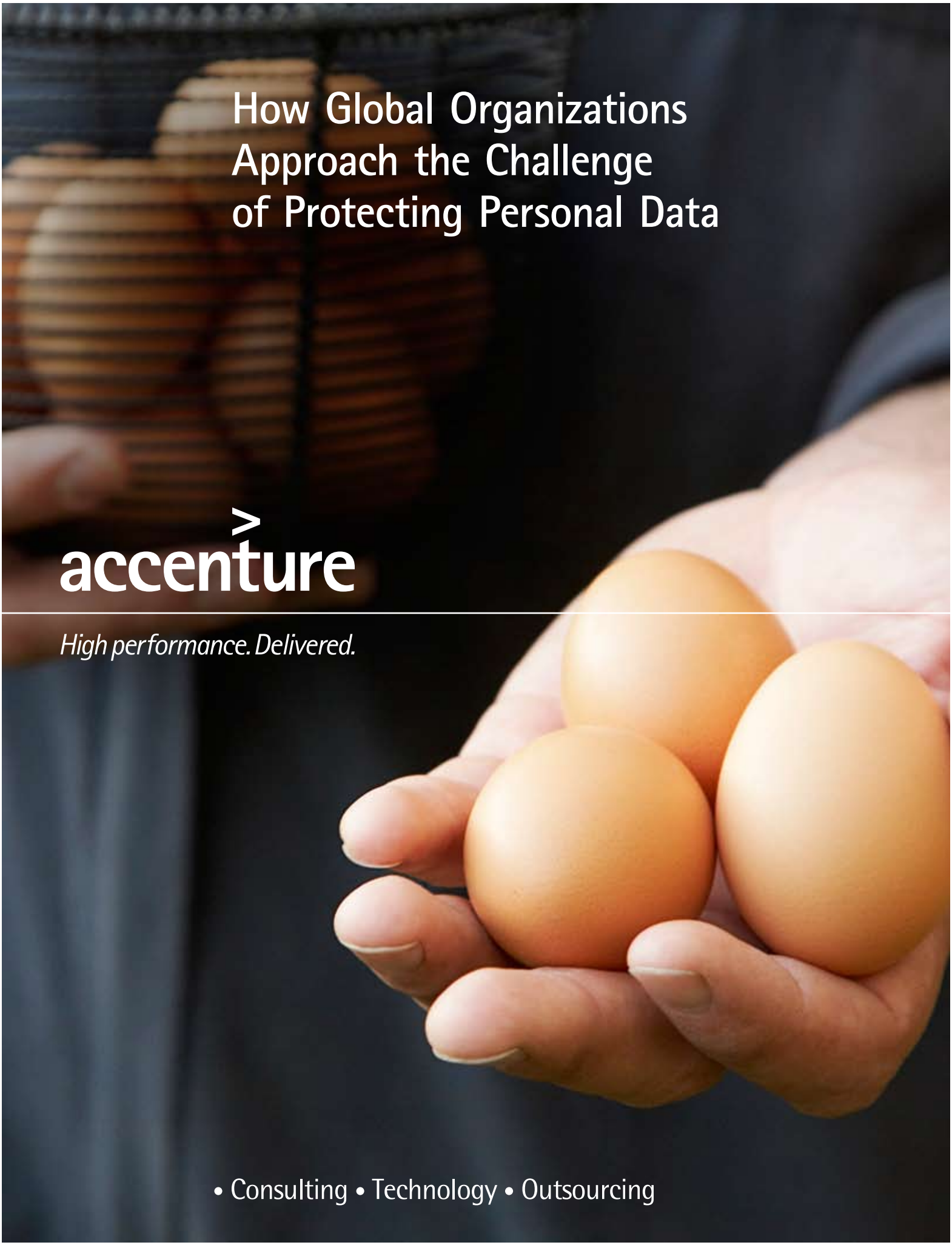
How Global Organizations Approach the Challenge of Protecting Personal Data



accenture

High performance. Delivered.

• Consulting • Technology • Outsourcing

Contents

Passing the Tipping Point

The volume of personal and often sensitive data being collected and shared by organizations today is growing exponentially—largely because of technology advances, lower data storage costs, the rise of the Internet and the emergence of major data brokerage companies.

However, as the amount of data an organization generates and collects has increased, so has the risk the organization faces of losing data and experiencing security breaches. Indeed, many organizations around the world have had their data compromised and have paid steep prices to repair the damage, fines, share-price declines and overall erosion of customer trust.

There is no doubt that organizations today are generating more data than ever. In fact, according to research firm IDC, despite the current economic downturn, the volume of digital data generated in 2008 increased 3 percent more than forecast and is expected to double every 18 months.[1]

Along with this increase in the volume of data has come a substantial rise in the potential for organizations to experience incidents in which their data is compromised in some way. Disruptive technologies such as software-as-a-service (SaaS) and cloud computing are one of the factors. Sourcing IT solutions from multiple content and service providers unlocks data held in IT silos and disperses it.

This increases risk by enabling confidential enterprise data to cross organizational boundaries, and the cloud itself presents risks because organizations have less direct control over how data is managed. Because their core business is based on securely storing customers' data, major cloud providers have made progress in IT security. In fact, many of them offer more sophisticated end-to-end, base-level security and privacy protection than might be found in the data centers of any single enterprise. However, there are still many open issues, such as data control and certification.

Data privacy and protection shortcomings can do irreparable harm to companies' balance sheets, not to mention their brands, credibility and customer trust and relationships.

Lightweight systems integration also contributes to the challenge. Taking advantage of Web 2.0-based collaboration tools, including "mash-ups" that combine disparate data stores in easy-to-use interfaces, can be an innovative way to improve productivity. Unfortunately, such user participation can lead to an increase in employees sharing sensitive enterprise data—anytime, anywhere, via any device. In fact, the portability of data (made possible by flash drives, CDs and other gadgets), coupled with the ability to access data via mobile devices (laptops and smart phones, for example), make it increasingly easy for data to be lost, stolen or abused. The security in a networked and interfaced world is as weak as its weakest link.

Unfortunately, while data privacy regulations continue to multiply, such regulations generally are not anchored on a common global standard. Worse, they also have trouble keeping up with technology advances and business practices that are dramatically changing how data is created, shared and stored. The result is a maze of regulations and privacy laws that are often intricate and complex at best, and at worst are costly and contradictory, or fail to properly address changing business models, global-data flows and technology advances.

Beyond regulations, organizations themselves have not kept pace in several critical areas. Many have trouble fully understanding how and where data flows across the organization, as well as establishing clear ownership and accountability for such data.

Furthermore, organizations often do not set clear expectations for employees in the area of data privacy and, in many cases, have technology infrastructures that no longer provide sufficient protection of sensitive data.

The preceding shortcomings have made organizations extremely vulnerable to security breaches and misuse of sensitive data. Indeed, in the United States alone, more than 263 million records containing sensitive personal information have been involved in security breaches since January 2005.[2] Such breaches can have serious implications.

