Privacy trends 2013
The uphill climb continues

Insights on governance, risk and compliance
January 2013
## Contents

- **Introduction** ........................................................................................................................................................................ 2
  - Privacy’s watchwords: governance and accountability ................................................................. 4

- **Governance evolves for regulators and businesses** ................................................................. 5
  - From enforcer to strategic advisor ............................................................................................ 6
  - Vendor assurance is not as easy as it looks ............................................................................. 8
  - The changing role of the privacy officer ............................................................................... 10

- **Technology offers opportunity, but includes a steep learning curve** ......................................... 13
  - Digital transformation demands accountability ..................................................................... 14
  - Monitoring uncovers privacy failures .................................................................................... 16
  - Personal privacy versus corporate security: it’s a fine balance ........................................ 18

- **Regulations struggle to keep up** ............................................................................................ 20
  - Privacy matures from compliance to accountability ............................................................ 21
  - Breach notification becomes a strategic imperative ............................................................... 24
  - *Privacy by Design* needs regulation to gain traction ....................................................... 26

- **Conclusion** ................................................................................................................................................................. 28
As the privacy landscape continues to evolve and mature, trends are forming around how market conditions are impacting organizations’ privacy decisions.

In years past, when preparing this report, we discussed the top privacy trends organizations faced individually. This year, we have organized them into three categories: governance, technology and regulation. These are the megatrends we see playing increasingly larger roles as we enter a new era in privacy protection.

Regulators globally are doing their best to keep up with the velocity of change that is pushing the need for stronger privacy protection. However, it seems that for every step forward, evolving technology sets them two steps back. It’s setting organizations back too. The digital world is still relatively young and boundaries are not yet fully established. Cyber attacks, inappropriate online etiquette and oversharing of personal information – these are just a few of the issues organizations need to navigate and regulate not only internally, but also on behalf of consumers who may not know better.

As the digital ecosystem evolves, regulators and organizations need to open the lines of communication. As regulators walk the fine line between advisors and compliance enforcers, organizations need to strive to create boundaries rather than push them. Together, regulators and organizations need to serve as the stewards of privacy protection.
These observations are echoed by the privacy leaders we asked to share their perspectives about today's privacy landscape and the challenges that lie ahead.

- **Allan Chiang**, Hong Kong's Privacy Commissioner for Personal Data, discusses the evolving role of the Data Protection Authority (DPA) and the importance of fostering open discussions with organizations rather than simply regulating.

- **John Gevertz**, Global Chief Privacy Officer at Automatic Data Processing (ADP), Inc. advocates for a standard privacy compliance framework that facilitates consistency in developing and assessing privacy programs, while addressing disparate requirements across industries and geographies.

- **Daniela Fabian Masoch**, Global Head of Data Privacy at Novartis, whose organization recently achieved binding corporate rules (BCR) status, talks about creating a global governance structure that is both strong, but also flexible enough to accommodate national or regional requirements.

- **Henri Kujala**, Privacy Officer in the Location and Commerce unit of Nokia, discusses the increasingly complex mobile ecosystem, and makes a strong argument for making privacy a foundational component of technology standards development.

- **Jules Polonetsky**, Director and Co-chair of the Future of Privacy Forum in Washington, DC, describes the legal challenges organizations can face in determining who owns personal data on mobile devices that may or may not be company-owned, but are used in a corporate setting. As the popularity of bring your own device (BYOD) rises, so too does the complexity of who gets to control the data that lives on an employee's smartphone or tablet and where to draw the line between personal privacy and corporate risk.

- **Fabrice Naftalski**, Ernst & Young Société d'Avocats® law partner and European Privacy Seal (EuroPriSe) legal expert, suggests that BCR status, once an optional goal for large multinational organizations, is becoming a must have.

- **Mary Ellen Callahan**, Partner at Jenner & Block LLP and former Chief Privacy Officer for the U.S. Department of Homeland Security dispels the myth that the European Union's (EU) privacy approach is more rigorous than the United States' sectorial approach – that, in fact, the two regions have far more in common than many would think.

- **Marielle Gallo**, Member of European Parliament and a Member of the Committee on Legal Affairs outlines how the role of the European Commission Data Protection Authority (DPA) will shift under proposed changes to the EU Directive on data protection. All observations follow a similar path toward governance and accountability. As the uphill climb to sound privacy management continues, organizations and regulators need make the journey together.
Privacy’s watchwords: governance and accountability

In the last 15 years, privacy regulations have had to evolve quickly to address operational and lifestyle changes brought forth by technology.

