Contents

Foreword................................................................................. 1
As the pace of technology continues to accelerate, 2014 promises to be another eventful year for privacy professionals.

Introduction........................................................................... 3
Eager to please the voracious appetite of the new super consumer, organizations are looking for every advantage. Through an ever-emerging array of new technologies, they can communicate, build relationships, gather reams of data and sell. But at what cost to privacy?

Technology trends have privacy implications ........ 4
Technology has fundamentally transformed the notion of privacy – what it means to affected stakeholders (individuals, regulators, organizations) and how each party can remain accountable in a world that technology has turned on its head.

Regulations fall behind as new technologies emerge........... 12
Today’s privacy regulations seem completely inadequate to protect individuals from the privacy risks that emerging technologies present. Yet, in the face of such daunting challenges, privacy commissioners and regulators around the world forge ahead.

To be accountable, organizations need to innovate ............. 14
Governments are making valiant efforts to protect privacy, but they cannot do it alone. Accountability for privacy and personal data protection needs to be a joint effort among governments, privacy commissioners, organizations and individuals themselves.

Conclusion............................................................................ 18
Ultimately, privacy shouldn’t be an either/or proposition. The future shouldn’t be about technology versus security versus privacy. The goal should be “and” – technology and security and privacy.
As the pace of technology innovation continues to accelerate, 2014 promises to be just as eventful for privacy professionals as in past years, if not more.

New and updated regulations, such as the new regulatory framework in the EU; new risks following intelligence leaks such as that by former US intelligence contractor Edward Snowden; as well as constantly evolving expectations from consumers, employees and regulators are all placing pressure on privacy professionals. Although the regulations and risks are always of interest to the field, it is these expectations, both of organizations and privacy professionals, that are most interesting.

We are managing privacy in a time where carefully considered, detailed regulatory requirements do not necessarily result in effective privacy or data protection. Technology innovations, at work and at home, are pushing the limits of privacy well beyond current regulatory standards and legal requirements.

In an effort to reinforce privacy protection as a top priority, it is incumbent upon organizations — particularly large, complex multinational organizations comprising multiple entities — to:

- Demonstrate privacy accountability and consistently apply privacy policies across functions and borders
- Embed privacy policies into new processes, products or services prior to launch
- Create a culture that understands the fundamental importance of privacy beyond reciting the organization’s policies

As the embodiment of the privacy management challenges organizations will face in 2014, technology was a natural choice to be the focal point of this year’s report. We hope this report, and the perspective it offers, helps to guide you as you navigate the existing and emerging privacy issues you are likely to face in 2014.

Foreward
Introduction

Behold, the digital revolution! It glitters with possibilities, opportunities and hope.

Consumers have seized the power to dictate what they want, when they want it, whom they buy from and how much they want to pay. Organizations, eager to please the voracious appetites of these super consumers, seize any opportunity available, often through an ever-emerging array of new technologies, to communicate, build relationships, gather reams of data and sell.

But at what cost?

Every time consumers browse the internet, log on and post to a social media site, or shop online, they are voluntarily – and sometimes involuntarily – giving away bits of information about themselves. Organizations gleefully collect these petabytes of data to better serve, market and sell. Yet both consumers and organizations often leave themselves vulnerable to disreputable entities that want this personally identifiable data for themselves.

In EY’s Privacy trends 2013 report (ey.com/privacy2013), we identified three megatrends that were playing increasingly larger roles across the privacy landscape: governance, technology and regulation. Last year, we led with governance, modeling the theme of the report around privacy accountability.

This year, our primary focus is on technology. Specifically, we explore the privacy implications associated with several emerging technology tools identified in EY’s 2013 Global Information Security Survey, Under cyber attack (ey.com/giss).

Technology is now moving far too quickly for privacy regulators to keep pace. Some regulatory mechanisms remain effective, such as the European Union’s Binding Corporate Rules (BCR). More often, regulations are outdated almost immediately upon release. And then there are some, such as Safe Harbor – the US-EU framework that has been in place for more than a decade – that are under siege.

