Bridging the Data Security Chasm

Assessing the Results of Protiviti's 2014 IT Security and Privacy Survey

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

EXECUTIVE SUMMARY

If data isn't the lifeblood of an organization, it without question is a critical component in its success. Analogous to the role of water in a hydroelectric plant, data powers an organization, pumping "fuel" – through information, knowledge and insights – to virtually every company function. It therefore must be managed – and managed well.

With the plethora of cyberattacks and data breaches – both publicized and otherwise – that have occurred over the past year, prevailing wisdom suggests companies are working diligently to "get their houses in order" with regard to IT and data security and privacy. However, the results of our latest IT Security and Privacy Survey suggest there is still plenty of work to do.

Remarkably, despite some positive developments and growth, there remain significant chasms between where organizations stand and where they need to be. Just as interesting, there are organizations that have bridged these chasms quite successfully. How have they accomplished this?

It starts at the top, with high engagement by the board of directors in the organization's information security risks, which requires establishing a risk appetite and implementing a security framework. It continues with having in place fundamental information management, security and retention/destruction policies.

Our five key findings

1. **Board engagement is a key differentiator in the strength of IT security profiles –** Nearly three out of four boards are viewed to have a good level of understanding about the organization's information security risks. Even more important, as is evident throughout our results, organizations with a high level of board engagement in these risks have significantly stronger IT security profiles.
2. **There remains a surprising lack of key "core" information security policies –** One in three companies do not have a written information security policy (WISP). More than 40 percent lack a data encryption policy. One in four do not have acceptable use or record retention/destruction policies. These are critical gaps in data governance and management, and ones that carry considerable legal implications. On the other hand, organizations with all of these key data policies in place have far more robust IT security environments and capabilities.
3. **Organizations lack high confidence in their ability to prevent a cyberattack or data breach –** While executive management has a higher level of awareness when it comes to the organization's information security exposures, lower confidence levels among IT executives and professionals in preventing an attack or breach likely speak to the creativity of cyberattackers and, in many respects, the inevitability of a breach – and the need for strong incident response planning and execution.
4. **Not all data is equal –** The percentage of organizations that retain all data and records without a defined destruction date has more than doubled – not necessarily a positive development. Companies can't protect everything – designating a subset of their data deemed most critical will help with their data security measures.
5. **Many are still unprepared for a crisis –** There is a significant year-over-year jump in the number of organizations without a formal and documented crisis response plan to execute in the event of a data breach or cyberattack. And less than half perform periodic fire drills to test their plans.

SURVEY METHODOLOGY

Protiviti conducted its IT Security and Privacy study in the second quarter of 2014. More than 340 Chief Information Officers, Chief Information Security Officers, Chief Technology Officers, IT Vice Presidents and Directors, and other IT management-level professionals completed an online questionnaire designed to assess security and privacy policies, data governance, data retention and storage, data destruction policies, and third-party vendors and access, among other topics.

Respondent demographics can be found on pages 30-31. In our discussion of the results and our commentary, we make observations that may apply in different ways depending on an organization's specific profile – size, type (public, private, nonprofit), industry, etc. While in this year's study we have a larger percentage of respondents from "small" organizations ($100 million or less in annual revenue), the guidance and best practices discussed herein still apply, in our view, given that every organization, regardless of size or industry, has IT security and data-related risks that they must manage.

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.

RESULTS AND ANALYSIS

The Top Performers – It Starts With High Board Engagement and Core Information Security Policies

In our analysis of the results, we have identified two critical success factors in establishing and maintaining a robust IT security and privacy profile:

1. High level of engagement by the board of directors in information security risks
2. Having all "core" information security policies in place

These results are detailed below and serve as key reference points in the discussion and analysis of our survey results in the following pages.

How engaged is your board of directors with information security risks relating to your business?

	All respondents	Large companies (≥ $1B)	Small companies (‹ $1B)
High engagement and level of understanding by the board	30%	34%	26%
Medium engagement and level of understanding by the board	41%	45%	36%
Low engagement and level of understanding by the board	20%	12%	30%
Don't know	9%	9%	8%

Commentary

- It is positive to see in the overall response that 71 percent of boards have a high or medium level of understanding with regard to information security risks.
- Still, one in five boards appear to have a low level of understanding, suggesting their organizations are not doing enough to manage these critical risks or engage the board of directors in a regular and meaningful way.
- As expected, there is stronger board-level engagement in large companies, but not dramatically so.
- It is important to note that the board generally is not aware of every detail and security practice in place within organizations (nor should it be expected to have this level of awareness). Still, having the board of directors set a strong "tone at the top" will drive the organization to plan and implement more robust IT security and privacy practices, particularly if the board understands the organization's current ability, or lack thereof, to deal with cyberattacks effectively. It is incumbent upon the CIO, IT organization and management to provide meaningful metrics and reporting to the board on a regular basis, which will drive awareness, support and action.

- The Institute of Internal Auditors Research Foundation™ (IIARF™) and ISACA® recently released a report in which they advocate that boards of directors should actively participate in measuring and monitoring an organization's strategy on cybersecurity. The guidance builds on five principles cited in a report by the National Association of Corporate Directors (NACD) in conjunction with the American International Group (AIG) and the Internet Security Alliance (ISA).[1]

Which of the following policies does your organization have in place? *(Multiple responses permitted)*

	2014	2013	2012	Large companies (≥ $1B)	Small companies (< $1B)
Acceptable use policy	76%	87%	86%	84%	69%
Record retention/ destruction policy	76%	86%	81%	84%	71%
Written information security policy (WISP)	66%	78%	75%	79%	52%
Data encryption policy	59%	68%	66%	67%	52%
Social media policy*	59%	NA	NA	67%	51%

** New category*

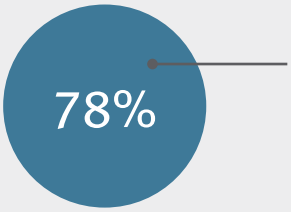
Commentary

- In the overall response, there is a surprising drop in the number of organizations that have different core data policies in place.[2]
- Again, large companies appear to perform better with regard to having these policies in place, but the differences are not dramatic.
- Organizations with high board engagement in information security are significantly more likely to have these policies in place compared to organizations with other levels of board engagement. The gap is especially wide with data encryption and social media policies.
- Of particular note, the percentages with regard to WISPs and data encryption policies are remarkable. These two policies are specifically identified in all state breach laws and serve as indicators of attention to this issue by an organization that has experienced a data breach. They also serve as determinants as to the level of negligence by an organization that has experienced a data breach.

[1] *Cybersecurity: What the Board of Directors Needs to Ask*, IIARF and ISACA, August 2014, www.theiia.org/bookstore/downloads/freetoall/5036.dl_GRC%20Cyber%20Security%20Research%20Report_V9.pdf.

[2] As noted in our Survey Methodology section, the year-over-year drop could be explained, in part, by a larger percentage of respondents from smaller organizations, which differ in their risk tolerance levels, budgets and priority placed on IT security. Still, we do not believe this serves as the sole explanation for the year-over-year variance. Among other reasons, smaller organizations still face significant IT security risks relative to their size and revenue level.

