Powerful Insights
Proven Delivery.®

The Current State of IT Security and Privacy Policies and Practices

Assessing Strengths and Areas for Improvement in Classifying, Managing, Securing and Retaining Data

In the fourth quarter of 2011 and first quarter of 2012, Protiviti conducted a survey on IT security and privacy standards, policies and practices. Respondents, who included chief information officers, chief information security officers, IT vice presidents and directors, and numerous other IT management-level professionals, answered a series of questions related to how their organizations are classifying and managing the data they accumulate on a daily basis, and specifically how they are handling the security of "sensitive" data that is critical not only to ensure customer and/or client privacy, but also to comply with federal and state privacy laws and regulations.

The findings revealed that companies are doing many things well, but there is significant room for improvement and cost savings. Of particular note:

- **Data classification** – Organizations can benefit greatly, in terms of operational efficiency as well as cost savings, from improving the differentiation between "sensitive" data and other information.
- **Security policies** – Companies have an opportunity to reduce their legal/regulatory and reputation risks significantly by implementing appropriate data security policies and practices.

Following is a summary of the results along with additional commentary from Protiviti.

Organizations need to do a better job of understanding and classifying their "sensitive" data and information.

With regard to understanding the company's data and information, one of the most notable findings from the survey is that, according to the respondents, management in 23 percent of organizations has limited or no understanding of the difference between sensitive information and other data.

Also of note, while 69 percent of companies have a clear data classification *policy* in place to categorize the organization's data and information (sensitive, confidential, public, etc.), just 50 percent have a *scheme* in place to perform the categorization. And within more than one in four

protiviti®
Risk & Business Consulting.
Internal Audit.

companies, there is substantial room for improvement in how management communicates these differences so that each type of data is handled appropriately.

When asked to select the statement that best describes the organization's data retention and storage process, just 29 percent of respondents reported that their organizations have a detailed classification system to define data with varying retention policies and destruction dates depending on that classification. Nearly 30 percent either retain all data and records for a certain period of time with a defined destruction date, or do so with no defined destruction date.

How would you rate your management's understanding of what comprises its "sensitive" data and information?	
Excellent understanding	26%
Good understanding	50%
Limited understanding	22%
Little or no understanding	1%
Don't know	1%

From the following, please select the statement that best describes your organization's data retention and storage process:	
We have a detailed classification system to define data, with varying retention policies and destruction dates depending on the classification.	29%
We have a basic classification system to define data, with a few specific retention policies and destruction dates depending on the classification.	34%
We retain all data and records for a certain period of time, with a defined destruction date.	22%
We retain all data and records with no defined destruction date.	7%
Our organization does not have a formal data retention and destruction policy.	3%
Don't know	5%

Commentary

Companies in virtually every industry have invested large sums of money in an effort to get to know their customers and their customer's activities in order to personalize service to them. To accomplish this, they must collect as much information as possible about a customer. These organizations are now capturing a wealth of data on a daily basis – at least some of which is considered personally identifiable information. Thus they must understand how to classify, manage and secure that data, not only for the sake of their customers and clients, but also to be in compliance with myriad privacy laws and regulations. Of note, 46 of the 50 states in the United States have data privacy laws. While each may have its own unique aspects and requirements, one of the consistent provisions that can be found in all of them is that any person

or organization holding private data and information is accountable if that information is breached (more specifically, the person or organization is accountable to that state's citizens).

The fact that management in close to one out of every four organizations has limited, little or no understanding of what comprises sensitive data and information should be considered troubling, especially given the potential ramifications related to regulatory compliance and reputation damage. In fact, just 26 percent of respondents said management in their organization has an excellent understanding of these areas, a figure that should be far higher.

With regard to data storage and retention, there is evidence in the results that companies are defaulting to keeping the data and information too long – i.e., there is no clear data retention and destruction policy in place, suggesting they "keep everything forever." Virtually every organization should have a detailed classification system in place to define its data, with varying retention policies and destruction dates depending on classification. Not having such a system creates unnecessary risks with regard to security and regulatory compliance, and also results in higher-than-necessary data retention and data management costs for information that an organization has no business need to keep.