So where does that leave us? How can organizations safeguard privacy in an age of technology? The answer lies more in governance than regulation, in innovation more than compliance. Organizations need to focus on privacy accountability that follows an ethical path as well as aligning with suggestions from regulators, that adheres to the spirit rather than the letter of any regulation, and that engenders the trust of those whose privacy an organization has pledged to protect rather than erode it by not instilling enough importance in privacy within the organization.

Privacy in the age of technology is quickly becoming a paradox. Privacy professionals, regulators and organizations need to work together to innovate new approaches that entrench privacy as a standard rather than an anomaly.
In 2011, the focus was on privacy in a borderless world. At the time, we noted that “technological advances will only continue to accelerate” and that organizations needed to be ready: that they didn’t have time to wait for global regulatory bodies to reach a consensus on privacy protection.

The following year, we made the case for growing accountability: organizations needed to take the lead on privacy and be more accountable for their actions. In 2013, we acknowledged that the uphill climb toward privacy protection and accountability needed to continue. We suggested that regulators and organizations needed to open the lines of communication and work together more effectively to serve as the stewards of privacy protection.

In 2014, our past vision about the accelerating speed of technological advances is now an unquestioning reality. It is fundamentally transforming every aspect of our personal and business lives, every industry, and every country across the globe. However, it also has the effect of fundamentally transforming the notion of privacy — what it means to affected stakeholders (individuals, regulators, organizations) and how each party can remain accountable in a world that technology has turned on its head.

In EY’s 2013 Global Information Security Survey, Under cyber attack, we asked respondents to rank by level of importance more than a dozen emerging technologies and trends. We grouped these technologies and trends into three categories: current, around the corner and on the horizon.

---

1 EY, Privacy trends 2011: challenges to privacy programs in a borderless world, January 2011.
We also asked respondents to rank emerging technologies and trends based on their level of importance, their level of familiarity with each and their confidence in being able to address the implications of these new technologies.

- **Familiarity**: are the emerging technologies known?
- **Capability**: are we able to deal with the security implications of emerging technologies?
- **Importance**: how much focus do we put on emerging technologies' threats?

We also asked our interviewees for their perspectives on emerging technologies and trends. From these results and the observations of our security professionals, we developed a correlation diagram that ranks level of importance against the level of familiarity and capabilities.

Of the 13 emerging technologies and trends respondents ranked, we believe seven technology trends will have the most significant privacy implications.
Current technologies

Digital devices and BYOD

One of the most pressing privacy issues related to digital devices today is the increasing ubiquity of bring your own device (BYOD) policies. According to Gartner, by 2018 up to 70% of mobile professionals will be using their smartphone to conduct work.²

As enticing as BYOD is for an increasing number of organizations, it is apparent that there are two sides to the BYOD coin: heads represents increased efficiencies; tails results in increased risk. And the risks are substantial.

In 2014, we expect to see organizations continue to deal with a number of privacy challenges related to BYOD. Organizations need to maintain ownership of their information. With BYOD, this information is stored on devices that now sit outside the organization’s immediate control. To keep an eye on their data, organizations tend to install monitoring tools on employee smartphones. However, when implementing these tools, organizations need to be very careful that they are only monitoring the company’s data and not collecting personal information about their employees and others such as friends and family who may use the device.

One solution, which is becoming more feasible as smartphones become more powerful, is the partitioning of the devices. This would allow employees to essentially operate two different desktops – one for work and one for personal. The other option is the use of a guest network that is separate from the main network. Organizations could create a “sandbox” where company data would reside, separated from any association with personal data, applications or online services.


---

Right to be forgotten

“It is increasingly more common for privacy regulation to include provisions for the employee’s right to be forgotten – to have a person’s personal data erased when leaving the organization – therefore, organizations operating in countries where such legislation exists should assess the impact to the organization and create formalized support procedures to handle such requests. These companies should consider leveraging these processes to also encompass BYOD-enrolled employees.”

