records" or "keep our company out of the papers" imply priorities for protecting custodial data. But "stop our designs from being stolen by our competitors" sends a different message. Understanding how your management's priorities map to the security team's control strategies is essential to understanding whether it is balanced.

These three actions will establish your security program's baseline. Based on the results, you should then:

- **Reprioritize enterprise security investments.** Programs whose control strategies are "overweighted" toward compliance and preventing employee accidents should consider data-centric technologies like enterprise rights management (ERM), fine-grained access controls, and DLP. To increase acceptance by the employees who must protect the information, use a simple data classification strategy with just three levels: public, internal use only, and need-to-know. For reducing theft of secrets by privileged insiders, build core competencies in network security monitoring (NSM) and SIM.

- **Increase vigilance of external and third-party business relationships.** Enterprises with significant exposure to third parties should take steps to monitor and restrict information flows. If possible, mandate the installation of technical controls on third-party devices that store significant quantities of secrets or custodial data. Consider data-sharing strategies that don't require third parties to store data on their devices, such as client virtualization.

- **Measure effectiveness of your data security program.** Security managers should rely on facts, rather than faith, for proof of effectiveness of their data security programs. Develop a process for tracking key performance indicators that measure the effectiveness of data protection efforts, such as frequency and cost of incidents. Wherever possible, benchmark against comparable firms using data from studies like this one or using public data sources like DataLossDB.

## Appendix A: Methodology

In this study, Forrester conducted an online survey of 305 organizations on three continents to evaluate data security drivers, practices, and costs. The survey base included 163 US-based companies, 102 in Europe, and 40 in Australia and New Zealand.

All companies we surveyed employed more than 5,000 people. Survey participants were decision-makers who had primary responsibility or authorization over IT security budgets. Questions provided to the participants asked basic demographic questions about their industry, number of employees, and IT and security budgets. Specific security question categories included:

- Business security drivers.
- Key perceived data security risks.
- Sensitive data types managed by the enterprises.
- Value of the top five most-important data types.
- In-use and planned data security controls.
- Data loss incidents, their sources, and their cost.

The survey totaled 30 high-level questions, many with multiple responses and multipart answers. In all, we obtained more than 2,000 data points per respondent.

The study began in November 2009 and was completed in December 2009.

Based on the results from the fielded survey, Forrester calculated the following key statistics for each company:

- Information value.
- Information value — toxic data.
- Information value — secrets.
- Number of outside parties.
- Number of security controls deployed.
- Mean effectiveness of security controls.
- Number of security incidents (past two years).
- Cost of security incidents.

We explain the calculation of each metric below.

## Information Value

We assigned an information value to the top five types of information the respondents considered “important” or “very important.” We gave respondents several value ranges to choose from. For each data type, if the respondent said it was worth less than $50,000, we assumed that data type had *no* value. If the respondent said it was worth more than $1 million, we capped the value at $1 million. Otherwise, we used the midpoint of the range. We then took the sum of these values to calculate the overall value of the firm’s information. Put more correctly, this value should be seen as a lower-bound estimate of the value of the firm’s five most-important data types. Because we only asked respondents to assign values to five data types, the maximum value of a firm’s information is $5 million. We realize that many enterprises value their information higher than this.

The 17 data types that respondents could choose from were: plans for new products and services; sales pipelines and forecasts; customer contact information; earnings and financial information; PII about customers; cardholder data related to compliance with PCI; medical records and PHI; financial models; source code; clinical trial information; bills of materials; product schematics and CAD drawings; pricing lists; competitive analyses; proprietary research; mergers and acquisitions data; and other (please specify).

## Information Value — Toxic Data

We calculated the value of information that is “toxic” by virtue of regulation or a compliance mandate like PCI. To do this, we summed the information values as described in the previous paragraph, but *only* for these data types: customer contact information; PII about customers; cardholder data related to compliance with PCI; medical records and PHI; and clinical trial information.

## Information Value — Secrets

We calculated the value of “secrets” (trade secrets, confidential and other kinds of nonregulated but otherwise valuable data) by subtracting the “toxic data” value from the firm’s overall information value.

## Number Of Outside Parties

We asked respondents to tell us how many third-party firms their enterprises do business with. We asked for specific numbers for each of these types of third party: supply chain raw materials or finished goods suppliers; contract manufacturers; outsourced customer contact center/call centers; healthcare insurance providers; payroll processors; outsourced or contracted IT support firms; outsourced application development firms, including offshore; CPAs; management consultants with privileged access to company financials; regulatory agencies; and contract professionals used for seasonal work. The *number of outside parties* metric is the sum of all of these responses.

## Number Of Security Controls Deployed

We asked respondents to tell us how many process-related and technology-based security controls they used to secure their information. For each of 21 specific controls, we asked to what degree they were deployed within the respondent’s environment, ranging from not deployed to full deployment.

We asked about five process controls: access controls; data security training; data incident/loss tracking; data breach reporting/response processes; and policies for classification and data protection.

We asked about six technical endpoint controls: device wipe/kill software for mobile devices; desktop/laptop port and device control software; file or folder encryption software; enterprise/information digital rights management; laptop or desktop full-disk encryption; and DLP software at the endpoint.

We asked about five technical network controls: DLP software for data in motion on the network; Web application firewall; email encryption software; email monitoring and filtering software; and encrypted file transfer software.

Lastly, we asked about five technical database and data center controls: database monitoring and protection tools; database encryption tools; DLP tools for discovering data at rest on servers/databases; security information and event management (SIEM) tools; and other.

The total *number of security controls deployed* is the count of the number of controls the respondent indicated they were "piloting" or have "fully deployed."