Substantial financial costs to respond to and remedy the breach

According to the Ponemon Institute, the costs associated with a security breach have been rising year over year.

Fines, regulatory enforcement and lawsuits

A number of organizations around the world have suffered fines and lawsuits as a result of breaches they experienced. For instance, U.S.-based retailer TJ Maxx has set aside more than $200 million to deal with potential liability in the massive breach it experienced in January 2007.[3]

Erosion of shareholder value

Publicly held companies experiencing breaches of confidential information typically suffer a 5 percent drop in stock price when such a breach is made public.[4]

Inability to conduct business or, in the most extreme case, a collapse of political and economic stability

Today's computing infrastructures (including networks, systems, applications and data) are inextricably linked to the successful functioning of government, society and the economy. Given the interconnected nature of commerce and geopolitics, if these infrastructures are compromised, daily operations will grind to a halt, creating a ripple effect across the globe.

In short, data privacy and protection shortcomings put organizations in the dangerous position of no longer being able to assure customers that their data is safe from misuse and at risk of massive breaches that do irreparable damage to their balance sheets, brands and customer relationships. The challenge is particularly acute for multinational companies, which operate across multiple countries with their own privacy laws and cultural attitudes and are subject to a variety of industry regulations.

[1] IDC White Paper sponsored by EMC, As the Economy Contracts The Digital Universe Expands, May 2009

[2] http://www.privacyrights.org/ar/ChronDataBreaches.htm

[3] http://www.usatoday.com/tech/techinvestor/industry/2008-04-02-tjx-data-breach_n.htm

[4] "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, *Journal of Computer Security*, Vol. 11, No. 3, 2003, pp. 431-448.

Accenture Research on Data Privacy and Protection

Given the primacy of the issue, Accenture set out to shed light on the current state of data privacy and protection by surveying business leaders and individuals around the world. Our findings reinforced the notion that data privacy and protection is becoming more difficult for organizations to address and that sensitive personal data increasingly is at risk.

The objective of Accenture's research was to understand how data privacy perceptions and practices around the globe—from both business leaders and individuals—inform and influence data protection practices.

Our research involved two global surveys. In one survey, we polled 5,500 business leaders in 19 countries (Figure 1). Fifty-one percent of those participants were in management positions and 45 percent of them represented organizations with more than $2 billion in annual revenue (Figure 2). The second survey we conducted involved more than 15,000 adult-age individuals in the same 19 countries (Figure 1).

It is important to note that organization size did not unduly influence our results. In virtually all cases, there was no substantive difference between how business leaders representing smaller organizations (those with fewer than 1,000 people) responded and how those from medium-size and large organizations (more than 75,000 employees) answered the questions. The lone exception is that larger organizations were far more likely than smaller organizations to report having experienced breaches.

Figure 1

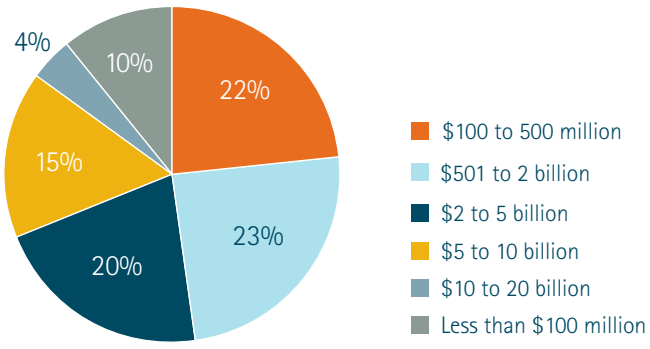
Business respondents and individuals participating in the survey represented 19 countries around the world.

Business Respondents	
North America (10%)	Canada United States
Europe (43%)	Belgium Italy France Germany Netherlands Russian Federation Switzerland United Kingdom
Asia (28%)	Australia Singapore Korea Japan India Hong Kong
Central/South America (16%)	Argentina Brazil Mexico

Individuals	
North America (11%)	Canada United States
Europe (43%)	Belgium Italy France Germany Netherlands Russian Federation Switzerland United Kingdom
Asia (32%)	Australia Singapore Korea Japan India Hong Kong
Central/South America (16%)	Argentina Brazil Mexico

Figure 2

Annual revenues (or public sector equivalent) of organizations participating in the survey.



Five key findings emerged from our research.

Finding 01

There is a notable difference between organizations' intentions regarding data privacy and how they actually protect it, creating an uneven trust landscape.

Finding 02

A majority of organizations have lost sensitive personal information, and among these organizations, the biggest causes are internal and therefore something they potentially could control.

Finding 03

Compliance complacency is prevalent throughout the world.

Finding 04

Understanding the perspective on and approach to data privacy and protection of business partners is crucial.

Finding 05

Organizations that exhibit a "culture of caring" with respect to data privacy and protection are far less likely to experience security breaches.

Finding 01

There is a notable difference between organizations' intentions regarding data privacy and how they actually protect it, creating an uneven trust landscape.

Not surprisingly, data privacy and protection is an issue of concern for businesses as well as individuals. Approximately 70 percent of both business and individual respondents strongly agreed or agreed that organizations have an obligation to take reasonable steps to secure consumers' personal information, disclose how they use consumers' personal information and deal with the ramifications if they lose consumers' personal information.

However, beyond the preceding, our survey revealed some troubling inconsistencies. Between 40 and 50 percent of the business respondents in our survey:

- Were unsure about or actively disagreed with granting individuals the right to control the type of personal information about them that is collected and how that information is used.
- Did not believe it was important or very important to limit the collection and sharing of sensitive personal information, protect consumer privacy rights, prevent cross-border transfers of personal information to countries with insufficient privacy laws and prevent cyber crimes against consumers and data loss or theft.
- Did not believe a range of typical organizational privacy practices were important or very important (including notice, consent, access, redress, security, minimization and accuracy).