— Bring your own device: security and risk considerations for your mobile device program
Current technologies have been on many organizations’ radar for several years. They are the technologies that a majority of organizations are using in some capacity. As these technologies continue to gain widespread use in 2014, organizations need to establish, review and update where necessary the accompanying privacy practices.

Social media

Social media has forever changed how companies, consumers, employees, regulators and governments communicate. Within the corporate environment, marketing functions use social media to develop and strengthen relationships with customers. Human resources functions use it to boost employee morale and improve internal communications. And organizations as a whole use social media to strengthen their brand and grow market share.

However, the same social media elements that generate business opportunity for companies to extend their brand can also destroy it.

In the past, companies generally focused their advertising budgets on traditional media, websites and sometimes blogs. However, as more organizations learn how to use the data they gather from social media to target individual customers – to create a customized customer experience – they will devote more ad buys in this direction. As a result, organizations tend to gather more information from their customers.

But as part of that collection process, who within the organization is thinking about protecting the personal information that customers so generously divulged? Many are thinking about what they can gain from mining that data. Few are thinking about how to protect the privacy of those who gave it.

In 2014, organizations need to be vigilant when collecting data from social media. Consumers are voluntarily providing intimate details about themselves. Organizations need to respect their privacy, even when the consumers themselves aren’t, by anonymizing the data before using and sharing it. Anonymous data can still provide deep insights into trends and opportunities, but with a much smaller privacy impact.

Regulatory considerations for social media in the power and utilities sector

The use of home-based remote sensors and smart grid technology can present privacy risks, not only because of data security-related issues, but also from a potential social media backlash as consumers worry about how utility usage may be used to exploit them.

In many countries, power and utilities are often governmental, or pseudo-governmental, and must comply with regulations and open records laws on issues around rates, the environment, customer education, disaster planning, legal discovery, data archiving and emergency communications.

More than addressing jurisdictional or industry regulatory compliance requirements, organizations should make privacy protection a fundamental tenet of their social media strategy and governance plan. This approach will enable organizations to strengthen their data protection processes and build trust with their customers.
Internet companies struggle to balance privacy and data collection

In the EY Global Technology Center’s View from the top: global technology trends and performance, April—August 2013 earnings season, the quarterly publication reported that internet companies remain at the forefront of collecting and digitizing the world’s information. However, their ongoing challenges continue to be a focus, including managing regulatory and privacy issues, which appear to be rising. In Europe, there was an online privacy “test case” lawsuit against an internet search engine provider that may help determine the balance between privacy and censorship. In the US, a Pew Research Center report revealed that teenagers appear far more concerned about online privacy than previously thought.

Big data and data analytics

Big data represents all the unstructured data that organizations collect internally from their own systems and employees, and externally from their customers, suppliers, partners and shareholders, as well as any technology tools that harvest data from users, such as social media. The amount of data organizations collect today is so massive and unwieldy that many organizations have no idea what to do with it, how to leverage it to drive revenue and, most importantly, how to store it safely to protect customers’ personal information.

Data analytics leverage these petabytes of data to understand and interpret past and present behaviors to anticipate future trends that speed decision-making, increase efficiencies and grow the business.

These technologies are very useful tools – when used appropriately. However, in the quest to improve efficiency and profitability, just as with social media, some organizations are forgetting that there are people behind the data and that their privacy needs to be protected.

In 2014, organizations should make anonymization of big data a priority before using it for analytical activities. Organizations need to verify that the sources they intend to use have appropriate permissions from the users who provided the data to perform any additional analytic activities. Even where those permissions exist, it is critical to minimize the exposure of identifiable elements as the data is handled and shared, even within the organization.