KEY FACT



Percentage of organizations with all core information security policies in which the board of directors has a high or medium level of engagement and understanding of the organization's information security risks

- In the United States, 46 out of 50 states have data privacy laws that impose significant penalties on organizations that expose confidential data. A consistent provision in every privacy-related law 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). Nearly all of these laws allow for leniency if the organization that experienced a data breach has a WISP and data encryption policy. Given this, there is little reason for an organization not to have such policies in place. This will better secure their data and reduce their legal liability substantially.
- Clearly, organizations lacking these policies need to address these gaps as soon as possible. Understandably, there are barriers, among them:
  - These are evolving areas – while policies are critical, they take time to craft, socialize and institute.
  - IT organizations are too busy dealing with other critical priorities.
  - There is a lack of knowledge and understanding about where to begin.

Cyberwarfare Press Coverage = Greater Focus on Information Security

Our results show that, with the rising tide of media coverage on cyberattacks, cyberwarfare and cybersecurity efforts, there are growing levels of interest in these issues among companies.

How has recent press coverage on "cyberwarfare" and/or "cybersecurity" affected your interest in, and focus on, the subject of information security?

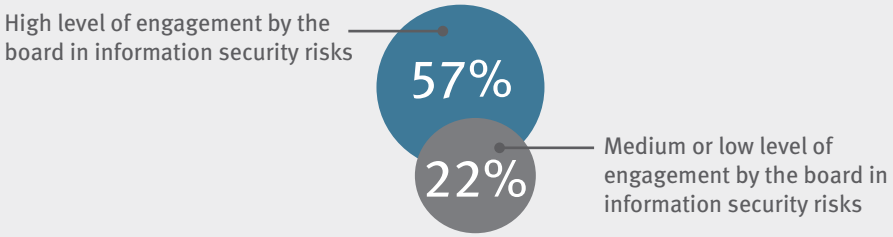
			Top-Performing Organizations			
	2014	2013	Companies with high board engagement in information security	Companies without high board engagement in information security	Companies with all core information security policies	Companies without all core information security policies
Significantly more interest and focus	32%	21%	57%	22%	39%	29%
Somewhat more interest and focus	37%	46%	24%	42%	34%	38%
No change in interest and focus	30%	31%	18%	36%	27%	32%
Somewhat less interest and focus	1%	1%	1%	0%	0%	1%
Significantly less interest and focus	0%	1%	0%	0%	0%	0%

Commentary

- While overall the year-over-year results among all respondents are similar, we see a rise in the "significant" level. This suggests that while overall interest levels remain similar to last year, the focus has become even sharper for organizations.
- There is a strong difference in interest and focus among organizations that have a high level of board engagement in information security compared to those with other levels of board engagement. There also is a notable difference between organizations with all core data policies in place and those without all of these policies.

KEY FACT

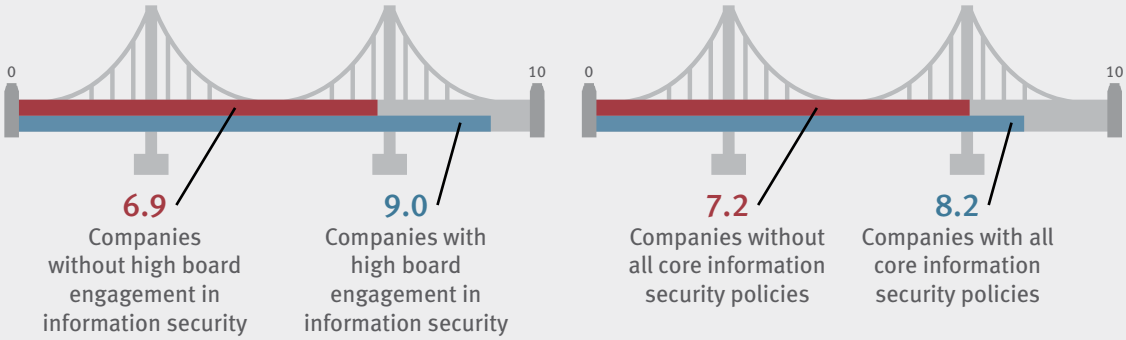
Percentage of organizations, by level of board engagement, that have significantly more interest and focus as a result of cyberwarfare press coverage



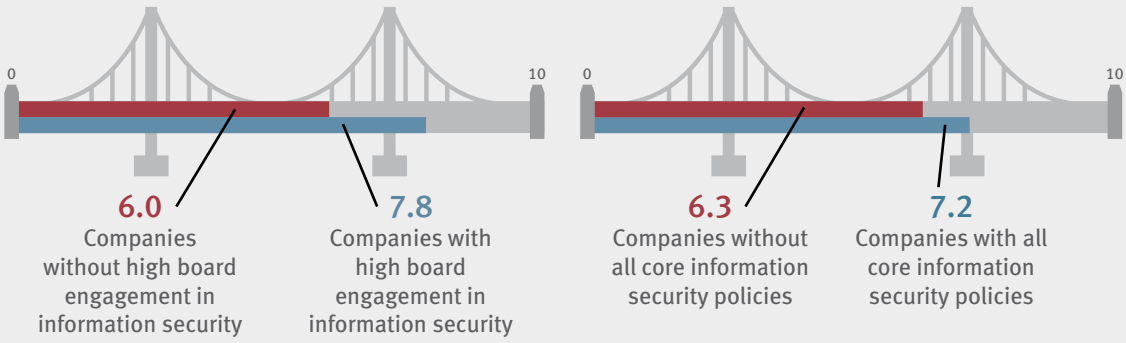
Organizations Lack High Confidence in Their Ability to Prevent a Cyberattack or Data Breach

There is a relatively high level of awareness at the senior management level with regard to the organization's information security exposures, but less confidence when it comes to preventing a breach.

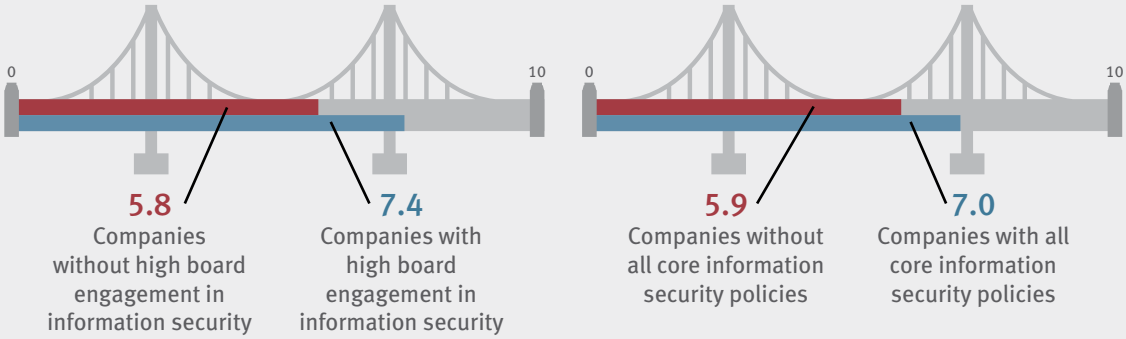
On a scale of 1 to 10, where 10 is a high level of awareness and 1 is little or no awareness, please rate senior management's level of awareness with regard to your organization's information security exposures.