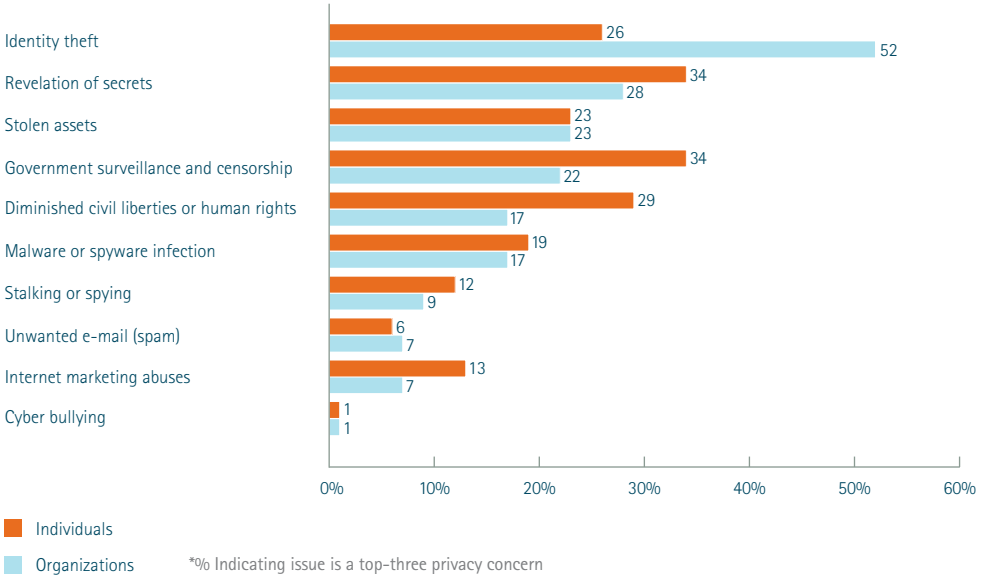
There are several possible explanations for this inconsistency, one of which is industry differences. In some industries, protection of consumers' data is paramount because of the type of information involved and the trust consumers place in the institution (such as financial services), while in others, it is not viewed as critical because the companies involved do not have direct contacts with consumers (for instance, in a business to business setting such as component manufacturers).

Cultural or regional differences also may play a role. Indeed, there are clear differences in how various cultures, countries and regions view the issue of privacy. The issue is far more important in the United States and European countries than in emerging markets and, thus, the former have much stronger regulations and laws concerning data and information privacy. Such differences can be exacerbated by the confusion created by different regulatory approaches or even conflicts of law. For instance, businesses with systems located in or accessible from the United States that host personal data for Europe and Canada may struggle to determine how to meet requirements of the U.S. Patriot Act (which gives the government the ability to request personal data in the name of national security), the Canadian Personal Information Protection and Electronic Documents Act (which codified a series of privacy principles established in 1996 as a national standard for the collection, use and disclosure of personal information), or any of the national data privacy laws implementing the European Union Data Protection Directive of 1995.

In addition, a lack of a clear definition of accountability and responsibility for data privacy and protection within the organization is a contributing factor. Many organizations do not clearly define where the oversight for data privacy and protection lies. They also may find that the management responsibility and accountability can be fragmented, with the Chief Information Officer, Chief Information Security Officer, Chief Privacy Officer or the legal function all having some involvement, depending on the specific aspect of data privacy and protection in question. For instance, the CIO could be responsible for maintaining IT and data security, the Privacy Officer for setting policies and procedures and general counsel for ensuring the organization is complying with regulations. Furthermore, organizations often do a poor job of assigning individual accountability to employees through appropriate policy education and training.

Figure 3

Individuals and organizations differ on privacy concerns.



*% Indicating issue is a top-three privacy concern

Organizations and individuals differ on privacy concerns

We also found there are some substantial differences in privacy concerns between individuals and businesses and government agencies, suggesting organizations may not be focusing efforts and investments in the areas about which individuals care most (Figure 3).

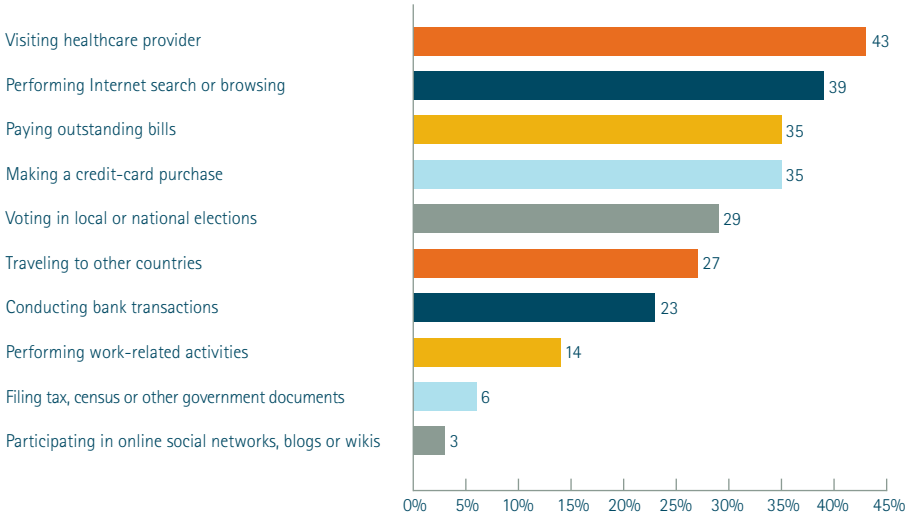
While business and government respondents were most likely to cite identity theft (52 percent) as one of their most significant privacy concerns, individuals were most likely to select revelation of secrets and government surveillance and censorship (each with 34 percent). These concerns among individuals are likely heightened in the wake of the post-9/11 push by governments to collect and share more intelligence on citizens in an attempt to more effectively root out threats to national security.

Interestingly, individuals' attitudes toward privacy and information sharing are highly dependent on the type of information being shared and the situation in which it is being shared—which can create challenges for organizations that depend on certain information (such as specific demographic data for targeted marketing).

Individuals are most comfortable sharing with governments and businesses typical contact information—name, home address, telephone number and gender (which are among the most likely types of information our business respondents reported collecting).

Figure 4

Individuals value privacy differently depending on the situation.



*% of individuals indicating privacy is most important when conducting this activity

Individuals are least willing to provide their race or ethnic background and medical history. Perhaps not surprisingly, the largest percentage of individuals (43 percent) said privacy is most important to them when visiting a healthcare provider (Figure 4). This finding is consistent with the fact that many laws now define health-related data as sensitive and are providing additional safeguards for them.

Individuals also are especially concerned about maintaining their privacy when searching or browsing the Internet. They worry about the ability of government and businesses to monitor their habits online and combine that information with other personal data to create personal profiles.

Conversely, individuals are least concerned about their privacy when participating in social networking, wikis and blogs—which are often the least secure kind of interaction on the Web. This particular finding certainly illustrates the shift in mindset among many individuals in the past five years in terms of what is considered "private" information—a shift that can create major challenges for employers when setting and enforcing privacy policies among a workforce that now contains a substantial portion of the younger generation, who have distinctly different views of what constitutes sensitive or personal information.

Finding 02

A majority of organizations have lost sensitive personal information, and among these organizations, the biggest causes are internal and therefore something they potentially could control. This suggests accountability for and ownership of how sensitive data is used may be lacking in many organizations.

Our survey revealed that security breaches are an ongoing challenge for many organizations. Fifty-eight percent of executives polled said they have lost sensitive personal information, and for nearly 60 percent of those who have had a breach, it was not an isolated event (Figure 5).

Larger organizations appear to struggle more to prevent breaches than smaller ones—likely because, with many more employees and more geographically dispersed operations, the opportunities for data to be lost or compromised are greater. Indeed, just under 70 percent of organizations with more than 75,000 employees have experienced a loss of sensitive personal information, compared with 40 percent of organizations with fewer than 500 people (Figure 6).