In the late 1990s and early 2000s, regulators around the world implemented regulations and guidelines to address specific compliance challenges, including Health Insurance Portability and Accountability Act (HIPAA), the clinical trial directive, spam and text message advertising. These regulatory responses were reactions to technological developments. For example, an important driver of the HIPAA privacy and security rules was the advances in genetic research and the concern that such health information could impact individuals as well as their blood-related relatives. The EU electronic communication directive also was created because of technology-driven communication. In China, the state imposed regulations limiting spamming on cell phones.

In the mid-2000s, personal information-based fraud became a regulatory focal point. Breach notification and information security legislation shifted the tide toward privacy as a material business risk. Companies and criminal organizations alike came to realize the immense value of gaining access to personal information. Criminals saw the monetary value. Organizations began to understand the financial and reputational costs of allowing unauthorized access to personally identifiable information. In the US, Asia-Pacific and Europe, regulators began fining organizations for privacy gaffes. The EU passed a breach notification law for the telecommunication industry. And other jurisdictions passed regulations requiring encryption solutions to protect data. In addition, organizations started talking of privacy, PCI and crisis management in the same breath. It is a trend that continues today.

We are now entering a new era, where governance and accountability play a central role in effective privacy management. Regulators realize that they can't keep chasing technological developments with specific requirements. Instead, they are emphasizing the importance of a “thinking” privacy program that assesses impact and applies the core requirements of privacy to changes in processes and technology. We saw it in the regulations developed by the State of Massachusetts in the US for detailed security programs over personal information. We see it in recent U.S. Federal Trade Commission (FTC) consent decrees. We see it in upcoming privacy regulation changes and the increased emphasis on BCR as solutions. We also see it coming directly from regulators, such as the guidelines from the Office of the Privacy Commissioner of Canada.

In this publication we discuss key trends in this new era and solutions to help organizations navigate the ever-evolving privacy landscape. We hope you enjoy the discussion.
Governance evolves for regulators and businesses

Globally, regulators are doing everything they can to keep pace with the changes that necessitate greater privacy protection. But for every one step they take forward, technology seems at least two steps ahead. Technology is evolving at such a rate that regulators may never catch up. Instead of climbing uphill to a peak they may never reach, regulators are recognizing that they may be more effective with a two-pronged effort: 1) continue to improve privacy protection through legislation and regulation; and 2) become strategic advisors and active participants in decision-making discussions with organizations and consumers.

On the business side, organizations have been attempting to use a number of tools that have been created to offer independent assurance of privacy programs. However, many organizations are not yet mature enough to meet all the rigorous requirements that assurance standards demand. Organizations and regulators need to find a middle ground that motivates organizations to be accountable without causing them to fail in their efforts.

One of the challenges organizations face is that information security and privacy remain relatively new phenomena. Still only approximately 30 years young, society as a whole is still struggling to understand the ever-expanding digital boundaries. Inappropriate online etiquette, cyber bullying and the over-sharing of personal information that constantly pushes privacy limits are just some of the issues the digital world has created. Within organizations, understanding and establishing these boundaries becomes increasingly important.

Organizations and regulators need to share the role of pillars of the digital community, setting the standards of trust and respect that the rest of society can follow.
From enforcer to strategic advisor

The accelerating pace of technological change has shifted regulators from regulation-makers to strategic advisors. Where their primary role was once to enforce the rules they created, many regulators are now equal parts compliance monitors, educators, liaisons between business and government, and active participants in the privacy debate.

For example, in Canada, the Ontario Information & Privacy Commissioner, Dr. Ann Cavoukian, has developed guidance relating to the personal data ecosystem (PDE) and the use of personal data vaults (PDV), which take advantage of emerging technologies to help consumers to collect, store, use, share, grant access to and manage their own personal information in a manner that is completely within their own control. Dr. Cavoukian also is credited with creating Privacy by Design (PbD), the seven-principle model that regulators globally strongly recommend organizations use to embed privacy into IT system implementations.

In fact, in June 2012, PbD was the topic of a large one-day conference hosted and organized by the Office of the Privacy Commissioner for Personal Data in Hong Kong. Described as a privacy landmark event in Hong Kong, the local commissioner invited a panel of distinguished speakers from Australia, Canada, the US and New Zealand. The intended audience of the conference was broad, ranging from data protection and compliance professionals, to privacy advocates and academics, to marketing managers, policy-makers, consultants and auditors. Sponsors included tech giants Google and Microsoft, as well as Ernst & Young. The objective was to educate local private and public sector organizations about PbD, the importance of its role in the future of privacy management and how organizations could go about implementing it.