On a scale of 1 to 10, where 10 is a high level of confidence and 1 is little or no confidence, rate your level of confidence that your organization is able to prevent a targeted external attack by a well-funded attacker.



On a scale of 1 to 10, where 10 is a high level of confidence and 1 is little or no confidence, rate your level of confidence that your organization is able to prevent an opportunistic breach as a result of actions by a company insider (employees or business partner).



Commentary

- As noted, there is a higher level of awareness at the senior management level with regard to the organization's information security exposures compared to the level of senior management's confidence in actually preventing a breach. This speaks to the creativity of cyberattackers and possible inevitability of experiencing a breach.
- Companies with a high level of board engagement in information security risks have substantially higher levels of awareness and confidence in these areas compared to other organizations. Based on our experience, there likely are two reasons behind this. First, operational teams in these organizations are compelled to become more aware of these issues as a direct result of oversight and questions from the board. In addition, they likely are generating meaningful metrics so that they can communicate with the board effectively and to the satisfaction of the directors. In turn, this has led to a better understanding of their organization's security status and where holes need to be fixed. Second, the board – knowing more about information security issues and risks – may be authorizing management to make larger investments in budget and resources to address them.

Are the Right Policies in Place to Prevent Data Leakage?

Along with the core information security policies we detailed earlier, there are numerous other data management and security policies organizations should have in place to help prevent data loss – information security, passwords, user access, incident response, etc. Remarkably, this year's results show across-the-board decreases in the numbers of organizations that have these policies in place.

What types of policies does your organization have in place to prevent data leakage? *(Multiple responses permitted)*

	2014	2013	2012
Password policy (or standard)	77%	87%	92%
Data protection and privacy policy	67%	74%	76%
Information security policy	67%	77%	84%
Network and network devices security policy	59%	70%	68%
Users (privileged) access policy	59%	72%	74%
Workstation/laptop security policy	59%	73%	67%
Data classification policy	53%	63%	59%
Third-party access control policy	49%	64%	62%
Incident response policy	46%	64%	74%
Removable media policy	44%	49%	53%
Information exchange policy	30%	35%	34%
Cloud acceptable usage*	24%	NA	NA

** New category*

Commentary

- Most of these policies are required in some form in order to comply with various government and industry regulations, thus organizations potentially face significant liability, along with security risks, by not having these policies in place.
- The year-over-year drops in many of these percentages are surprising and are not explained entirely through different views of the data, such as large versus small company. For example, a majority of the responses from participants with companies under $1 billion in annual revenue are comparable to those with revenue greater than $1 billion. Exceptions include data classification policy (71 percent for large companies versus 39 percent for small companies), incident response policy (61 percent versus 34 percent), and removable media policy (54 percent versus 33 percent).
- It is possible that many organizations currently are working to modify and strengthen their various data security policies, but have yet to complete this process or are not yet satisfied with them. In our experience, companies are more aware than ever of the importance of having these policies in place and are focused on making all of their policies both clear and effective in helping the organization secure and manage its data.
- As we continue to see in our results, there are notable differences when looking at organizations that have a high level of board engagement in information security risks, and as expected, those that have all core data policies in place (see accompanying table).

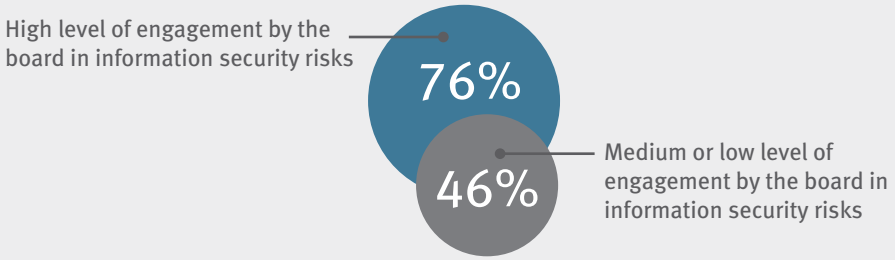
What types of policies does your organization have in place to prevent data leakage? *(Multiple responses permitted)*

	Top-Performing Organizations			
	Companies with high board engagement in information security	Companies without high board engagement in information security	Companies with all core information security policies	Companies without all core information security policies
Password policy (or standard)	76%	46%	92%	70%
Data protection and privacy policy	75%	63%	91%	55%
Information security policy	75%	64%	93%	55%
Network and network devices security policy	66%	56%	84%	47%
Users (privileged) access policy	60%	59%	82%	48%
Workstation/laptop security policy	65%	57%	85%	47%
Data classification policy	70%	46%	83%	38%
Third-party access control policy	52%	47%	76%	35%
Incident response policy	58%	41%	73%	33%
Removable media policy	53%	40%	77%	28%
Information exchange policy	37%	27%	51%	20%
Cloud acceptable usage*	34%	21%	46%	14%

** New category*

KEY FACT

Percentage of organizations, by level of board engagement, that have a password policy



How does your organization communicate the expectations of its security policies and procedures to employees?

(Multiple responses permitted)

		Top-Performing Organizations			
	All respondents	Companies with high board engagement in information security	Companies without high board engagement in information security	Companies with all core information security policies	Companies without all core information security policies
We include security policies and procedures in our annual training, which is mandatory for all employees	53%	66%	49%	75%	43%
We have internally developed, security-specific training modules that we require all employees to take in addition to our standard annual training	35%	48%	30%	49%	29%
We support participation by our employees in outside education on security policies and procedures	20%	30%	16%	19%	20%
We do not have any formal employee communications or training related to security policies and procedures	22%	8%	28%	7%	30%

Commentary

- The relatively low numbers with regard to training indicate an area for improvement. Successful awareness campaigns require regular training and tactics for keeping up to date with threats and making security a topic people see and hear on a regular basis, not just annually.

Not All Data Is Equal

Does your company have a clear data classification scheme and policy in place that categorize the organization's data and information – sensitive, confidential, public, etc.?

	Scheme			Policy		
	2014	2013	2012	2014	2013	2012
Yes	58%	63%	50%	71%	72%	69%
No	33%	20%	30%	24%	18%	19%
Don't know	9%	17%	20%	5%	10%	12%

Commentary

- There's an increase in the number of organizations that lack a data classification scheme.
- A positive trend is the drop in the "Don't know" responses for both data classification scheme and policy, which suggests more organizations are engaged in the data classification process and at least have an understanding of whether or not these best practices are in place.
- A look at the findings by respondent group reveals significant gaps between top-performing organizations and other companies. As noted in the accompanying table, large organizations, companies with strong board engagement in information security risks, and those with all core information security policies in place are far more likely to be employing these best practices.
- Effective data classification, without question, is difficult to achieve. Companies should strive to simplify their approach where possible, which will enable greater progress and success with these efforts.