Individuals themselves are somewhat skeptical that organizations are doing enough to prevent such breaches, as 42 percent said they either are not sure or do not believe that companies and government agencies are adequately protecting personally identifiable data they have shared with these organizations.

Healthcare providers were named by the largest percentage of individuals as the type of organization most likely to protect information (44 percent), followed by the individuals' own employers (39 percent). Interestingly, only 14 percent said government agencies are most likely to protect personally identifiable information (Figure 7)—a finding that, again, seems to reinforce individuals' unease with the steps governments have taken in the post-9/11 era to enhance national security, as well as the increase in well-publicized data breaches by government agencies in the past year.

Internal issues—employees (48 percent) and business or system failure (57 percent)—were cited most often as the source of the breaches (Figure 8)—a finding that is in stark contrast to common perception that external forces are the biggest threats to privacy and security. However, this result is consistent with reports of major breaches, many of which were caused not by malicious external hacking but by simple error or negligence by an organization's employees.

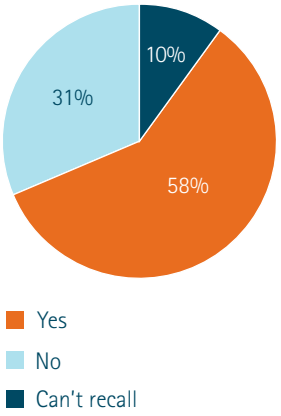
Indeed, a study by Cisco Systems found that two-thirds of end users in organizations have done one or more activities that could compromise corporate IT security, such as stepping away from their computer without logging off or shutting down, leaving their computer on their desk overnight, or carrying corporate data on portable-storage devices outside of the office.[6]

[6] "Security Thought Leadership: Data Leakage Study," Cisco Systems, August 2008.

Figure 5

A majority of organizations have experienced a security breach—and many have more than once.

a. Did your organization ever lose sensitive personal information?



b. If yes, how often has this occurred in the past 24 months?

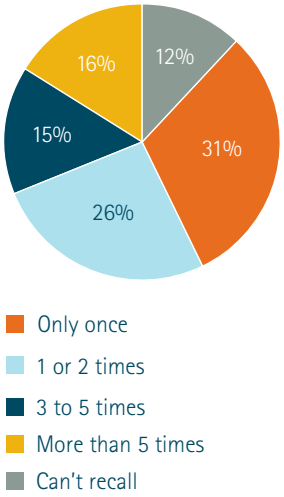


Figure 6

Larger organizations are more likely than smaller organizations to have lost sensitive personal data.

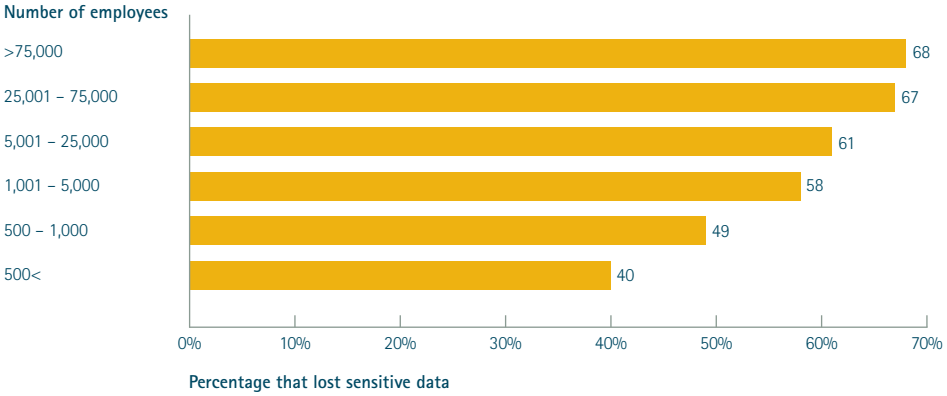
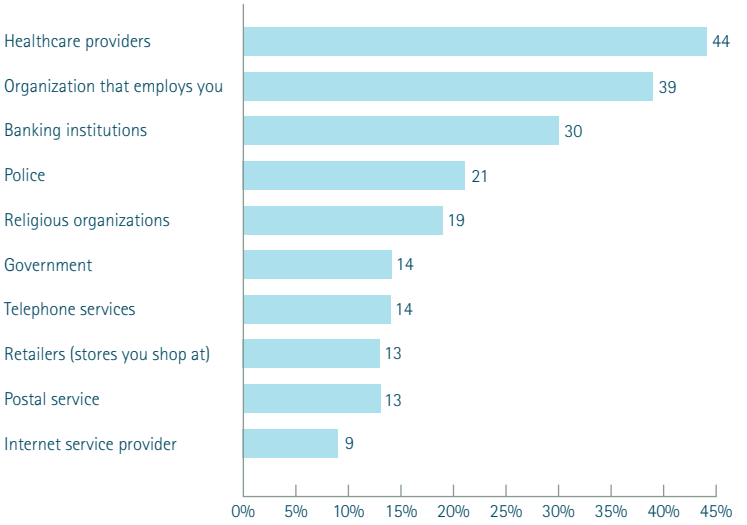


Figure 7

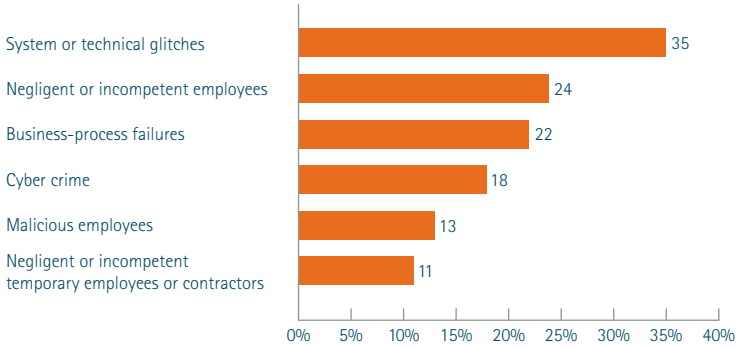
Individuals believe healthcare providers are most likely to protect information.



*% of individuals indicating organization types most likely to protect personally identifiable information

Figure 8

Internal issues are the most frequent causes of security breaches.



Why are the biggest threats coming from inside the organization? In our experience, there are several potential reasons.

One of most common reasons is a lack of adequate policies and training programs. A prevalence of breaches being caused by negligent or careless employees suggests the organization has not done a good enough job of developing and communicating strong policies for how sensitive data should be handled. Indeed, only 56 percent of organizations surveyed said it was important or very important to have a policy about their privacy practices. Furthermore, breaches may indicate there are shortcomings in the privacy- and security-related aspects of organizations' employee-training programs.