Cloud service brokerage

According to Gartner, by 2015 cloud service brokerages (internal or external) will provide at least 20% of all cloud services, up from less than 5% today. By 2018, the global cloud services brokerage market is expected to reach $10.5b, up from $1.57b in 2013.

The more comfortable organizations become with using cloud service providers to store their data, the more cloud service providers they will use. This creates a complexity that many organizations are ill-prepared to manage. Instead, they turn to cloud service brokers to help coordinate and manage multiple service provider relationships. Cloud service brokers

---

Technologies around the corner have been a focus of consideration for a short while. A small number of organizations may have started implementing these technologies, with a larger number seriously considering their adoption. As organizations consider mainstream use of these technologies in 2014, privacy implications should be front and center.

consolidate, coordinate and customize cloud service providers. They remove the burden of managing multiple cloud providers by offering a “one-stop shop” for buying and managing cloud services.

As the use of cloud services within organizations proliferates, and the procurement of these services increasingly occurs outside of IT, we expect to see a continuing rise in the use of cloud service brokers in 2014.

However, before turning to a cloud service broker, organizations must first verify that the use of a cloud service broker does not in any way derogate the level of information protection. Cloud service brokers will not only need to assume responsibility for managing cloud solutions, managing service level agreements, platforms, scalability and cost, but also understanding, applying, monitoring and maintaining the organization’s privacy policies across cloud service providers. As well, they will need to monitor and manage cross-border transfer of information. Many national regulations apply specific restrictions to the cross-border transfer of personal information.

Bring your own cloud

Just as BYOD began small before exploding into a major issue for many organizations, IT and privacy professionals within leading organizations expect bring your own cloud (BYOC) services to have the same trajectory.

They are easy to acquire – you need little more than half an hour to set it up and a credit card to pay for it – and therefore don’t require the involvement of IT, which is still seen as the “no” department. However, without IT oversight, security and privacy risks abound.

In reality, BYOC is an extension of the risks organizations have faced for years around employees sending company information through private (free) email services, such as Yahoo! Mail, Gmail, Hotmail and AOL. These email services, which almost everyone uses, provide, in essence, a cloud service that collects and helps users organize personal information. The difference between free email services and BYOC is in scalability. BYOC can easily accommodate more people loading and retrieving information. Basecamp, Dropbox, Evernote, SkyDrive and Google Drive are all good examples of BYOC.

In 2014, we expect to see many more departments within organizations engaging in BYOC. However, just as IT departments everywhere learned with personal devices and social media, IT cannot police BYOC by banning it. Instead, organizations need to proactively establish clear protocols that outline the security and privacy standards a BYOC must meet to be used.
In-memory computing

In-memory computing is the storage of information in the main random access memory (RAM) of dedicated servers rather than in complicated relational databases. It enables users to develop applications that can perform complex transactions in a more scalable way – and with the feeling of an instantaneous response.

This emerging technology will offer many opportunities for organizations, the most significant being the ability to collect and analyze data. In-memory computing will allow big data analytics to reach new heights. However, it will also present enormous privacy risks.

In 2014, amid this crush of data collection and analysis, privacy needs to be a primary consideration. There is a chance that the privacy policies an organization creates today may be obsolete by the time in-memory computing reaches critical mass. However, that doesn’t mean organizations shouldn’t set the boundaries. By creating a privacy framework, organizations can create a foundation for privacy that is flexible and scalable enough to adapt as new technologies, such as in-memory computing, emerge.
The ‘internet of things’

Have you heard of Shodan? Unlike other mainstream search engines, Shodan searches for what operates behind the scenes – security cameras, routers, webcams, home automation devices and heating systems. If it is connected to the internet, Shodan can find it. In fact, the headline-grabbing copy on its website reads: “EXPOSE ONLINE DEVICES.”

The fact that personal information is laid bare through online access to home heating systems and security cameras is bad enough, but what happens when an organization decides to triangulate consumers’ online behavior with purchasing habits offline by tracking movements on the internet, smartphones and even the traffic cameras outside of stores – without their consent?