## Mean Effectiveness Of Security Controls

For each security control that the respondent indicated was "fully rolled out," we asked the respondent to grade its effectiveness on a 3-point scale, where 0 meant "shelfware," 1 meant "not at all effective," 2 meant "somewhat effective," and 3 meant "very effective." We then averaged the effectiveness score for all of the technologies to calculate a mean score for the enterprise.

## Number Of Security Incidents (Past Two Years)

We asked respondents to tell us the number of incidents they had experienced over the past two years for each of 14 specific kinds of incidents. One group of incidents was the type that an insider (employee) might commit; the other was for outsiders. Respondents could also indicate they experienced no incidents.

The "employee" incidents were nine different types: IT operations lost an unencrypted backup tape or drive; employee lost a laptop; employee lost a smartphone; IT administrator abused privileges and stole data; customer service representative inappropriately accessed customer records; employee accidentally emailed or posted sensitive information; rogue employee used his or her privileges to access sensitive company documents; rogue employee stole sensitive company documents; and terminated employee stole information because they had not been adequately deprovisioned.

The "outsider" incidents were five different types: outside business partner lost a laptop; outside business partner lost sensitive information via other means; outside attacker compromised a server and stole data; supply chain or business partner abused their privileges and obtained data they should not have had access to; and other.

The *number of security incidents metric* was the sum of the number of incidents for each type of incident. We further calculated metrics for the number of incidents *by employees* and the number of incidents *by outsiders*.

### Cost Of Security Incidents

For each type of incident that the respondents indicated they had non-zero numbers of incidents for, we asked what the hard-dollar costs (excluding labor) were for all incidents of that type. For each type of incident, we gave the user several cost ranges to choose from, ranging from "minimal cost" (less than $1,000) to "large incident" (more than $1 million). If the respondent said the hard-dollar cost was less than $1,000, we assumed that the cost was zero. If the respondent said it cost more than $1 million, we capped the cost at $1 million. Otherwise, we used the midpoint of the range. To calculate the total *cost of security incidents* metric for a firm, we summed the costs for all incidents. We further calculated metrics for the average incident cost for each type of incident across all firms.

## Appendix B: Supplemental Material

### Related Forrester Research

"Data Security Predictions For 2010" by Andrew Jaquith, December 2, 2009

"Selecting Data Protection Technologies" by Andrew Jaquith, October 28, 2009

"Inquiry Spotlight: Data Leak Prevention, Q1 2009" by Natalie Lambert and Andrew Jaquith, February 10, 2009

## Appendix C: Endnotes

[1] Source: David Drummond, "A new approach to China," *The Official Google Blog*, January 12, 2010 (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html). For Forrester's take, see *The Forrester Blog For Security & Risk Professionals*. Source: Andrew Jaquith, "The Attack on Google: What It Means," *The Forrester Blog For Security & Risk Professionals*, January 15, 2010 (http://blogs.forrester.com/srm/2010/01/the-aurora-attack-on-google-what-it-means.html).

[2] For more about the major search engine company incident, see Forrester's blog post. Source: Andrew Jaquith, "Plain speaking about industrial spying," *The Forrester Blog For Security & Risk Professionals*, January 25, 2010 (http://blogs.forrester.com/srm/2010/01/plain-speaking-about-industrial-spies-not-apt.html).

[3] Eighty-nine percent of respondents agreed (40%) or strongly agreed (49%) with this statement: "Compliance with incident disclosure laws, Payment Card Industry Data Security Standard (PCI-DSS), and data privacy regulations is the primary driver of our data security." Source: "The Value Of Corporate Secrets," a commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009. Base: 305 senior-level IT security decision-makers. Question Q1: "Please indicate how strongly you agree or disagree with the following statements about your company's use of communications technologies and their associated data security risks."

[4] Forrester asked respondents to indicate the degree to which "the following regulations and compliance-related issues have driven your data security programs: a) statutes and regulations such as CA SB 1386, MA-201, Sarbanes-Oxley, ARRA, and the EU Privacy Directive; b) contractual standards like the Payment Card Industry Data Security Standard (PCI-DSS); c) ITAR/Export Control; and d) internal corporate IT security policy." Source: "The Value Of Corporate Secrets," a commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009. Base: 305 senior-level IT security decision-makers.

[5] Ninety percent of respondents agreed (46%) or strongly agreed (44%) with this statement: "Collaboration tools that cross company boundaries are essential to run our business." Source: "The Value Of Corporate Secrets" a commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009. Base: 305 senior-level IT security decision-makers. Question Q9: "Please indicate how strongly you agree or disagree with the following statements about your company's use of communications technologies and their associated data security risks."

[6] Forrester asked each respondent to indicate how many third-party firms their enterprise does business with. We asked for specific numbers for each of 11 specific third-party categories. See Appendix A (Number of outside parties).

[7] As described in Appendix A, an enterprise's information portfolio value is calculated by summing the value assigned to each of the top five most-valuable information assets. Our survey conservatively capped the value of any type of information at $1 million.

[8] See Appendix A for a description of "security controls" and how we measured deployment.

[9] Ninety-six percent of respondents agreed (32%) or strongly agreed (64%) with this statement: "Data security is the most important security priority for our company." Ninety-five percent agreed (44%) or strongly agreed (51%) with the statement, "We know where our most sensitive data flows to and from." Source: "The Value Of Corporate Secrets," a commissioned study conducted by Forrester Consulting on behalf of RSA and Microsoft, November 2009. Base: 305 senior-level IT security decision-makers. Question Q9: "Please indicate how strongly you agree or disagree with the following statements about your company's use of communications technologies and their associated data security risks."