Percentage of organizations with a clear data classification scheme and policy

	Scheme	Policy
Companies with high board engagement in information security	79%	87%
Companies without high board engagement in information security	49%	64%
Large companies (≥ $1B)	72%	82%
Small companies (< $1B)	45%	61%
Companies with all core information security policies	78%	95%
Companies without all core information security policies	48%	59%

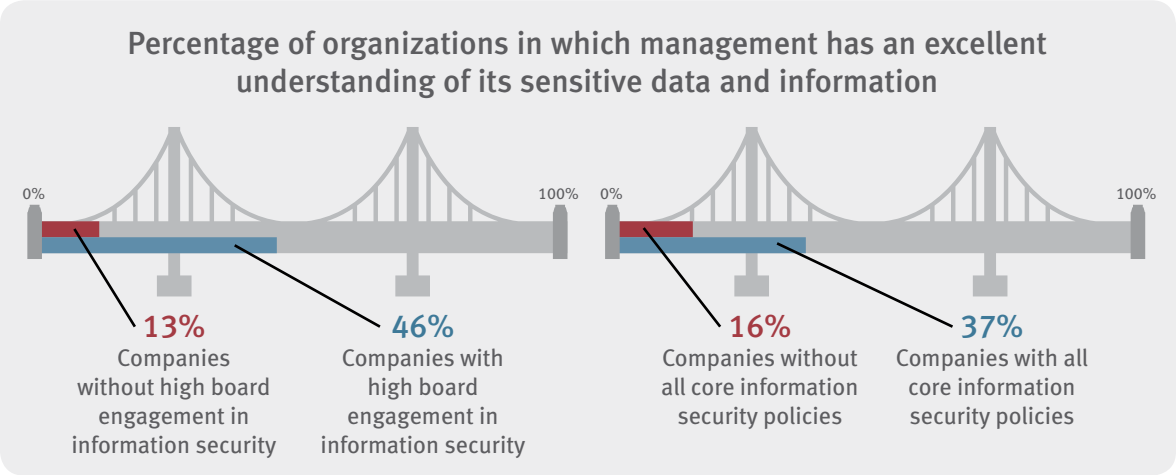
KEY FACTS

Data classification scheme – The groups or categories under which data is classified; for example: PII, sensitive, health, confidential IP, non-sensitive, public, etc.

Data classification policy – The guidelines dictating how, when and where the organization – including but not limited to all employees, functions and third parties working on behalf of the organization – classifies, manages and secures its data.

How would you rate your management's understanding of what comprises its "sensitive" data and information?

	2014	2013	2012
Excellent understanding	23%	27%	26%
Good understanding	51%	48%	50%
Limited understanding	22%	22%	22%
Little or no understanding	3%	2%	1%
Don't know	1%	1%	1%



Commentary

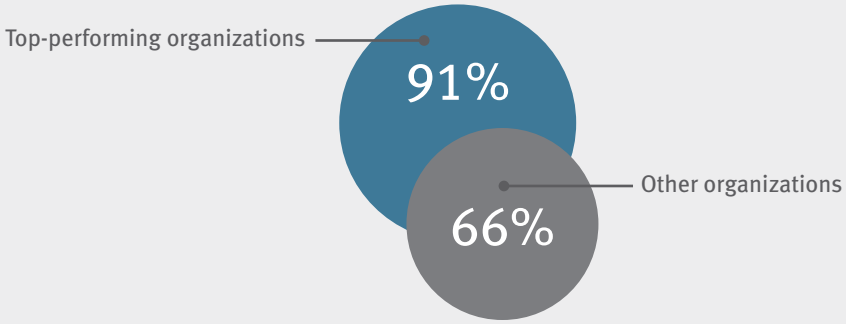
- Similar to last year's findings, in one out of four organizations, management is viewed to have limited or no understanding of its sensitive data and information. Given the risks and liabilities this information poses if not managed properly, these findings continue to be surprising.
- It is possible these findings are driving the data classification scheme results detailed earlier. Some organizations may lack definitions of their sensitive data, thus fail to make meaningful progress in formalizing a scheme and policy. It's important to note, though, that these definitions do not need to be perfected in order to get started with categorizing data effectively.
- There are striking differences in the results among top-performing organizations (high level of board engagement in information security risks, all core information security policies in place). Clearly, these practices are driving much greater understanding of the organization's sensitive data and information.

If you have not done a full data classification, how would you rate your level of awareness with regard to what your most "valuable" assets are?

		Top-Performing Organizations			
	All respondents	Companies with high board engagement in information security	Companies without high board engagement in information security	Companies with all core information security policies	Companies without all core information security policies
Very aware	45%	68%	35%	65%	36%
Somewhat aware	46%	26%	54%	32%	52%
Little awareness	9%	6%	11%	3%	12%
No awareness	0%	0%	0%	0%	0%

KEY FACT

Percentage of companies in which management has an excellent or good understanding of what comprises its sensitive data



From the following, please select the statement that best describes your organization's data retention and storage process.

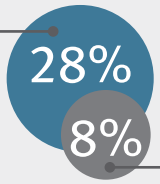
	2014	2013	2012
We retain all data and records with no defined destruction date	17%	9%	7%
We retain all data and records for a certain period of time, with a defined destruction date	43%	38%	22%
We have a basic classification system to define data, with a few specific retention policies and destruction dates depending on the classification	18%	25%	34%
We have a detailed classification system to define data, with varying retention policies and destruction dates depending on the classification	15%	19%	29%
Our organization does not have a formal data retention and destruction policy	5%	5%	3%
Don't know	2%	4%	5%

Commentary

- The percentage of organizations that retain all data and records without a defined destruction date has nearly doubled – this is not a positive development. Of note, with few exceptions (see Key Fact below), the findings do not vary significantly by respondent group. Retaining all data and records without a defined date to discard/destroy not only is inefficient and costly, but opens the organization to significant security risk and liability. The greatest effects of large-scale, high-impact breaches are felt in organizations that hold on to large volumes of data that they no longer need. Quite simply, "If you don't need it, don't store it."
- In our study, we continue to see a relatively small percentage of organizations that have a detailed data classification system in place, which involves stratifying the importance of data types and applying appropriate retention periods to each type based on regulatory and legal requirements as well as industry or company-defined standards.
- Such a system becomes more critical every day due to the growing volumes of data organizations are accumulating. An essential practice in effective data management and security is a comprehensive classification system that provides a clear understanding of how the organization is managing all types of data – sensitive, confidential, public, etc.