Although the focus may be shifting, enforcement remains a crucial tool in a regulator’s arsenal. One of privacy’s biggest challenges remains a lack of enforcement action among certain industries and countries. Regulators voice these very concerns – the tension between working with organizations and enforcing regulations – during discussions about the proposed changes to privacy regulations in the EU. UK Information Commissioner Christopher Graham said of the issue that the proposals “demand that data protection authorities must impose fines … leaving no room for regulators to exercise discretion.” He went on to say that it would force regulators to “pick and choose,” and result in inconsistencies in the regulation’s application across Europe.

Fortunately, when it comes to enforcement, privacy regulators are getting some help from industry regulators and others operating outside the privacy sphere.

In the US, for instance, health care industry regulators have enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act, which calls for the states’ attorney generals and the U.S. Department of Justice (DOJ), to enforce HIPAA. At a state level, California’s Attorney General recently announced the formation of a Privacy Enforcement and Protection Unit within the DOJ. The unit is mandated to protect consumers through civil prosecution of both state and federal privacy laws. Similarly, in the UK, the Financial Services Authority is responding to privacy violations and levying heavy fines for non-compliance.

Personal data protection needs to be a business imperative

In my work as Privacy Commissioner for Personal Data in Hong Kong, I am constantly confronted with legal challenges related to our regulatory role under the Personal Data (Privacy) Ordinance (the Ordinance). There have been several cases in the last two years of organizations falling afoul of the Ordinance that we have sought to investigate. In many cases, our office faced legal challenges as to whether we were empowered under the Ordinance to act.

Our response to these challenges was simple: we asked these companies to ask themselves whether it made business sense just to leave the issue in the hands of their legal and compliance professionals. Invariably, they determined that the reputational risk associated with the privacy contraventions was too high to only meet what they considered to be the minimum legal requirements. As such, we were able to work with the top management of these organizations to address the relevant privacy and data-protection issues.

However, this shouldn’t be done after the fact. Organizations should be incorporating privacy into their business processes in much the same way that they incorporate other core values such as fairness, transparency and proportionality. To achieve an enduring and higher level of success, enterprises have to embrace personal data protection as a business imperative.
Vendor assurance is not as easy as it looks

In 2010, the American Institute of Certified Public Accountants (AICPA) finalized the Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization (SSAE 16). This global auditing standard replaced the SAS 70, which had been the authoritative guidance for reporting on service organizations. SSAE 16 enables organizations to obtain service organization controls (SOC) reports in the areas of privacy, security, integrity, confidentiality and availability. The demand for Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (SOC 2) has increased significantly since it took effect in 2011. However, in its first full reporting year (2012), many organizations have been challenged to meet the rigorous requirements of developing, maintaining and documenting the necessary controls, especially when it comes to privacy.

The Health Information Trust Alliance (HITRUST), borne from the need for health care providers to assure information security for health information systems and exchanges, has developed a common security framework (CSF) that can be used by any organization within or outside the health care industry that creates, accesses, stores or exchanges personal health and financial information. It is a framework that organizations consult, yet few actually use for attestation.

The world of privacy assurance looks much the way the financial landscape looked when the Sarbanes-Oxley Act was first introduced. Initially, many public companies thought it would be easy to meet the requirements. Many suffered a rude awakening when they realized that a substantial portion of their financial controls were insufficient for their auditors. Companies found themselves having to invest significant resources into improving their internal controls.

SOC 2 represents the future for assuring privacy management, but it may take organizations some time to improve their controls to meet the rigors the audit criteria require. However, as the risk associated with personal information continues to escalate, the trend for independent assurance in the privacy sphere will continue to grow.
The need for a standard privacy compliance framework grows

Automatic Data Processing (ADP) is one of the world’s largest providers of business outsourcing solutions. Every day, we work with clients to manage their human resources, payroll, tax and benefits administration, among other businesses. Our business success depends on the efficient and safe handling of sensitive information. As a result, our privacy program and our security program are closely entwined – not only conceptually, but organizationally. Our privacy program is principally focused on: 1) security; 2) compliance; and 3) business enablement. Our privacy team forms part of our security organization, but it also reports into legal, given the importance of compliance within the program.

In the face of ever-changing and quickly evolving threats, technology and regulations, ADP has implemented a governance, risk and compliance (GRC) approach that enables our privacy program to remain agile in responding globally to constantly changing regulations, threats and technologies, as well as the evolving needs of our clients.