It also is clear that management is not doing nearly enough to communicate to the organization and its employees how to differentiate between sensitive and other data, and how to treat each of these. The survey results related to data classification policies and schemes (see pages 1-2) underscore this. Most companies appear to have a policy in place to classify data, but are not doing enough to establish clear processes to do so, provide training, or communicate these policies and processes on a regular basis.

It is critical for organizations to establish policies on the retention, destruction, encryption and acceptable use of sensitive data.

As detailed in the following tables, there are varying degrees of effectiveness and knowledge when it comes to how organizations are managing and protecting the data they collect.

Which of the following policies does your organization have in place?	
Acceptable use policy	86%
Record retention/destruction policy	81%
Written information security policy (WISP)	75%
Data encryption policy	65%
None of these	3%

Commentary

The good news is that, with regard to managing data leakage, a strong majority of companies appear to be employing many effective and proven policies, such as those for passwords, information security, and data protection and privacy. While there is room for improvement in these and several other policies, many organizations clearly recognize the importance of having these foundational directives in place.

That said, the relatively low percentage of organizations that have policies for such things as workstation and laptop security, data classification, and information exchange represents significant gaps and areas for improvement.

What types of policies does your organization have in place to prevent data leakage?	
Password policy (or standard)	89%
Information security policy	82%
Data protection and privacy policy	74%
Incident response policy	72%
User (privileged) access policy	72%
Encryption policy (or standard)	70%
Network and network devices security policy	66%
Workstation/laptop security policy	65%
Third-party access control policy	60%
Data classification policy	57%
Removable media policy	51%
Information exchange policy	33%

What is perhaps most critical to understand is that organizations with these policies in place significantly reduce the risk of substantial legal fines and reputation damage. Consider again that 46 out of 50 U.S. states have data privacy laws. However, most of these laws allow for leniency if the entity has two things in place operationally: data encryption and a written information security policy (WISP). This means that, based on the survey findings, not only is there much room for improvement for organizations to do something that they should be doing to secure their data, but in doing so they also can significantly reduce their liability relative to state laws and regulations.

The other notable finding pertains to records retention and destruction policies. While 81 percent of organizations have such policies, which is a positive result, there is still room for improvement considering that one in five organizations apparently have no such policy. As previously stated, managing and protecting sensitive data is critically important, yet it also is vital to avoid a “default” policy of saving everything forever. Such an approach drives huge costs, including but not limited to the costs of acquiring and maintaining otherwise unnecessary storage capacity.

By classifying their data appropriately, companies gain significant advantage in terms of cost savings, operational efficiencies, and legal and regulatory compliance.

Data governance should not be relegated to IT.

Interestingly, with regard to creating and overseeing data governance in the organization, there is a substantial disparity in the results. In nearly one in three organizations (31 percent), the CIO is responsible, while within one in five organizations (21 percent) the chief security officer is responsible. In 18 percent of companies, individual department leaders have this responsibility.

There is a similar disparity in looking at who is responsible for executing the data governance strategy/policy in organizations. The CIO has this responsibility in 28 percent of organizations, but in one in three companies (34 percent) that responsibility falls to individual department leaders.

Who is responsible for *creating and overseeing* data governance in your organization?	
Chief Information Officer	31%
Chief Security Officer	21%
Individual department leaders (HR, Legal, Marketing, etc.)	18%
Chief Privacy Officer	7%
Chief Financial Officer	5%
Other	12%
Don't know	6%

Who is responsible for *executing* the data governance strategy/policy in your organization?	
Individual department leaders (HR, Legal, Marketing, etc.)	34%
Chief Information Officer	28%
Chief Security Officer	13%
Chief Privacy Officer	5%
Chief Financial Officer	3%
Other	10%
Don't know	7%

Commentary

Many companies that have been focused intensely on data management are concluding that 1) there are differences in data that an organization collects; 2) there needs to be stewardship of this data; and 3) responsibility for stewardship should rest not necessarily with IT, but with the individual/department most knowledgeable about the data being collected. For example, the steward of employee data should be the head of HR, while the steward for financial data and metrics should be the CFO.