Lack of adequate controls also can result in recurring breaches. In many organizations, employees simply have too much access to sensitive data. For instance, nearly half of the organizations in our survey said limiting the collection and sharing of sensitive personal information was either only sometimes important, not important or irrelevant. Furthermore, approximately the same percentage believe it is either only sometimes important, not important or irrelevant to limit data collection to only that which is needed to fulfill legitimate business needs, or to adequately protect and secure individuals' or customers' personal information. And, perhaps most tellingly, just 19 percent of businesses said it is never acceptable to sell personal information for profit.

Many organizations also typically do not have a full understanding of data flows across the organization. As the amount of sensitive data an organization collects increases, it is often difficult to keep up with all the areas in which such data is generated, collected, stored and used. For instance, about three in 10 business respondents said they either did not know or were unsure of where personal information about customers and employees resides within their organization's IT enterprise.

Beyond people and organization issues, shortcomings in organizations' data privacy and protection technologies can result in data being compromised. Human error is inevitable. Yet organizations are not doing enough to implement technical tools that prevent employees from taking an action that will compromise an organization's data security.

Finding 03

Compliance complacency is prevalent around the world. Indeed, many organizations believe simply complying with existing regulations is sufficient to protect their data. However, such a mindset is ill-advised given the fact that regulations generally are not sufficiently sophisticated for today's business environment, nor are they consistent or equally applied across industries and countries.

Despite the fact that nearly 60 percent of organizations indicated it is important or very important to avoid regulatory and compliance violations, and just below 70 percent said they regularly monitor privacy and data protection regulatory-compliance requirements, breaches still have occurred in 58 percent of organizations polled. Even more intriguing is the fact that more than 66 percent of businesses in Europe, where privacy regulations are most stringent, admit having had a data breach incident in the past 24 months, and just under half of these organizations have had two or more data breach incidents.

The fact is, the current spectrum of regulations simply are not sophisticated enough to be able to account for all possible problems that could emerge given the rapidly increasing volume of data that organizations collect and the complexity inherent in how such data is accessed and used by organizations.

Making matters worse is the fact that there are no common or consistent standards for dealing with data privacy and protection from country to country or even within individual countries. For example, in the United States alone, there are 49 different state laws that regulate notification of security breaches, as well as separate laws that govern the use of various types of data (such as financial and health data). How does an organization know which applies and, more importantly, create and implement the internal controls that enable it to comply with all of them?

Another example demonstrates how regulations vary by industry. In the United States, the Payment Card Industry (PCI) Data Security Standard, Health Insurance Portability and Accountability Act (HIPPA), and the Gramm-Leach-Bliley Act (GLBA) all were created with the same goal in mind: to protect sensitive data. However, they focus only on specific data elements. The PCI standard, for instance, is only concerned with a credit-card holder's primary-account number, while HIPPA is designed to safeguard personal health information and GLBA focuses on protecting consumers' financial information.

Organizations that believe being in compliance with existing regulations is sufficient are not doing enough to proactively protect data and improve their overall security posture.

Finding 04

Understanding the perspective on and approach to data privacy and protection among third parties with which an enterprise does business is crucial. Organizations should “choose carefully the company they keep.”

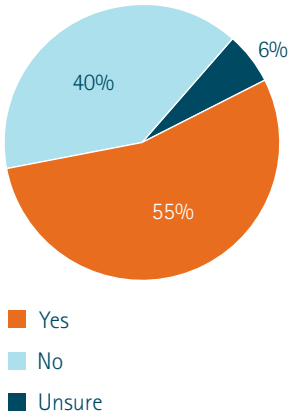
According to our survey, 55 percent of organizations outsource the collection or processing of personal information about customers to a third party (Figure 9). Data must be kept in the safest hands possible, and therefore trust and confidence in outsourcing providers is absolutely crucial.

Organizations must understand not only the provider's own data privacy and protection program to ensure it meets (or better yet, even exceeds) their own efforts, but also its knowledge of and experience with managing data within and across national boundaries.

For instance, Accenture operates a comprehensive global client data protection program that provides a standardized, consistent approach to protecting clients' data. This program covers all critical elements of data privacy and protection, including employee training, regular monitoring and auditing, oversight, appropriate responses in case of a breach, enforcement and discipline for inappropriate actions, and comprehensive protective measures to prevent breaches. The program reflects the fact that Accenture views safeguarding client information as one of its most fundamental and important responsibilities, and essential to maintaining the trust that forms the cornerstone of its client relationships.

Figure 9

A slight majority of organizations outsource the collection or processing of personal information about customers to a third party.



Finding 05

Organizations that exhibit a “culture of caring” with respect to data privacy and protection are far less likely to experience security breaches. Such organizations tend to view themselves as stewards, not owners, of personal data and take actions to protect data entrusted to them.

As mentioned earlier, 58 percent of organizations experienced at least one security breach in the past two years while 31 percent did not. And in fact, 21 percent of organizations actually had two or more breaches, suggesting serious security shortcomings in some areas of those businesses. Recurring breaches were just as likely to occur in large organizations as they were in smaller enterprises.

When we compared the group that had no breaches with the group that had two or more incidents, we found the former group demonstrates some substantial differences from the latter in terms of their attitudes and policies regarding data privacy and protection, as well as in what they thought were acceptable uses of personal data. In general, our analysis indicates that those organizations with no breaches seem to exhibit an overall "culture of caring" with regard to sensitive data and a mindset that they are not owners of such data but, rather, stewards of that data and it is their responsibility to protect and safeguard it.

Attitudes

Organizations with no breaches were more likely than those with two or more to believe individuals own their personal information and the enterprise is responsible for managing and protecting it.

As noted in Figure 10, the former tended to believe individuals have substantial rights to manage, correct and control information collected about them and to understand how such information is being used. Additionally, the "no breach" group were more likely to feel a stronger obligation to uphold data privacy and protection—for instance, by taking reasonable steps to secure individuals' personal information, control who has access to such information, disclose to individuals how their personal information is used, and help them if the organization loses their personal information.

Figure 10

Attitudes. Organizations with no breaches were more likely than those with two or more to believe individuals own their personal information and the enterprise is responsible for managing and protecting it.