As a global service provider, one of the challenges we have, and see continuing into 2013, is a lack of consistency in the development and application of regulations globally. We are seeing both convergence and divergence in the regulatory space. Multinational clients are struggling to address disparate regulatory developments in multiple jurisdictions. Regulations and standards vary, not only from region to region, but also from one industry to another. As such, each organization is trying to establish its own baseline of requirements it places on its vendors. Some requirements are geared toward regulators who are raising the bar. Others are responding to past breaches. Still others are seeking to meet their own internal standards. Although we are standardizing our security and privacy controls enterprise wide, we often are called to respond on an individual organizational basis. No one set of policies, standards or controls meets the needs of all of our clients – or even a segment of our clients. This creates inefficiencies in our privacy and security management programs.

As the proliferation and complexity of regulations grows globally, so too does the need for a solution in the form of a standard framework or approach that clients can use to establish their baselines and vendors can use to develop consistent, streamlined and effective privacy management programs. SOC 2 reporting may be one such solution. However, much like the discussions occurring around harmonizing regulations globally, consensus around a framework or reporting standards will take time to achieve.
The changing role of the privacy officer

The role of the privacy officer continues to evolve. Where it was once leading practice to have a privacy officer, today, it is common business practice. In fact, in many regulatory jurisdictions, the position is mandatory.

The need for a privacy officer (the title is different across industries and jurisdictions) is mentioned in existing privacy regulations such as HIPAA in the US, as well as proposed privacy regulations such as the EU privacy regulation, the consent decrees by the FTC and guidance provided by data protection authorities in Canada.

We see two different types of developments in the privacy officer role. In the large multinationals and the rapidly-changing, information-intensive organizations, the role of the privacy officer has evolved significantly. As the role of the privacy officer has matured, these privacy officers find that they need to be more than luminaries or policy-setters. They also need to deal with ongoing business issues and oversee a growing network of privacy professionals in their organizations to which they may only have a dotted reporting relationship.

However, another class of privacy officers has emerged. These are the privacy officers that are managing programs that experience small changes over time. Once their privacy program is in place and operating effectively, their organizations move from low maturity to the moderately mature level where maintenance, breach handling and program updates are the main functions. In this context, the need for a “Chief Privacy Officer (CPO)” disappears. Once a career destination, privacy responsibilities in slowly evolving or medium-size organizations that are not data intensive are increasingly held by low- to mid-level managers for whom privacy is one of many positions along the career path.

In fact, the number of privacy officers in mid-level management positions is increasing even in large and leading multinationals. This divergence in the privacy officer position is not negative. In fact, when structured appropriately, it should align well to the needs of the organizations. Not every organization needs a “super CPO.”

The maturation of the privacy officer has a direct effect on the maturity of privacy management as a whole. When a privacy manager moves on within the organization, that person takes that knowledge with them. This not only creates a fluency in privacy across other parts of the organizations, but also makes privacy everyone’s responsibility. In this way, privacy becomes imbedded into the fabric of the organization. It is as integral to an organization as HR, procurement or internal audit.

Privacy maturity is no longer measured by the sophistication of solutions. Rather, it is measured in terms of consistency and consideration among a wide range of business demands. For some organizations, it is the ability to maintain a large network of professionals, often spanning borders and continents, to maintain a level of attention necessary to be effective in day-to-day operations. For others, it is maintaining a consistent level of compliance, not more but not less.
Daniela Fabian Masoch
Global Head Data Privacy, Novartis International AG
Basel, Switzerland

Standards for data privacy need to be both strong and flexible

Our approach to managing data privacy within the Novartis Group requires Novartis affiliates to take ownership and be accountable for local compliance with data privacy laws and regulations and for implementing our global privacy program.

Our privacy program is designed to support Novartis affiliates worldwide to comply with privacy requirements and to govern global projects and international data flows. While the Novartis Privacy Policy framework establishes a common standard on the appropriate protection of personal information within the Novartis Group, it is also important to keep some flexibility to accommodate national requirements. For example, standard operating procedures that companies must follow may vary from country to country, as could the requirements for setting up awareness and training programs, ensuring that our privacy standards are implemented and monitored on an ongoing basis.

A critical component for an effective implementation of our privacy program and BCR is the establishment of a global privacy network, including privacy officers at various levels of the organization — within divisions, countries, functions and affiliates throughout the Novartis Group. Data Privacy Officers are responsible for ensuring compliance with data privacy requirements and for embedding the appropriate management of data privacy into processes and systems. Regular assessments of privacy controls indicate the maturity level at company level and help to identify existing gaps in the implementation of the program and potential risks for our organization.