KEY FACT

Percentage of organizations with all core information security policies in place that have a detailed classification system to define data



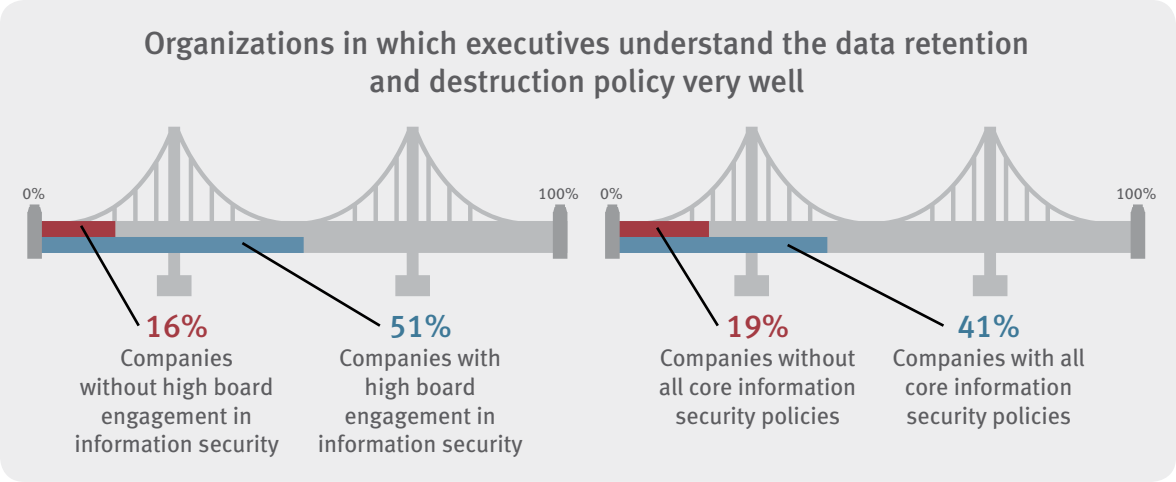
Percentage of organizations without all core information security policies in place that have such a system

How well do your C-suite executives (CEO, CFO, etc.) know and understand your organization's data retention and destruction policy?

	2014	2013	2012
They know and understand the policy very well	26%	30%	22%
They have some knowledge and understanding of the policy's general concepts	48%	43%	47%
They have limited knowledge about the policy	16%	18%	21%
They have little or no knowledge about the policy	4%	7%	6%
Our organization does not have a formal data retention and destruction policy	6%	2%	4%

Commentary

- Our year-over-year results are relatively consistent. However, similar to other findings in our study, there are substantial differences between top-performing companies (with regard to information security) and other organizations.

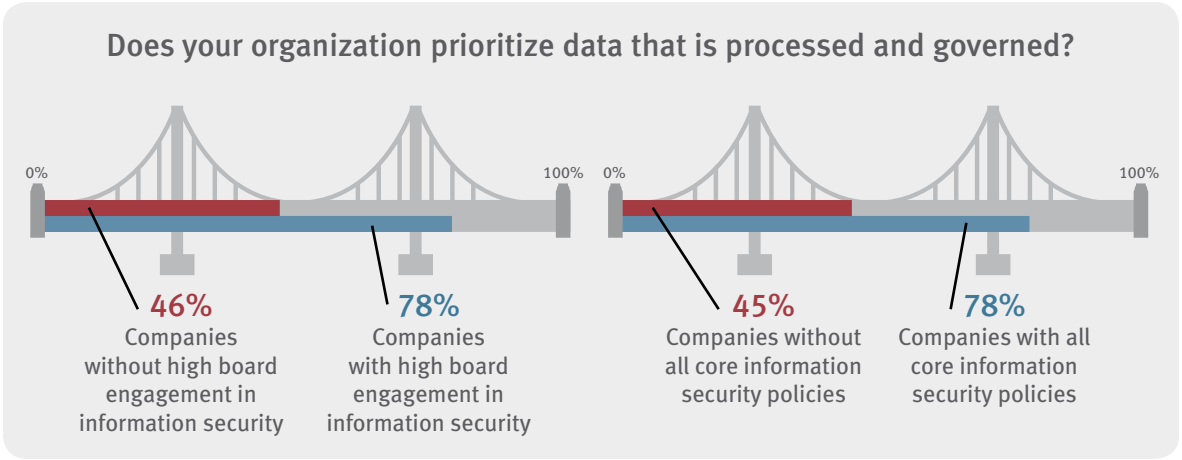


In your company, how well do you think management communicates to the organization/all employees the need to differentiate between public and sensitive data and how each is treated?

				Top-Performing Organizations			
	2014	2013	2012	Companies with high board engagement in information security	Companies without high board engagement in information security	Companies with all core information security policies	Companies without all core information security policies
Management does an excellent job of communicating these differences and how to treat each type of data	20%	23%	18%	45%	9%	30%	15%
Management does an acceptable job of communicating these differences and how to treat each type of data, but there is room for improvement	50%	50%	49%	43%	53%	59%	45%
There is substantial room for improvement in how management communicates these differences and how to treat each type of data	22%	21%	27%	10%	28%	10%	29%
Management has not communicated these differences or how to treat each type of data	7%	4%	4%	2%	9%	1%	10%
Don't know	1%	2%	2%	0%	1%	0%	1%

Commentary

- The overall results over the three-year period are very consistent. There are striking differences when reviewing the results of top-performing organizations.



Which of the following sensitive data types does your organization specifically prioritize? *(Multiple responses permitted)*

		Top-Performing Organizations			
	All respondents	Companies with high board engagement in information security	Companies without high board engagement in information security	Companies with all core information security policies	Companies without all core information security policies
Private client/ customer data	76%	84%	71%	88%	67%
Organization's intellectual property	57%	64%	53%	62%	54%
Payment Card Industry (PCI) data	40%	44%	37%	51%	31%
Healthcare data	34%	35%	34%	42%	28%

Commentary

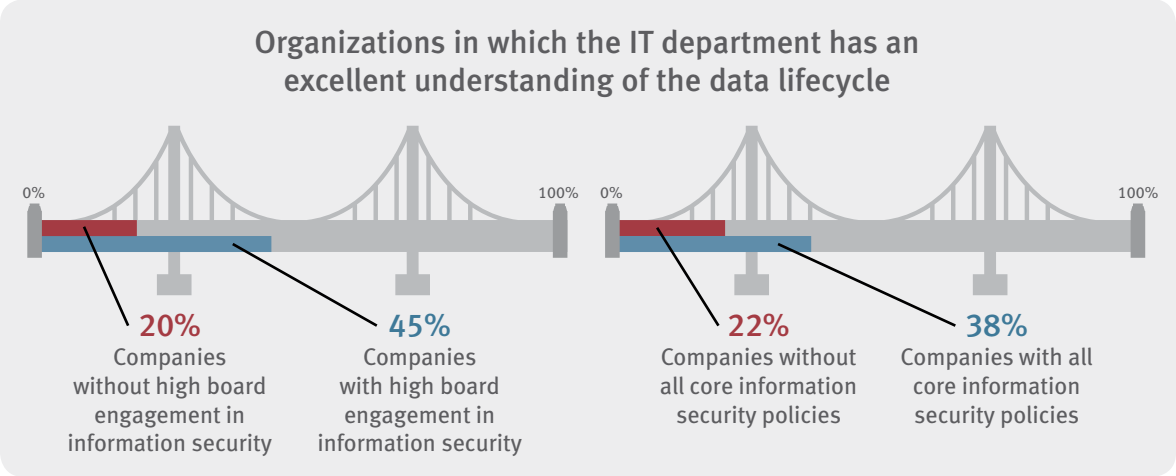
- It appears a significant number of organizations are not prioritizing their sensitive data. The response is especially for low for companies that fall outside the top-performing categories.

How would you rate your IT department's understanding of the lifecycle of the organization's data, from acquisition to retention/storage to (if applicable) destruction?