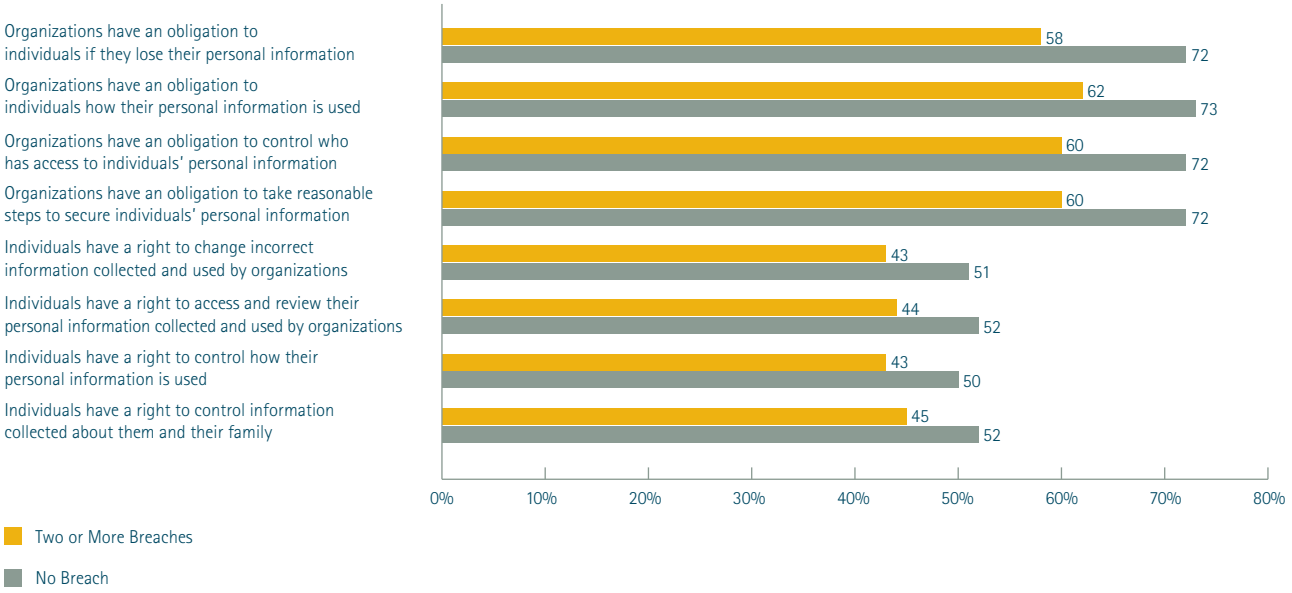


Figure 11

Policies. Organizations with no breaches tend to have policies that value the protection of sensitive data and how such data is used.

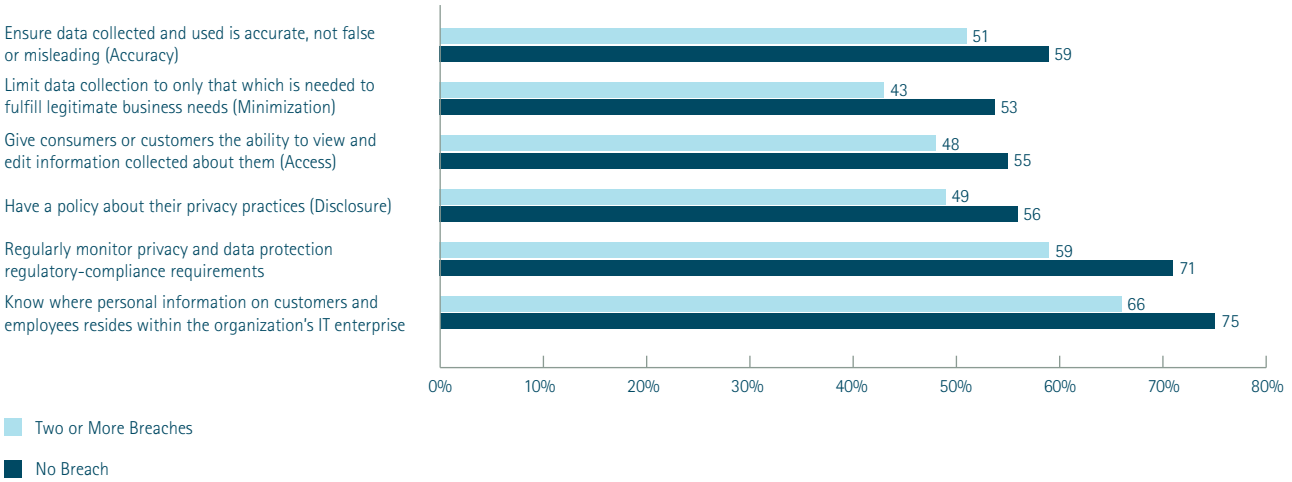
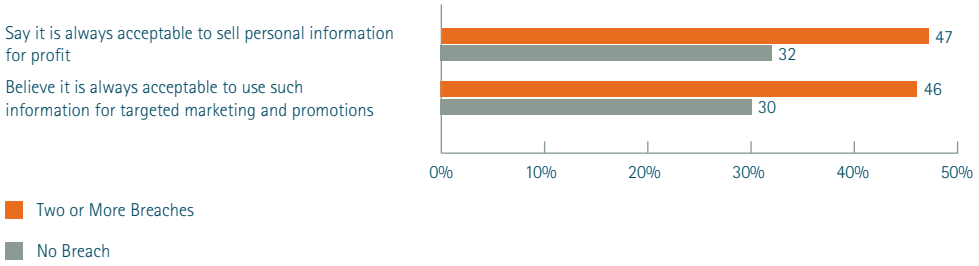


Figure 12

Uses. Organizations with no breaches are more likely than those with two or more to take a stricter line in terms of what they think are appropriate uses of personal information.



Policies

Organizations with no breaches tend to have policies that value the protection of personal data and how such data is used.

For instance, no-breach organizations are more likely to know where personal information on customers and employees resides within the organization's IT enterprise. This understanding enables these organizations to more effectively protect data across the enterprise. Furthermore, organizations with no breaches are more likely to regularly monitor privacy and data protection regulatory-compliance requirements. And, organizations with no breaches are more likely than those with two or more to consider a number of data privacy and protection practices important or very important (Figure 11).

Uses

Organizations with no breaches are more likely than those with two or more to take a stricter line in terms of what they think are appropriate uses of personal information.

Both groups largely agree that it is acceptable to use personal information to identify and authenticate customers and for research and product development, as well to share such information with law enforcement personnel for fraud prevention and the government for national security purposes.

However, the groups differ substantially in their opinions on using personal information in other ways. The group with two or more breaches is more likely to believe it always is acceptable to use such information for targeted marketing and promotions and to sell personal information for profit (Figure 12).

Addressing the Data Privacy and Protection Challenge

Key Actions and Practices

It is clear that organizations today have an urgent need to take a more proactive approach to data privacy and protection to not only minimize the risk of regulatory violations and major fines for non-compliance, but also to avoid experiencing breaches of sensitive personal data that can alienate customers, erode customers' trust and destroy the organization's brand and credibility.

With data privacy and protection now a major challenge for all organizations, it is time for the issue to receive more serious attention among not only senior executives, but also all employees. The findings of our research, as well as our work with leading organizations around the world, suggest a number of actions organizations should take to improve their ability to secure sensitive data, and proactively combat threats and position themselves to achieve high performance.

At a broad industry level, organizations must undertake two critical initiatives—the first of which is reexamining their data protection and compliance framework. In most industries, not enough work has been done to ensure that data protection and compliance frameworks have kept pace with how, and how quickly, data is generated, collected and shared. The data protection framework should address data protection at a holistic level and avoid addressing regulatory compliance in a silo. Such a framework not only can reduce overall compliance costs, but also improve an organization's overall posture for data privacy and protection.