Our approach to data privacy has proven to be effective. However, as regulations in the EU and elsewhere evolve, we need to keep our approach to data protection dynamic so that we can remain nimble and responsive to a constantly changing privacy environment.
Many organizations see themselves as moderately mature when it comes to privacy

In Ernst & Young’s 2012 Global Information Security Survey: fighting to close the gap, we asked survey participants to rate the maturity of their privacy function and several information security functions within their organizations in terms of maturity on a scale from nonexistent to very mature. Only 7% of respondents view their organizations as very mature when it comes to privacy. A near majority – 41% – see themselves as moderately mature. They’ve made progress, but know that they can do more when it comes to privacy protection.

What is the approximate percentage of total spend on the following information security functional areas in your organization?

- Security operations: 18%
- Business continuity management and disaster recovery: 15%
- Identity and access management: 7%
- Compliance management and support: 6%
- Security governance and management: 6%
- Security incident and event management: 6%
- Security testing: 5%
- Threat and vulnerability management: 5%
- Data integrity-related activities: 5%
- Security awareness, training and communication: 5%
- Privacy: 3%
- Other: 4%
Technology offers opportunity, but includes a steep learning curve

The technology evolution is something of a double-edged sword. For organizations and consumers alike, technology opens the doors to a world of opportunities. But there are risks. Consumer demand is driving the need for digital transformation – a fundamental shift in customer relationships, business models and value chains. Some organizations are using technology to introduce new products or services, improve efficiency and collect more information about their customers than they currently need or know how to use. It is the latter that creates the biggest privacy risk.

To better manage that risk, many organizations have implemented monitoring technology. However, this raises new issues as the monitoring technology tends to shine a spotlight on privacy failures that are often costly to correct. Internally, the BYOD phenomenon is creating challenges between the need to secure the organization’s data without compromising employee privacy.
Digital transformation demands accountability

Digital is widely seen as the most transformative business force since mass production. It is affecting how almost every industry interacts with its customers and enables organizations to create a seamless, unified experience across channels, processes and geographies.

By using the internet, social media, mobile and real-time 360° analytics, organizations can enhance customer relationships, increase top-line growth, streamline operations, empower talent and use innovation to reinvent competitive solutions and business models.

The app revolution is a prime example. Almost every organization wants an app to drive more consumer traffic. Even organizations that are relatively immature in technological maturity understand the value an app can provide, from increasing their appeal in the market to collecting reams of consumer information, whether they need it or not. In fact, many organizations have little or no idea what to do with all the information they collect. The challenge this creates is that where leading edge technology organizations have been plugged into the privacy debate for some time, organizations slow to join the digital party often know very little about privacy risks or management and have no resources on staff to either identify or address them. As a result, we are seeing an increasing number of “rookie” mistakes impacting strong global brands as they step into the digital world. Their learning curve is steep. They will need to determine the requirements, establish a privacy program and become accountable for their digital transformation.
When creating technology standards, put privacy first

Mobile is a complex, global ecosystem with many contributing players in different roles and from different regions. Often, one player acts in multiple roles simultaneously. For example, a device manufacturer also may be the operating system (OS) provider, run its own application distribution channels and publish its own applications. Alternatively, these roles could all be performed independently by different parties.

At the same time, vast numbers of individuals and companies are finding new ways to participate in the world as users and creators of applications as well as processors and controllers of personal data. Advertising and analytics providers create new opportunities for application developers to monetize and develop their applications.

The dynamics of the ecosystem forms a puzzle where all contributors must provide pieces if the privacy challenge is to be solved. One small mishap by one of the contributing players can cause significant privacy issues to individuals. No one player can act as the ultimate one-stop shop to manage privacy across the ecosystem. Each player needs to do its part to ensure that there is no hidden, uncontrolled, excessive or unsecured collection and use of personal data.

Accordingly, OS providers must make hardware capabilities, such as various sensors, exposed by device manufacturers, accessible to developers in a controlled and privacy-friendly manner. OS providers need to ensure that access to information, such as contacts or content on the OS is controlled and transparent to users. As well, application stores should impose privacy requirements on developers. This important step improves privacy awareness among the developer community. Users also need to be made aware of the privacy impacts of features of OS, hardware and applications and there should be ways for users to report malicious practices. Mainstream application stores have already developed privacy requirements with which developers must comply before an application can be published.