These survey results are encouraging in that they indicate movement away from a clerical, technology-oriented mindset for responsibility of this data to an approach in which data

governance decisions are made by the appropriate department or business unit. Data governance is not just a technology issue, and it is good to see more organizations are not treating it as such. The next step – and one that some organizations already are taking – is to establish information governance councils or steering committees to create, oversee and execute data governance, and ensure that this process is linked to the legal department and the board of directors.

With regard to executing the data governance strategy/policy, the survey findings should be considered positive and encouraging, provided that there is a bridge or link to a data governance strategy and that this has been communicated to the organization. Otherwise, execution is taking place in a virtual vacuum, which can lead to critical mistakes.

Moving to the cloud? Not so fast, at least in terms of sensitive data.

Respondents were asked about the location of their organization's sensitive data. In most companies (85 percent), sensitive data is stored in on-site or off-site servers. Relatively few reported using a cloud-based vendor for this purpose, while 8 percent said this data is not stored in any centralized location.

Where is your company's sensitive data stored?	
On-site servers	71%
Off-site servers	14%
Cloud-based vendor	2%
Not stored in any centralized location	8%
Don't know	5%

Commentary

The results suggest that the movement to the cloud, at least in terms of storing sensitive data, is slower than market watchers are suggesting. But there is movement. The question is whether organizations know and understand the data they are storing off-site or in the cloud, or even if they are classifying what they are storing and where they are storing it. In most cases, a centralized environment – whether that is on-site or off-site – offers better control. Breaking this down further, there generally is less control over off-site servers and vendors than for on-site servers. Thus organizations need to be very careful when it comes to storing their sensitive data anywhere beyond an on-site server. Storage on a server that is physically located on company property must take place with the proper security standards and protocols, but these are easier to manage, monitor and control than at any off-site entity, whether that is in the cloud, at another location or multiple locations. This is not to say that organizations should not do this – rather, the key point is that it must be done carefully and with the proper security standards in place.

When organizations are storing data off-site with another vendor, whether through the cloud or traditional outsourcing, they should ensure that the contracts appropriately deal with how data is stored and where it is stored to avoid any privacy or regulatory issues.

Too many are not ready for a crisis.

Survey participants were asked if their organization has a crisis response plan that would be activated and executed in the event of a data breach or hacking incident. Three out of four companies (73 percent) have such a plan in place.

If your organization experienced a data breach or hacking incident, does it have a formal and documented crisis response plan that would be activated and executed?	
Yes	73%
No	12%
Don't know	15%

As defined in your organization's documented crisis response plan, who needs to be involved in addressing a data breach or hacking incident?	
Chief Information Officer/Chief Security Officer	58%
General Counsel/Chief Legal Officer	50%
Corporate Communications	40%
Chief Privacy Officer	30%
Chief Executive Officer	18%
Other	14%
Don't know	3%

Commentary

It is encouraging to find that many companies have crisis response plans in place. Still, to see that 12 percent do not and 15 percent of respondents apparently don't know is problematic. As can be seen almost every day in the media, a high percentage of companies have experienced some type of data breach. The odds are that if an organization has not had such a breach, it will at some point. The questions then become: Are you ready for it? Do you have a detailed and tested crisis response plan in place? Is this reviewed and updated on a regular basis? Has it been vetted by an independent group or third party to ensure it is complete? Are the executives and professionals who are part of this plan trained on a regular basis? Does the plan address vendor relationships? An effective crisis response plan depends on positive responses to these questions.

The findings with regard to who needs to be involved in addressing a data breach or hacking incident also are interesting. It is good to see relatively high percentages for an array of IT executives and functions in the organization. Still, there is significant room for improvement and, in some cases, remediation. For example, given the statistics cited earlier noting that 46 U.S. states have specific laws with regard to data security and privacy, how can the general counsel or chief legal officer not be engaged in every data breach or hacking incident? There almost assuredly will be legal issues in every case. There also will be issues related to reputation risk and a need for careful and planned message control, particularly considering how social media

can cause news of a data breach or hacking incident to erupt in a matter of minutes or hours. Given this, it is conceivable that corporate communications and/or public relations should be engaged in any crisis response plan related to such an incident.

Closing Comments

Organizations have made significant strides over the past few years in understanding how to manage the data they are collecting on a daily basis, classifying that data according to what is sensitive, confidential, nonconfidential, etc., and setting agreed-upon policies for retaining and destroying data at the appropriate times. However, there remains significant room for improvement, particularly in building knowledge of the differences between legally confidential data and other data.