Secondly, organizations should create a common set of data privacy and protection standards that can be applied consistently from country to country to minimize complexity, cost of compliance and chances for breaches while, at the same time, enabling responsible data sharing and global data flows. A global standard must recognize the data privacy and protection ecosystem and assign accountability appropriately across key stakeholders: organizations, individuals and regulators. Each has a role in protecting data and privacy rights. The standard should provide prescriptive guidance on what data must be protected, what the main requirements for data collection and use are, the rules for access to sensitive data, and how to protect the sensitive data based on data sensitivity and classification.

Microsoft has been a leader in urging lawmakers to give data privacy and security a higher priority. "On the legal front, we at Microsoft believe the United States needs an all-inclusive, uniform privacy law that will give consumers more control over their personal data and more reason for confidence in providing information to legitimate businesses and other organizations," the company stated. "With the flow of information becoming increasingly global, we also see a growing need to align U.S. law with current and emerging privacy standards in the rest of the world."[7]

At an individual organization level, organizations should emulate the leaders in our survey by creating a "culture of caring" with regard to data privacy and protection. There are a number of tangible steps organizations can take and practices they can employ to begin creating such a culture to help safeguard sensitive individual information.

Assigning ownership of and accountability for data privacy and protection through a data governance program.

Organizations that want to create a culture of caring and become good stewards of individuals' sensitive data should assign executive responsibility and oversight for data privacy and data protection, and put in place a data governance program that integrates the processes, people and technology needed to manage data effectively and efficiently. It begins with a custom model consisting of defined roles and responsibilities for data owners and data stewards.

Bringing together those people and functions can help an organization create a comprehensive and coordinated approach to protection and privacy (as well as to the management of information overall). In some cases, it may make sense to establish a data privacy and protection council—comprising stakeholders, data owners and data stewards from across the business—that is responsible and accountable for overseeing how sensitive data is managed and used, as well as for the continuous improvement of the organization's security posture. Such a coordinated, cross-functional approach helps to reinforce the fact that data privacy and protection is the responsibility of everyone in the organization, and to weave awareness of the issue into the fabric of the organizational culture.

Sun Microsystems, General Electric and Intel all have formally extended the remit of their privacy officer's role to information governance and/or data security to ensure a holistic approach to information management and protection. And Procter & Gamble has committed to following data privacy policies based on six fundamental tenets: global consistency of principles, local flexibility in implementation, accountability of data owners, privacy across the extended enterprise, choice and access to the individual and a community approach to privacy issues.[8]

Creating an information strategy that enables the organization to identify, track and control how data flows across all areas of an organization's systems and processes.

By taking a holistic approach to information management, an organization will be able to manage the entire information life cycle, clearly delineating how data is collected, stored, managed and used (including who is allowed to access and use which data).

To implement such a program, an organization first should conduct an enterprise-wide evaluation of its systems and processes to identify all flows of sensitive data. With such intelligence in hand, the organization can put in place the mechanism for an ongoing evaluation of the legitimacy of various uses of sensitive data within all business processes to limit the collection and storage of such data, as well as an ongoing regular review of all business processes that involve sensitive data to identify the creation of any new sources of data and new data flows that could be compromised if left unprotected.

Procter & Gamble, often cited as a leader in data privacy, is committed to understanding where its data resides. The company has identified and monitors data repositories within the organization that contain personal data on individuals in 14 categories.[9]

One of the ways to keep tabs on new sources of potentially sensitive data is to conduct a Data Privacy Impact Assessment for new systems and processes that collect and use personal data. Such an assessment has long been endorsed by privacy regulators in Europe and North America, and recently it has become a requirement for all US federal departments and the UK government departments. Many companies, too—including Accenture, Google and Acxiom—use the method to evaluate new business processes, offerings and services and ensure that data privacy is addressed from the very beginning.

Evaluating their current data privacy and protection technologies to confirm they are providing the necessary level of protection.

Because computer incident-response technologies are not generating adequate insights from prior breaches—thus impairing proactive risk management—organizations should reevaluate their installed base of such tools and consider enhancing or replacing them. Implementing the right technology will help an organization manage information effectively and support its security, governance, and information management goals. More importantly, because technology alone does not prevent potential information loss, it must work in concert with the agreed-upon data governance framework and standards, as well as the data governance council.

Companies such as Microsoft and Intel have sought to help companies address this issue by embedding data privacy in their product and technology development to ensure new technologies and products are better equipped to comply with data privacy and data security requirements.

Procter & Gamble has been a pioneer in using technology to support its data privacy efforts. The company was among the first to adopt privacy-monitoring software worldwide to help the organization comply with the patchwork of laws governing information from country to country. Among the technology installed are online monitoring tools that automatically check P&G's consumer websites for compliance with countries' laws relating to cookie regulation, opt-in marketing and advertising to children. Such software enables P&G's data privacy team to keep tabs on hundreds of its websites and, by cataloging online content, substantially cut the time necessary to find potential vulnerabilities.[10]

Building a consistent level of awareness of the importance of data privacy and protection among the workforce and providing employees with the appropriate guidance for how to handle sensitive data.

It is increasingly important for organizations to create more comprehensive and robust employee-education and training programs that promote a consistent and common understanding of data privacy and protection policies and procedures and give specific guidance on how to adhere to them.

However, to create a true culture of caring, an organization must do more than train employees to raise their awareness of the importance of data privacy and protection to both the organization and its customers. They need to motivate employees to take these requirements very seriously by explaining the consequences of a breach for the organization, its mission, its customers and its employees.

Procter & Gamble, General Electric and Accenture are among those that have well-established employee-training and communication platforms that go beyond pure training on data privacy and security policies by seeking to establish a culture of responsible use and sharing of information (including the use of social networking and other Web 2.0 technologies).

Reexamining their data privacy and protection investments.

Few organizations have a true enterprise view of their investments in security—a situation that not only prevents them from understanding the true cost of security, but also makes it difficult for them to reallocate investments as necessary to areas of high priority.

An organization should have a balanced investment when it comes to data privacy and protection. The investment strategy should not be focused on technology alone, but should consider all key aspects of the issue: people (the appropriate training and awareness-building programs); process (process improvement that

limits the collection and storage of sensitive data to minimize the exposure of sensitive data and overall scope of compliance); and technology (implementing or enhancing the appropriate data protection controls).

Additionally, any data protection and privacy initiative should be implemented in phases. Such an approach enables an organization to spread the implementation cost over time and allow the implemented controls and processes to become mature, repeatable and optimized.

A growing number of global organizations—including Accenture, General Electric, Phillips and British Petroleum are developing and implementing comprehensive data privacy compliance programs that are mandatory, are implemented uniformly across their global organizations and provide a high level of privacy and protection for personal data on their employees, customers and website users. These so-called Binding Corporate Rules (BCR) enable these organizations not only to share data across their global operations and processes, but to embed, manage and measure data privacy compliance effectively in all areas.