Current privacy regulatory regimes may not be sufficient to address privacy issues in highly interdependent ecosystems, where data is flowing across regions and continents, and where different players are subject to different laws and users can access the services anywhere. Often some of the activities of some of the key players, such as OS providers and application stores appear not to be covered by traditional data protection definitions, such as a data controller. In fact, for many services, users themselves may act as data controller.

Nokia understands the importance of technology standards to sustain the future of the mobile ecosystem. Accordingly, we have shared with a number of technology standards bodies a model to facilitate the transformation of privacy principles into actual privacy considerations in technology standards. Our goal is to enshrine privacy in the standards development process, so that each party implementing the standard is informed and can adhere to these expectations.

Henri Kujala
Privacy officer, Location & Commerce, Nokia
Berlin, Germany
Monitoring uncovers privacy failures

The elements of any program include policies, controls and monitoring. For years, privacy programs had robust policies and average controls, but very little monitoring. Many organizations didn’t have the tools to monitor privacy given the vast amounts of data and processes involved.

In Ernst & Young’s Privacy trends 2012 – the case for growing accountability, we discussed the rise in organizations’ awareness of the need to monitor how personal information is managed. We also talked about the increasing implementation of DLP tools tracking for sharing data, tools to track network folders and applications that monitor use patterns on databases.

We indicated that in 2012 we expected that organizations would increase their investment in privacy monitoring tools to demonstrate greater accountability by monitoring the personally identifiable information they collect. However, once implemented, the new privacy monitoring tools demonstrated more than accountability. It also uncovered more evidence of privacy failures.

These failures reveal the importance of implementing these tools and the need for accountability. The challenge organizations now face is the significant cost for remediation. In fact, many of the issues cannot simply be addressed with stop-gap measures. Rather, they require a substantial investment in new technologies. Many organizations still rely on systems that were developed in the 1990s, when limiting access to sensitive information and encryption solutions were on few organizations’ radar. As such, many organizations would have to undertake a complete IT transformation to address the privacy issues monitoring tools are flagging. With many organizations still feeling the effects of a sluggish economy, few are ready to make the required investment. In fact, we anticipate that privacy budgets (and the security budgets supporting the protection of personal information) will stay largely the same as in 2012.

In Ernst & Young’s 2012 Global Information Security Survey, Fighting to close the gap, 70% of respondents indicate that they planned on spending relatively the same amount over the next year as they did in the previous year on privacy. That number may have to change to address the increased investment required to improve privacy controls.
Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the next year for the following activities? Select only those areas where you have planned expenditure.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Spend more</th>
<th>Spend the same</th>
<th>Spend less</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing new technologies</td>
<td>55%</td>
<td>39%</td>
<td>6%</td>
</tr>
<tr>
<td>Business continuity/disaster recovery</td>
<td>47%</td>
<td>46%</td>
<td>7%</td>
</tr>
<tr>
<td>Data leakage/date loss prevention technologies and processes</td>
<td>45%</td>
<td>49%</td>
<td>6%</td>
</tr>
<tr>
<td>Identity and access management technologies and processes</td>
<td>42%</td>
<td>52%</td>
<td>6%</td>
</tr>
<tr>
<td>Security awareness and training</td>
<td>38%</td>
<td>56%</td>
<td>6%</td>
</tr>
<tr>
<td>Information security risk management</td>
<td>36%</td>
<td>59%</td>
<td>5%</td>
</tr>
<tr>
<td>Security testing</td>
<td>34%</td>
<td>58%</td>
<td>8%</td>
</tr>
<tr>
<td>Security operations</td>
<td>34%</td>
<td>59%</td>
<td>7%</td>
</tr>
<tr>
<td>Security governance and management</td>
<td>32%</td>
<td>62%</td>
<td>6%</td>
</tr>
<tr>
<td>Threat and vulnerability management technologies and processes</td>
<td>31%</td>
<td>64%</td>
<td>5%</td>
</tr>
<tr>
<td>Compliance monitoring</td>
<td>31%</td>
<td>64%</td>
<td>5%</td>
</tr>
<tr>
<td>Security incident and event management</td>
<td>30%</td>
<td>64%</td>
<td>6%</td>
</tr>
<tr>
<td>Implementing security standards</td>
<td>28%</td>
<td>63%</td>
<td>9%</td>
</tr>
<tr>
<td>Incident response capabilities</td>
<td>27%</td>
<td>67%</td>
<td>6%</td>
</tr>
<tr>
<td>Information security transformation</td>
<td>26%</td>
<td>61%</td>
<td>13%</td>
</tr>
<tr>
<td>Secure development processes</td>
<td>25%</td>
<td>66%</td>
<td>9%</td>
</tr>
<tr>
<td>Privacy</td>
<td>24%</td>
<td>70%</td>
<td>6%</td>
</tr>
<tr>
<td>Recruiting security resources</td>
<td>22%</td>
<td>63%</td>
<td>15%</td>
</tr>
<tr>
<td>Forensics/fraud support</td>
<td>18%</td>
<td>75%</td>
<td>7%</td>
</tr>
<tr>
<td>Offshoring/outsourcing security activities</td>
<td>17%</td>
<td>67%</td>
<td>16%</td>
</tr>
</tbody>
</table>