In 2014, as organizations begin to think about the endless possibilities associated with the “internet of things” – nanotechnology, product sensors, sensor-driven analytics and sophisticated tracking capabilities – they also need to think about the privacy risks. There is a strong possibility, for example, that when an organization embeds a tracking mechanism into a product or service, it has not first sought the permission, either implicit or explicit, of the consumers being tracked. And when consumers find out, chances are they’re going to be irate. These kinds of privacy gaffes erode the very trust many organizations are attempting to cultivate to create the ultimate customer experience.

There is no question that the internet of things holds huge promise for an organization to vastly improve its strategic trajectories and business models, generate efficiencies and lower costs. However, this promise needs to be balanced against the privacy that consumers innately expect, and the privacy that they will demand alongside their customized customer experience.

---

Today’s privacy regulations, as well as those being considered by regulatory bodies around the world, seem completely inadequate to protect individuals from the privacy risks emerging technologies present.

Yet, in the face of the daunting challenges ahead, participants at the 34th International Conference of Data Protection and Privacy Commissioners met in Uruguay in October 2012 to forge on. They acknowledged both the progress many nations had made to improve privacy legislation, as well as the setbacks resulting from rapidly evolving technology and globalization. And they implored all parts of the world to review their data protection and privacy rules through the lens of consolidation and cooperation. Participants advocated for a coordinated response to cross-border data protection, better information sharing to maximize the benefits of scarce resources, and greater interoperability among legal and privacy bodies.8

In 2013, participants at the 35th International Conference of Data Protection and Privacy Commissioners continued their progress by adopting eight new declarations and resolutions that delved deeper into the issues raised the year before. Four resolutions focused on technology challenges (appification, profiling, digital education and webtracking), two addressed better coordination among jurisdictions (enforcement coordination and international law), and one urged greater transparency on what data organizations are collecting and why (openness).9

At a more granular level, many government bodies at federal and state levels are continuing to update their breach notification laws. Unfortunately, the massive intelligence leak by former US intelligence contractor Edward Snowden has cast a pall on the goals of cooperation. In fact, the Snowden affair has so eroded trust among nations that the European Union is considering a motion to suspend the US-EU Safe Harbor Framework. Once a respected guideline for US organizations to provide satisfactory protection for personal data of EU residents as required by the European Union’s Directive on Data Protection, the Framework now lies in limbo. This leaves Binding Corporate Rules (BCR) as one of the few frameworks available for global organizations to adhere to when seeking to transfer data of EU residents across borders.

---


“Compliance with the regulations on personal data protection is becoming an effective way for businesses to convey their ethical and social commitment. Respect of good practices as regards the protection of data of a personal nature certainly represents a competitive advantage for businesses, in any industry, and also helps them to guard against any risk to their reputation.”

— Cultural behavior and personal data at the heart of the big data industry, EY

Regulatory changes around the world

In 2013, a number of jurisdictions around the world improved or expanded their privacy regulations. We expect similar progress to occur around the world in 2014.

### Americas

- **Brazil**: Brazil seeks to mandate that global internet providers store data gathered from Brazilian users within Brazil.

- **Canada**: Bill C-475, working its way through Parliament, would unify and strengthen the country’s approach to breach notification.

- **US**: Although US lawmakers continue to push for a federal data breach notification law, Congress continues to debate whether federal law should supersede state laws.

### Asia-Pacific

- **Australia**: In late 2012, the Australian Parliament passed the Enhancing Privacy Protection Act. The Act is set to take effect in 2014.

- **China**: In late 2012, China’s Standing committee of the National People’s Congress approved a directive that strengthened online personal data protection. That directive came into force in February 2013.

- **Singapore**: Singapore’s Personal Data Protection Act 2013 came into force in 2013.

### Europe

- **EU**: Under a policy implemented in August 2013, European communication services providers are now required to notify not only affected individuals but their respective national authority within 24 hours of detection.