It is likely that many organizations have an opportunity to streamline their processes and reduce costs by moving away from "over-retention" of data that is stored without a defined destruction date. Further, by ensuring certain best practices and policies are in place – including WISPs and data encryption policies – companies not only can make considerable improvements in how they are classifying and managing their data, but they also will reduce their legal and regulatory risks substantially. Those looking for further motivation to make this a higher priority would do well to remember a familiar saying today: "There are only two types of companies – those that know they've been hacked, and those that don't know they've been hacked."[1]

[1] This quote, or variations thereof, can be attributed to several individuals, including U.S. Representative Mike Rogers, chairman of the U.S. House of Representatives Permanent Select Committee on Intelligence, in the 11/20/2011 press release, "Rogers & Ruppersberger Introduce Cybersecurity Bill to Protect American Businesses from 'Economic Predators'," http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/113011CyberSecurityLegislation.pdf.

Methodology and Demographics

Protiviti conducted its IT Security and Privacy study in the fourth quarter of 2011 and the first quarter of 2012. IT executives and management-level professionals were invited to complete an online questionnaire designed to assess security and privacy policies, data governance, data retention and storage, and data destruction policies.

Since completion of the survey was voluntary, there is some potential for bias if those choosing to respond have significantly different views on matters covered by the survey from those who did not respond. Therefore, our study's results may be limited to the extent that such a possibility exists. In addition, some respondents answered certain questions while not answering others. Despite these limitations, we believe the results herein provide valuable insights regarding IT security and privacy standards in place in organizations today.

More than 100 individuals participated in the study. Following are details regarding the respondents and the size of companies represented in the study.[2]

Respondents (title/role)

IT Audit Manager	15%
IT Manager	13%
IT VP/Director	11%
Chief Information Security Officer	10%
IT Audit VP/Director	6%
Chief Information Officer	2%
Chief Security Officer	1%
Other	42%

[2] All demographic information was provided voluntarily by respondents. Percentages in the tables correspond to those providing this information rather than the total sample of respondents.

Industry

Financial Services	16%
Healthcare Provider	15%
Government/Education/Not-for-profit	10%
Manufacturing	9%
Insurance	6%
Retail	6%
Utilities	6%
Consumer Products	4%
Energy	4%
Technology	4%
Communications	2%
Hospitality	2%
Real Estate	2%
Other	14%

Size of Organization (by gross annual revenue)

$20 billion+	17%
$10 billion - $19.99 billion	11%
$5 billion - $9.99 billion	12%
$1 billion - $4.99 billion	29%
$500 million - $999.99 million	17%
$100 million - $499.99 million	9%
Less than $100 million	5%

Type of Organization

Public	55%
Private	25%
Not-for-profit	15%
Government	5%

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Our IT Security and Privacy Solutions

As the business world becomes more and more connected, it is critical to view information security and privacy as a business issue, not just an IT issue. Security threats, vulnerabilities and privacy exposures challenge every organization today, creating risks that must be understood and managed. Often organizations do not know what risks they face or how they will manage these risks. Equally important, good security and privacy practices can provide revenue growth opportunities through personalized support to clients.

Protiviti provides a wide variety of security and privacy assessment, architecture, transformation and management services to help organizations identify and address security and privacy exposures (e.g., loss of customer data, loss of revenue, or reputation impairment to a customer) before they become problems.

We have a demonstrated track record of helping companies react to security incidents, establish security programs, deal with identity and access management, and handle industry-specific data security and privacy issues, including PCI and HITRUST. We invite you to explore the various IT security and privacy services we offer.

- Security Strategy & Program Management Services
- Identity & Access Management Services
- Data Security & Privacy Management Services
- Vulnerability Assessment

For additional information, please contact:

Kurt Underwood
Managing Director, Global IT Consulting Solutions Leader
+1.503.227.1131
kurt.underwood@protiviti.com

Cal Slemp
Managing Director, Security and Privacy Solutions
+1.203.905.2926
cal.slemp@protiviti.com

protiviti®
Risk & Business Consulting.
Internal Audit.