Select only those areas where you have planned expenditure.
More than ever before we are seeing a transition to a fully mobile workforce. Some organizations have closed entire brick and mortar offices in a shift to a fully virtual workplace model. These organizations are managing the risks with administrative checks and balances. But is it enough?

Less than five years ago, the focus was on protecting the perimeter. More recently, as the perimeter gave way to a borderless world, organizations shifted their focus to protecting the data. Now, with the rise of the mobile workforce, organizations may have to shift their focus again. Unable to control the data, organizations will need to determine who can be trusted with the data.

The proliferation of BYOD — whether inside the more traditional workplace or as part of the new virtual mobile workplace model — has generated both efficiencies and true concerns. Many of the more popular mobile devices don’t have sufficient built-in controls to meet security expectations. As well, employees are able to upgrade their mobile device themselves — without having to go through the corporate IT department. And then there is the privacy challenge. For security management purposes, organizations want to use monitoring tools to keep an eye on their data. However, in the process, the tools also end up monitoring an employee’s personal information.

An ideal solution for resolving some of the privacy issues associated with dual use devices is to consider partitioning the device. The device would have two different desktops — one for work and one for personal — located on two separate components of the device’s hard drive. Unfortunately, the size of the mobile device’s hard drive and the power of its battery does not yet support this solution.

Another option available that may be more feasible is the use of a guest network that is separate from the main network. This allows employees to use their personal device to gain access to the web directly, perhaps even through a work-only email account. Organizations also may want to consider using third-party services or their own coding to create “sandboxes” where company data and company-issued applications reside, effectively separating them from any interaction with personal data, applications or online services. These options serve the dual purpose of protecting the organization’s data from unauthorized access as well as the employee’s personal information from being monitored by the organization.
Who owns the data?

As mobile devices become central to our personal lives and crucial to work productivity, discerning who owns the data that lives on our mobile devices has become incredibly challenging. Policies and practices that were reasonable when a mobile device was clearly the property of the company, with only minor personal use allowed, are less reasonable in a world where the line between work and personal is indistinguishable. Employees are expected to be available 24 hours a day, work time may include typing an email at midnight while on vacation; and personal time may include doing an online search for just the right birthday gift on an employer-issued tablet in between meetings in the office. This is an area where law and compliance practice are being challenged to adapt.

We need solutions that are both convenient and effective in segregating work and personal information. Technologies that can compartmentalize devices are helpful, but organizations also need to adopt a more flexible and balanced view of what constitutes personal versus work.

To date, with only a few court cases departing from the norm, employers have been able to rely on clear policies that notify employees that their equipment may be monitored and that devices may be wiped if the employee is terminated. But it is increasingly likely that if a company takes steps to wipe personal data from a device is owned by the employee, the courts will apply their scrutiny to protect the employee. Consider the junior assistant who checks email on the weekend at his boss’s insistence, and who has minimal access to sensitive data, but who loses the video of his child’s first steps when his device is wiped after he is laid off just before Christmas.

In a highly regulated environment, or an environment that deals with highly confidential data, the organization’s actions may hold up under that scrutiny. However, in cases where the information access is more general, companies will need to have a more accommodating and flexible policy in place.