- **EU**: Crafted in 2012 and expected to pass in 2014, the EU General Data Protection Regulation is designed to simplify and strengthen the European Union’s data protection framework. Instead of adhering to requirements from 27 individual data protection authorities, organizations will only have to address one set of data protection rules.

EY supports standardization of privacy

When EY first began offering privacy protection services to clients in the 1990s, there were no set standards or established benchmarks in the privacy field. So when the International Association of Privacy Professionals (IAPP) formed and began developing the Certified Information Privacy Professional (CIPP) program in 2004, EY leaped at the opportunity to participate.

Since its inception, EY has worked with the IAPP to help define focus areas within the CIPP program, including the IAPP’s newest certification program – the Certified Information Privacy Manager (CIPM).

“We are applying certification in a way that matches the skill sets with the activities our privacy professionals are performing on a regular basis,” explains Sagi Leizerov, CIPP/US, EY’s Executive Director of Privacy Services.

“With the emerging global digital economy and the increasing popularity of cloud computing services, legislation which reinforces trust in the market will be a key driver for business growth.”

— European Commission

---

Governments are making valiant efforts to protect privacy, but they cannot do it alone. Accountability for privacy and personal data protection needs to be a joint effort among governments, privacy commissioners, organizations and individuals themselves.

Without such a coordinated effort, the whole notion of “right to privacy” may disappear. As the pace of technology increasingly outstrips governments’ abilities to regulate privacy protection, all stakeholders must take joint responsibility. Accountability needs to be about following the spirit more than the letter of the law. It needs to be about changing a collective culture and mindset so that everyone is accountable. It also needs to be about innovating rather than seeking solely to comply.

Leading practices to instill accountability

According to EY’s Global Information Security Survey 2013, 30% of respondents rate privacy as their number one or two priority in terms of investment, putting privacy 10th in the hierarchy of required information security investments. Privacy needs to rank higher.

“Privacy, security and fraud functions need to integrate. What customers and employees see as privacy information will have to change.”

– Financial services organization, EY Global Information Security Survey 2013
Which information security areas do you define as “top priorities” over the coming 12 months?