	2014	2013	2012
Excellent understanding	27%	21%	16%
Good understanding	52%	46%	39%
Limited understanding	16%	27%	34%
Little or no understanding	3%	3%	5%
Don't know	2%	3%	6%

Commentary

- In a positive development, there is a substantial jump in the number of IT departments that have an excellent or good understanding of their organization's data lifecycle. The results are even better for top-performing organizations.
- Companies are becoming more aware of their data lifecycle, and in particular, where and how long their data is stored. Gaps and deficiencies that we've identified in other results of our survey will likely begin to decrease as awareness continues to grow.



Growth in the Cloud – But Still Minimal Use for Confidential Data

Where is your company's sensitive data stored?

	2014	2013	2012	Large companies (≥ $1B)	Small companies (< $1B)
On-site servers	66%	57%	71%	68%	65%
Off-site servers	18%	21%	14%	19%	17%
Cloud-based vendor	8%	3%	2%	4%	12%
Not stored in any centralized location	6%	8%	8%	7%	4%
Don't know	2%	11%	5%	2%	2%

Commentary

- Similar to results from previous years of this survey, we see relatively few organizations moving their sensitive data into the cloud, despite news reports to the contrary. Yet there is a significant year-over-year jump. This is attributable primarily to the variance between large and small companies. That said, the use of cloud-based storage warrants attention to address emerging threats to data leakage and other risks.
- Also, while not shown, 11 percent of organizations with a high level of board engagement in information security risks rely on cloud-based vendors to store sensitive data.
- When storing sensitive data through a cloud-based resource, organizations need to focus carefully on the terms and conditions under which the cloud provider is operating, such as defining what data they will or will not retain and store, and information security standards. More companies are learning, through discovery or investigation, that their cloud-based vendors are holding more data than they originally were contracted to store. Setting these terms and conditions, along with service-level agreements, is critical.

CIOs Are Taking Charge of Data Governance

Who is responsible for creating and overseeing data governance in your organization?

	2014	2013	2012
Chief Information Officer	41%	38%	31%
Chief Security Officer	20%	16%	21%
Chief Financial Officer	5%	2%	5%
Chief Privacy Officer	4%	4%	7%
Individual department leaders (HR, Legal, Marketing, etc.)	14%	12%	18%
Other	8%	17%	12%
Don't know	8%	11%	6%

Who is responsible for executing the data governance strategy/policy in your organization?

	2014	2013	2012
Chief Information Officer	41%	31%	28%
Chief Security Officer	17%	18%	13%
Chief Privacy Officer	3%	3%	5%
Chief Financial Officer	2%	1%	3%
Individual department leaders (HR, Legal, Marketing, etc.)	20%	24%	34%
Other	8%	13%	10%
Don't know	9%	10%	7%

Commentary

- It is encouraging to see a three-year trend of growth in the CIO's role with regard to creating, overseeing and executing data governance strategy and policy. The CIO is in the best position to be responsible for these efforts, rather than individual department leaders.

Still Not Ready for a Crisis

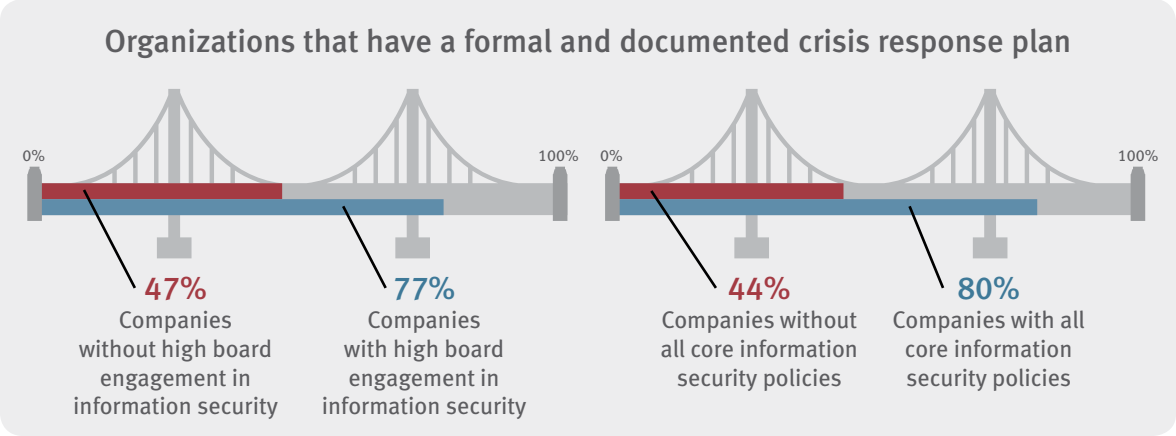
A significant number of organizations – even more than indicated in last year's results – lack a formal and documented crisis response plan to execute in the event of a data breach or cyberattack. And less than half perform periodic fire drills to test their plans.

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?

	2014	2013	2012
Yes	56%	66%	73%
No	34%	21%	12%
Don't know	10%	13%	15%

Commentary

- The overriding message here is that organizations cannot expect to stop all breaches, thus they need to have an incident response plan ready to execute, encompassing everything from tabletop exercises to full-blown testing (including disaster response).
- These results are consistent with findings from Protiviti's 2014 IT Priorities Survey, in which business continuity management and disaster recovery program testing, along with developing and maintaining IT disaster recovery plans, ranked among the major issues for CIOs and IT organizations to address.[3]
- Again, the results are noticeably better among organizations with high board engagement in information security risks, as well as companies with all core information security policies in place.
- Among those organizations that have a crisis response plan, there continues to be growth in the role of the CIO and other key roles that should be involved in executing this plan. Having these different critical perspectives is the best approach to ensuring the organization can respond swiftly and effectively to an incident or breach.



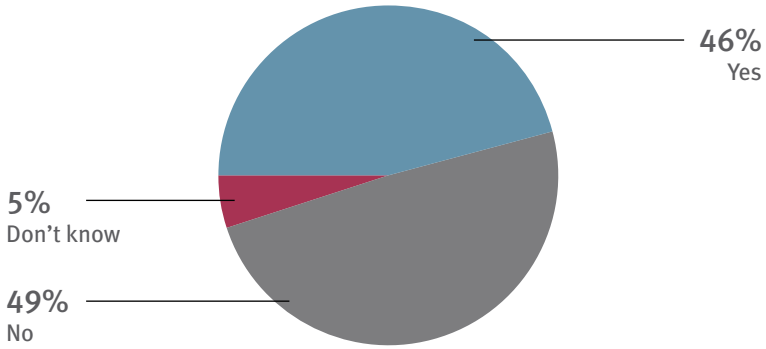
[3] For more information, please visit www.protiviti.com/ITpriorities.