General Electric, in fact, was recognized by the International Association of Privacy Professionals (IAPP) for the progress it has made in implementing Binding Corporate Rules. GE won the IAPP Privacy Innovation Award in 2006 for being the first company in the world to "pursue a BCR policy that assures employees that their data will be handled using the highest and best practices no matter where in the world the employee or the data is located."[11] The company's BRC model is the basis for GE's relationship with its 350,000 global employees and is communicated in 27 languages.

In the public-sector arena, many government agencies that are putting more information and offering more services online are implementing a process to review technology investments to ensure both employee and taxpayer information are adequately secured.

Choosing business partners with care.

Organizations should collaborate with business partners that take equal or greater care with data, and rigorously assess partners' knowledge, practices and experience in managing sensitive data across organizational and national boundaries in accordance with local privacy laws and industry regulations. Organizations must be vigilant when it comes to confirming the security posture of the companies with which they do business, especially as business takes them to countries with differing standards for data privacy and protection.

Awareness of suppliers' and other business partners' security practices—including understanding the country's data protection regulations under which the organization operates and strictly monitoring how and when their data is used by providers and where such data is sent—is critical to verify proper practices are in place to protect sensitive data. Organizations also should ensure that providers', as well as their own, responsibility and accountability are clearly understood.

Microsoft is one of a number of leading organizations that have developed vendor-management programs to enable them to embed data privacy considerations and requirements in the procurement process and during delivery. Such companies also have implemented auditing processes to test the providers' security practices.

Having formal incident response policies, procedures and teams.

Despite the best intentions, incidents do happen. And when they do, it is critical for organizations to have a pre-defined and tested incident-response plan that enables the organization to quickly respond to and address the situation to minimize potential damage the breach can cause. Organizations should have formal policies and procedures for how to deal with breaches, as well as identified incident-response teams (representing all required functional areas) that mobilize when a breach is detected. Also vital to the post-incident response process is a definition of metrics that are important for the organization to track—such as type of incident (virus, malware or inappropriate sites accessed, for instance), frequency of incidents and cost to the enterprise. And, organizations should ensure that the findings of the response team investigating a breach are reviewed with stakeholders outside of the core-security team.

Incident response can be especially challenging in global organizations, where offices often address local incidents on their own without the involvement of the corporate entity's data security team. Such a localized response can result in the situation spreading to other areas of the organization as well as a failure of the broader enterprise to learn from the incident and make necessary changes to the rest of the organization to help stem such breaches from occurring in the future. To help avoid such disconnects, organizations should more tightly integrate their processes governing the reporting of and response to incidences.

[7] "Microsoft Lobbying for Data Privacy Laws," Joe Lewis, *WebProNews*, March 21, 2007, http://www.webpronews.com/topnews/2007/03/21/microsoft-lobbying-for-data-privacy-laws

[8] "12 Questions Every GC Should Ask," Corporate Executive Board, 2007, http://74.125.95.132/search?q=cache:NFvwH3dmBEcJ:https://gcr.executiveboard.com/Members/12Questions/

[9] "12 Questions Every GC Should Ask," Corporate Executive Board, 2007, http://74.125.95.132/search?q=cache:NFvwH3dmBEcJ:https://gcr.executiveboard.com/Members/12Questions/

[10] "P&G Privacy Plan Tackles Data Laws," Daniel Thomas, *Computing*, December 2, 2004, http://www.computing.co.uk/computing/news/2071314/g-privacy-plan-tackles-laws

[11] "The IAPP Announces Winners of the IAPP Privacy Innovation Awards," organization news release, October 24, 2006, https://www.privacyassociation.org/index.php?option=com_content&task=view&id=967&Itemid=116

Making Data Privacy and Protection a Core Business Value

As personal and sensitive data continue to be generated in ever-greater volumes, it is imperative that organizations take greater strides to protect this important asset—and not just because the laws say they should. Indeed, as our research shows, compliance should be only one part of a much larger and comprehensive approach to data privacy and protection.

More importantly, an organization's approach to data privacy and protection must not only be legally compliant, but also be a central element of the organization's value proposition. And because of the global nature of data flows today and the fact that many countries don't view the issue in the same way, the most effective data privacy and protection programs are globally reaching.

Organizations that view the issue of data privacy and protection as a C-suite concern and make it a core principle that guides their business will reap the benefits of lower risk of fines and enforcement action; a consistently high level of protection regardless of where in the world sensitive data is generated, stored, accessed or used; and a stronger brand and reputation that helps attract and retain customers. In other words, a superior approach to safeguarding sensitive data—one that positions data privacy and protection as a core corporate value—can be a distinctive capability that can help drive high performance in a dynamic and unpredictable global economy.

Contact

For more information about our Data Privacy and Protection services, visit **accenture.com/dataprivacy**.

Global Security lead
Alastair MacWillson
alastair.macwillson@accenture.com
+44 20 7844 6131

Global Data Privacy and Protection lead
Paul O'Rourke
p.orourke@accenture.com
+61 3 98387488

Chief Risk Officer
BPO and Technology Growth Platform
John B. McCormick
john.b.mccormick@accenture.com
+1 312 693 2589

Geographic Data Privacy and Protection leads

Austria, Switzerland and Germany
Mario Knop
mario.knop@accenture.com
+49 175 57 61046

Canada
Andy Truscott
andrew.j.truscott@accenture.com
+1 416 641 4114

Benelux and France
Frederic Peters
frederic.peters@accenture.com
+33 1 565 27 080

Italy, Greece and Emerging Markets
Enrico Palme
enrico.palme@accenture.com
+39 06 595 61111

Nordics
Gaute Lien
gaute.lien@accenture.com
+47 991 191 60

Australia, Singapore and South Korea
Troy Braban
troy.braban@accenture.com
+61 3 983 87 555

Spain and Portugal
Javier Martin
javier.martin@accenture.com
+34 91 546 9630

United States
David Kuo
david.kuo@accenture.com
+1 415 537 5094

United Kingdom and Ireland
Theresa Pa
Theresa.pa@accenture.com
+44 20 7844 8432

About Ponemon Institute LLC

Ponemon Institute conducts independent research on consumer trust, privacy, data protection and emerging data-security technologies. Their goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

As a member of the Council of American Survey Research Organizations (CASRO) Ponemon Institute upholds strict data confidentiality, privacy and ethical research standards. They do not collect any personally identifiable information from individuals or company identifiable information in our business research. Furthermore, they have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions. For more information, visit www.ponemon.org.

15 percent total recycled fiber

About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. With approximately 177,000 people serving clients in more than 120 countries, the company generated net revenues of US$21.58 billion for the fiscal year ended Aug. 31, 2009. Its home page is www.accenture.com.