<table>
<thead>
<tr>
<th>Area</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity/disaster recovery</td>
<td>51%</td>
<td>17%</td>
<td>12%</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Cyber risks/cyber threats</td>
<td>38%</td>
<td>24%</td>
<td>14%</td>
<td>14%</td>
<td>10%</td>
</tr>
<tr>
<td>Data leakage/data loss prevention</td>
<td>26%</td>
<td>30%</td>
<td>20%</td>
<td>13%</td>
<td>11%</td>
</tr>
<tr>
<td>Information security transformation (fundamental redesign)</td>
<td>25%</td>
<td>19%</td>
<td>20%</td>
<td>16%</td>
<td>20%</td>
</tr>
<tr>
<td>Compliance monitoring</td>
<td>22%</td>
<td>31%</td>
<td>16%</td>
<td>16%</td>
<td>15%</td>
</tr>
<tr>
<td>Implementing security standards (e.g., ISO/IEC 27002:2005)</td>
<td>20%</td>
<td>21%</td>
<td>20%</td>
<td>19%</td>
<td>20%</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>18%</td>
<td>24%</td>
<td>23%</td>
<td>18%</td>
<td>17%</td>
</tr>
<tr>
<td>Security governance and management (e.g., metrics and reporting, architecture, program management)</td>
<td>15%</td>
<td>15%</td>
<td>20%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Information security risk management</td>
<td>13%</td>
<td>19%</td>
<td>26%</td>
<td>25%</td>
<td>17%</td>
</tr>
<tr>
<td>Privacy</td>
<td>13%</td>
<td>17%</td>
<td>21%</td>
<td>27%</td>
<td>22%</td>
</tr>
<tr>
<td>Securing emerging technologies (e.g., cloud computing, virtualization, mobile computing)</td>
<td>13%</td>
<td>17%</td>
<td>23%</td>
<td>23%</td>
<td>24%</td>
</tr>
<tr>
<td>Security operations (e.g., antivirus, IDS, IPS, patching, encryption)</td>
<td>12%</td>
<td>19%</td>
<td>22%</td>
<td>25%</td>
<td>22%</td>
</tr>
<tr>
<td>Recruiting security resources</td>
<td>11%</td>
<td>18%</td>
<td>26%</td>
<td>25%</td>
<td>20%</td>
</tr>
<tr>
<td>Offshoring/outsourcing security activities, including third-party supplier risk</td>
<td>10%</td>
<td>18%</td>
<td>30%</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>Secure development processes (e.g., secure coding, QA process)</td>
<td>10%</td>
<td>15%</td>
<td>25%</td>
<td>24%</td>
<td>26%</td>
</tr>
<tr>
<td>Security incident and event management (SIEM)</td>
<td>10%</td>
<td>20%</td>
<td>21%</td>
<td>28%</td>
<td>21%</td>
</tr>
<tr>
<td>Forensics/fraud support</td>
<td>6%</td>
<td>19%</td>
<td>24%</td>
<td>23%</td>
<td>26%</td>
</tr>
<tr>
<td>Security awareness and training</td>
<td>8%</td>
<td>15%</td>
<td>20%</td>
<td>25%</td>
<td>32%</td>
</tr>
<tr>
<td>Threat and vulnerability management (e.g., security analytics, threat intelligence)</td>
<td>8%</td>
<td>16%</td>
<td>21%</td>
<td>21%</td>
<td>34%</td>
</tr>
<tr>
<td>Incident response capabilities</td>
<td>6%</td>
<td>18%</td>
<td>25%</td>
<td>25%</td>
<td>26%</td>
</tr>
<tr>
<td>Security testing (e.g., attack and penetration)</td>
<td>6%</td>
<td>13%</td>
<td>21%</td>
<td>29%</td>
<td>31%</td>
</tr>
</tbody>
</table>

Survey respondents were asked to mark five bars showing their top priority with a 1, down to their fifth priority with a 5.

Key: 1st  2nd  3rd  4th  5th
In that same report, we identified four areas where organizations could improve their information security programs. In 2014, organizations can equally apply these leading practices specifically to privacy:

1. **Commitment from the top.** Gain board support to establish a charter and a long-term strategy for privacy protection.

2. **Organizational alignment.** As part of the organization’s strategy, develop a formal governance and operating model, align all aspects of privacy to the business and build relationships across the enterprise. Also, be willing to increase investment in privacy protection.

3. **People, processes and technology.** Document and communicate business processes related to privacy, and make them agile enough so that they can be updated when necessary. Consider new technology choices not only in terms of their benefits to the organization, but also the privacy risks they may pose.

4. **Operational enablement.** Allow good privacy governance to drive compliance, not the other way around. Measure leading indicators to monitor performance and make improvements as opportunities present themselves. Facilitate greater collaboration among functions. And leverage behavior-based analytics for more effective analysis.

The last leading practice that we will add, which wasn’t included in our list of leading practices for information security is: change the culture. Accountability for privacy needs to be everyone’s responsibility — from the boardroom to the shop floor. Use the forces of change to enable the use of new technologies with appropriate privacy protocols rather than banning them entirely. Additionally, consider robust training programs for employees so that they clearly understand and can act in accordance with established boundaries associated with privacy and personal data protection.

**US health care company takes leadership role in protecting personal and private data**

**The challenge:**
A not-for-profit health care organization with multiple hospitals and partner companies sought to strengthen the security of two types of data that it used and stored on a continuous basis: personally identifiable information (PII) for each staff and its providers, and protected health information (PHI) for each patient.