As defined in your organization's documented crisis response plan, who needs to be involved in addressing a data breach or hacking incident? *(Multiple responses permitted)*

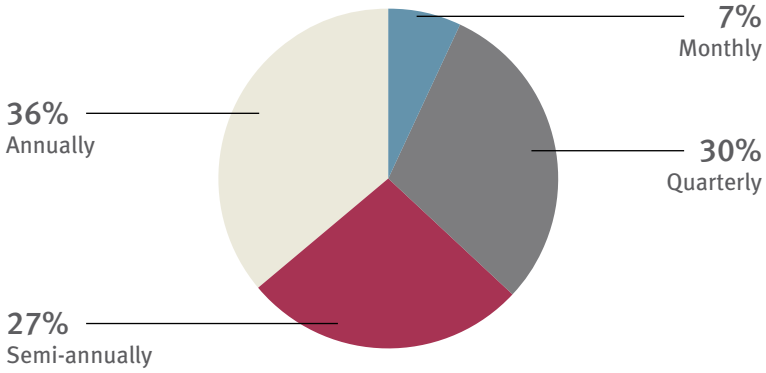
	2014	2013	2012
Chief Information Officer*	75%	72%	58%
Chief Security Officer*	56%	72%	58%
Chief Executive Officer	43%	38%	25%
Chief Privacy Officer	26%	38%	42%
General Counsel/Chief Legal Officer	46%	67%	71%
Corporate Communications	41%	63%	56%
Don't know	1%	20%	19%

** These roles were grouped together in previous years of this survey, but listed separately in this year's study.*

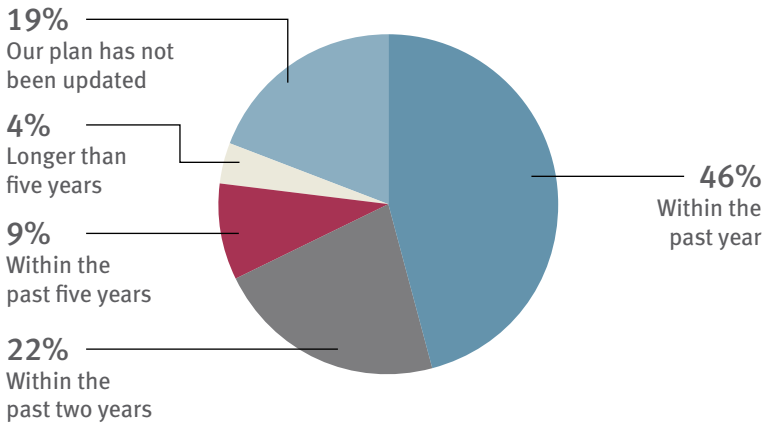
With regard to IT security, does your organization periodically perform "fire drills" to test your ability to execute the organization's incident response plan?



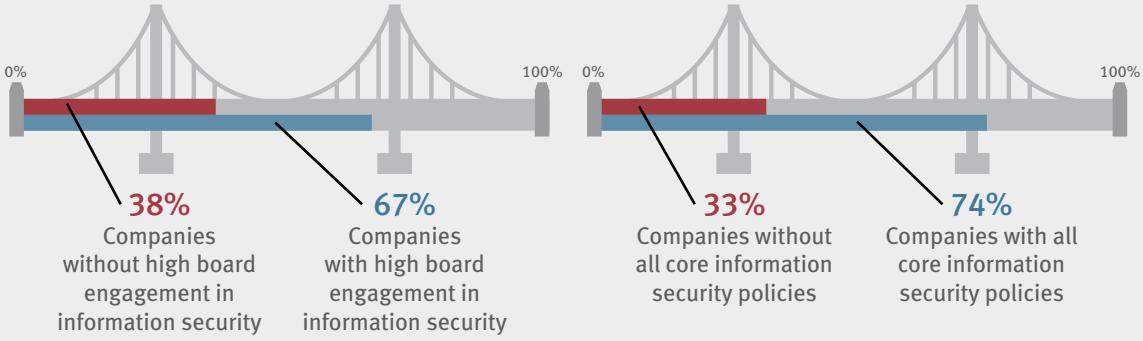
IF YES: How frequently does your organization perform its fire drills?



When was your organization's incident response plan most recently updated?



Organizations that have updated their incident response plan within the past year



Commentary

- While top-performing organizations have better numbers, a surprisingly large number of organizations fail to follow best practice with regard to testing their incident response plans. Again, it's important to understand that a security incident is very likely a question of "when," not "if," for almost any company.
- Even those organizations that have a crisis response plan may gain a false sense of security if that plan is not being exercised regularly. This minimizes the effectiveness of the plan and may mask deficiencies in it.
- Regulations such as HIPAA and PCI DSS, among others, include recommendations for at least annual testing of crisis response plans, as well as periodic reviews of the threat environment.
- While every organization is unique, general best practice calls for an annual risk assessment and testing every six months. Organizations also must consider any major implementations or infrastructure changes that have taken place, and update and test their crisis response plans as needed to ensure they are aligned with the changes.

Big Data Isn't That Big for Some Companies

Compared to two years ago, is your organization working more today with large databases ("big data") for business intelligence purposes?

	2014	2013
Yes – Significantly more	20%	20%
Yes – Somewhat more	36%	46%
No – We are working with large databases for BI purposes, but at the same level as 2 years ago	16%	15%
No – We are not working with large databases for BI purposes	22%	9%
Don't know	6%	10%

IF YES: From what source is that information being accessed or pulled?

	2014	2013
Existing, company-owned data	58%	44%
Combination of company-owned and third-party data	34%	54%
Third-party data	8%	2%

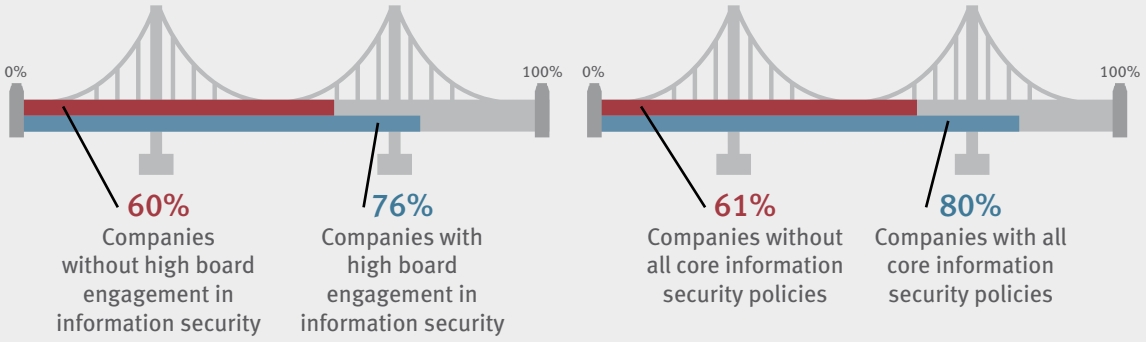
Commentary

- There is an overall drop in the number of organizations that are increasing their use of these databases, and one in five are not working with them at all.
- In one sense, this is not a bad trend. Security around big data is still in its infancy, thus there are greater security threats around it. It is prudent to be cautious.

Ensuring Security With Third-Party Vendors Is Just as Critical

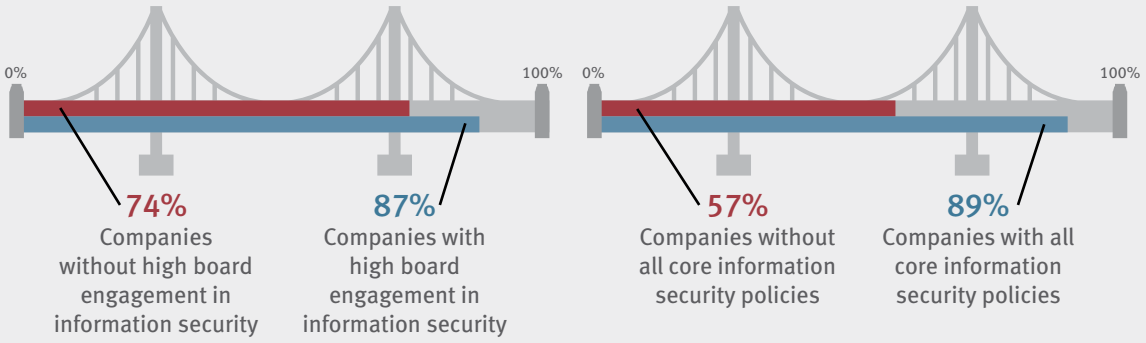
Following up on our earlier findings with regard to working with third parties and their data, a substantial number of organizations lack the standards, policies and practices needed to ensure the proper security measures are in place as part of these business relationships.

If data is being acquired/accessed from one or more third parties, has your organization ensured that it has all proper contracts and policies in place (including breach notification processes)?*



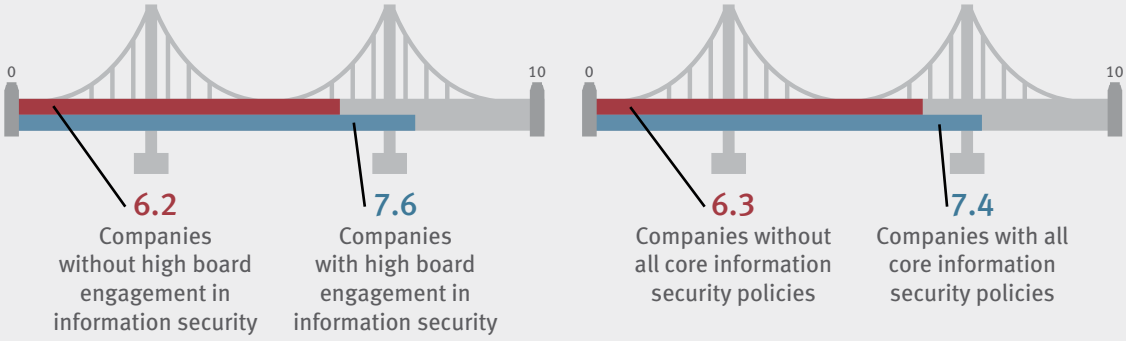
** Percentage of "Yes" responses shown.*

Are your vendors aware of the sensitivity of data being shared, and are they managing and securing that data in a manner consistent with your data classification requirements?*



** Percentage of "Yes" responses shown.*

On a scale of 1 to 10, where 10 is highly knowledgeable and 1 is not at all knowledgeable, how would you rate your organization's level of knowledge about the data security management programs and procedures of its third-party vendors?



Commentary

- One out of three organizations either don't ensure proper contracts and policies are in place regarding third-party access to their data, or simply don't know. It is possible that these organizations are unsure of what is required, thus they don't ask for terms with the vendor.
- Note that, across the board, the numbers are significantly better for top-performing organizations.

What is your company's policy on provisioning accounts for external access?

	2014	2013
Create accounts within an internal active directory	28%	29%
Create accounts within an active directory for external users only	20%	11%
Never create such accounts and do not permit access	18%	13%
Company has custom in-house solution	11%	13%
Federate with external parties	3%	4%
Federate with third-party providers	3%	1%
Do not have such a policy	10%	3%
Don't know	7%	26%

What is your company's policy on granting external access to sensitive data?

	2014	2013
Unique credentials accessible over a secured VPN	39%	44%
Never grant access	19%	13%
Grant access on the premises only	18%	12%
SSL access over Internet	10%	11%
Do not have such a policy	8%	3%
Don't know	6%	17%

DEMOGRAPHICS

More than 340 IT executives and professionals (n = 347) participated in the study. Following are details regarding the respondents and the size of companies represented in the study.[4]

Position (Title/Role)

Chief Information Officer	14%
Chief Technology Officer	5%
Chief Information Security Officer	5%
Chief Security Officer	2%
IT VP/Director	24%
IT Audit VP/Director	3%
IT Manager	33%
IT Audit Manager	3%
IT Staff	3%
IT Audit Staff	1%
Other	7%

Industry

Technology	21%
Financial Services	17%
Government/Education/Not-for-profit	17%
Manufacturing	10%
Healthcare Provider	8%
Insurance	6%
Communications	4%
Consumer Products	4%
Retail	4%
Energy	3%
Hospitality	2%
Utilities	2%
Healthcare Payer	1%
Real Estate	1%

[4] 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.

Size of Organization (by Gross Annual Revenue)

$20 billion or greater	8%
$10 billion - $19.99 billion	7%
$5 billion - $9.99 billion	11%
$1 billion - $4.99 billion	17%
$500 million - $999.99 million	10%
$100 million - $499.99 million	12%
Less than $100 million	35%

Type of Organization

Public	27%
Private	53%
Not-for-profit	7%
Government	13%

Location

United States	91%
Japan	6%
Italy	3%

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, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works 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 (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our IT Consulting Services

In today's rapidly evolving technological environment, a trusted adviser – one who not only provides relevant insights, but delivers a combination of strategic vision, proven expertise and practical experience – can enhance the value of your business with technology.

Our global IT Consulting practice has helped CIOs and IT leaders at more than 1,200 companies worldwide design and implement advanced solutions in IT governance, security, data management, applications and compliance. By partnering with us, you ensure that your IT organization performs with the same focus and excellence with which you manage day-to-day business operations. We will work with you to address IT security and privacy issues and deploy advanced and customized application and data management structures that not only solve problems, but add value to your business.

Contacts

Kurt Underwood
Global Leader, IT Consulting
+1.503.889.7771
kurt.underwood@protiviti.com

Scott Laliberte
Leader, Vulnerability & Penetration Testing
+1.267.256.8825
scott.laliberte@protiviti.com

Jeff Sanchez
Leader, Data Security & Privacy
+1.213.327.1433
jeffrey.sanchez@protiviti.com

Michael Walter
Leader, Security Operations Centers
+1.404.926.4301
michael.walter@protiviti.com

Rocco Grillo
Leader, Incident Response & Forensics
+1.212.603.8381
rocco.grillo@protiviti.com

Ryan Rubin
Leader, Identity & Access Management
+11.44.207.3890.436
ryan.rubin@protiviti.co.uk

Cal Slemp
Leader, Security Program, Strategy & Policy
+1.203.905.2926
cal.slemp@protiviti.com

THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
São Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

MEXICO*

Mexico City
Monterrey

PERU*

Lima

VENEZUELA*

Caracas

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Perth
Sydney

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*

Bangalore
Mumbai
New Delhi

INDONESIA**

Jakarta

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

SOUTH KOREA

Seoul

* Protiviti Member Firm
** Protiviti Alliance Member

EUROPE/MIDDLE EAST/AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

UNITED KINGDOM

London

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

SOUTH AFRICA*

Johannesburg

protiviti®
Risk & Business Consulting.
Internal Audit.