**The solution:**
EY provided wide-ranging support to help the organization grasp opportunities to improve the security of PHI and PII data. Team members documented the processes involved in data use and used a PHI/PII maturity model to assess associated levels of risk.

**The result:**
They performed a gap analysis of the organization’s PHI and PII data governance practices compared to leading industry practices. The team then prepared a future state model for data governance that enabled the health care organization to more easily comply with regulatory requirements.

They were able to reduce the risk of financial losses resulting from PHI data security breaches and related negative publicity, as well as enhance the organization’s public image as a leader in safeguarding personal and private data.
Technology is moving too fast for privacy regulators to keep pace; individuals don't know what they don't know about their privacy rights or the trade-offs they may be making. Organizations are so focused on delivering the ultimate customer experience that they sometimes lose sight of where the boundaries should be.

Ultimately, privacy shouldn't be an either/or proposition. The future shouldn't be about technology versus security versus privacy. The goal should be “and” — technology and security and privacy. However, to achieve this goal, organizations will have to do more than comply; they will need to innovate new policies for privacy protection as fast as emerging technology threatens to compromise it. This future is possible. However, it will require a fundamental change by all stakeholders in how we view privacy and what we are willing to do to protect it.

Questions for the C-suite

- Do you know your organization’s level of maturity when it comes to privacy?
- Is privacy a board-level priority within your organization?
- What steps do you take to anonymize the data to ensure customer privacy?
- Is privacy a consideration when acquiring and implementing new technology?
- Do you have privacy governance and operating models?
- Does your privacy program include documented processes and regular risk-based assessments?
- Do you monitor and measure your privacy performance on an ongoing basis?
Want to learn more?

*Insights on governance, risk and compliance* is an ongoing series of thought leadership reports focused on business and IT risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our *Insights on governance, risk and compliance* series at ey.com/GRCInsights

---

**2013 Global Information Security Survey:**
*under cyber attack*
ey.com/giss2013

**View from the top:**
*global technology trends and performance, April-August 2013 earnings season*
ey.com/ViewFromTheTop_2013Q2

**Bring your own device:**
*security and risk considerations for your mobile device program*
ey.com/byod

**Privacy trends 2013:**
*the uphill climb continues*
ey.com/PrivacyTrends

**Identity and access management:**
*beyond compliance*
ey.com/iam

**Knowledge is power:**
*using data analytics to drive your growth agenda*
ey.com/KnowledgeisPower
EY’s risk services

We have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance, as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our clients’ applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

The leaders of our RISK practice are:

### Global RISK Leader

Paul van Kessel
+31 88 40 71271  
paul.van.kessel@nl.ey.com

### Area RISK Leaders

#### Americas

Jay Layman
+1 312 879 5071  
jay.layman@ey.com

Jonathan Blackmore
+44 20 795 11616  
jblackmore@uk.ey.com

Iain Burnet
+61 8 9429 2486  
iain.burnet@au.ey.com

Shohei Harada
+81 3 3503 1100  
ahara-shh@shinnihon.or.jp

#### EMEIA

Ken Allan
+44 20 795 15769  
kallan@uk.ey.com

#### Asia-Pacific

Mike Trovato
+61 3 9288 8287  
mike.trovato@au.ey.com

Yoshihiro Azuma
+81 3 3503 1100  
avuma-yshhr@shinnihon.or.jp

The information security leaders within our RISK practice are:

### Global Information Security Leader

Ken Allan
+44 20 795 15769  
kallan@uk.ey.com

### Area Information Security Leaders

#### Americas

Jose Granado
+1 713 750 8671  
jose.granado@ey.com

Ken Allan
+44 20 795 15769  
kallan@uk.ey.com

Mike Trovato
+61 3 9288 8287  
mike.trovato@au.ey.com

Yoshihiro Azuma
+81 3 3503 1100  
avuma-yshhr@shinnihon.or.jp

© 2014 EYGM Limited.
All Rights Reserved.
EYG no. AU2093
ED none

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com