Looking more broadly at privacy issues in the mobile world, it is clear that the rapid pace of change is forcing new thinking about privacy. The digital evolution has created a fragmented ecosystem comprising of carriers, platforms, content creators and distributors, devices, apps and analytics – all of whom have some role to play in how privacy is managed, but none of whom has sole responsibility or accountability. This fragmentation will continue to stress the boundaries of privacy. And yet, despite these concerns, the ecosystem will continue to innovate to feed a voracious consumer appetite. Amid the chaos and innovation this digital evolution brings, privacy cannot be forgotten. Legislation and regulation will have to keep chasing the trends, ensuring that policy, compliance and legal structures for the privacy of personal information are no more than one step behind.
Regulators continue to face an uphill climb when it comes to protecting privacy. An ongoing focus on specific privacy requirements rather than sweeping regulations has some organizations responding tactically rather than strategically, while others look for the loopholes. There is no doubt that regulators have increasingly complex questions to answer. Consider, for example, the balance needed between the right to be forgotten and the right of others to remember, which hinges greatly on freedom of expression. Rapid advances in technology have directly impacted our social norms. Privacy programs need to be able to bridge these gaps – faithfully adhering to regulatory requirements while practically addressing the challenges of their organizations and stakeholders. To achieve this balance, privacy programs need to form an integral part of an organization’s decision-making process rather than a simple check-the-box compliance exercise that only seeks to meet minimum regulatory requirements.

The ideal solution would be for organizations to use Privacy by Design (PbD) or Privacy by ReDesign to embed privacy into new system implementations or IT transformation initiatives. However, although PbD has been widely accepted as a concept, it has yet to gain traction with organizations in terms of implementation.
Privacy matures from compliance to accountability

The EU, long seen as setting the standard for other countries to follow when it comes to data protection, is raising the bar again. Mere months after the cookie law came into force, the EU is looking to update its Data Protection Directive to harmonize the data protection laws across the EU Member States and address evolving technology advancements. The proposed legislation will apply to anyone processing data within the EU, including any organization outside of Europe that offers goods and services to EU residents. As well, for the first time, data processors will share in both the responsibility and liability related to complying with the new laws.

Under the proposed EU regulations, organizations will be required to prove that they undertake regular data protection audits and privacy impact assessments. Organizations with more than 250 employees will also have to hire a data protection officer. These new EU requirements don’t ask organizations to be accountable — they are demanding it. Any organization wanting to do business in the EU or with its citizens will need to review and improve, where necessary, data protection and privacy programs to ensure compliance.

To achieve such compliance, many organizations are pursuing BCR status. As we discussed in Privacy trends 2012: the case for growing accountability, BCR comprises a set of internal guidelines, similar to a Code of Conduct, that establishes policies for transferring personal information within the organization and across international boundaries. BCR status is challenging to achieve, but early adopters, such as GE and Philips, are already yielding the benefits. Over the next several years we expect an increasing number of multinational organizations to pursue BCR status.
Just as the EU seeks to improve its data protection regulations, the FTC is busy taking similar action. In 2012, the FTC issued a final report that establishes leading practices for protecting consumer privacy and giving consumers greater control over collection of their personal information. The report also recommends that the U.S. Congress introduce legislation at a federal level that would address privacy protection, data breach notification and data brokering. To aid compliance with these leading practices, the final report recommends that businesses: adopt PbD; simplify choice for businesses and consumers about what information is shared and with whom; and provide greater transparency around the collection and use of consumer data.5

In addition to these recommendations, the FTC has pursued legal action against several social media and internet services companies for violating their own commitments to privacy. These consent decrees also emphasized the importance of establishing the tenets of an effective privacy program in a manner that addresses program changes, compliance with requirements and privacy risk management.

In the Asia-Pacific region, the Asia-Pacific Economic Cooperation (APEC) Electronic Commerce Steering Group has developed a voluntary, certification-based system. Known as the Cross-Border Privacy Rules (CBPR) System, it enables organizations doing business in the 21 participating APEC countries, which includes the US, to establish a consistent set of data privacy practices.6

In a July 2012 APEC news release, Lourdes Yaptinchay, Chair of the Electronic Commerce Steering Group, was quoted as saying that “the goal of the system is to enhance electronic commerce, facilitate trade and economic growth, and strengthen consumer privacy protections across the Asia-Pacific region, thereby promoting regional economic integration.”7 Added Acting Secretary of Commerce and Deputy Secretary of Commerce Rebecca Blank: “This system will enable participating companies in the United States and other APEC member economies to more efficiently exchange data in a secure manner and will enhance consumer data privacy by establishing a consistent level of protection and accountability in the APEC region.”8

As regulators around the world seek to bolster requirements for privacy program accountability, the differences among regulations continues to diminish. This is good news for organizations seeking to develop encompassing privacy programs that achieve accountability, governance and monitoring objectives. This comprehensive approach addresses a wide range of compliance requirements rather than focusing privacy efforts on specific, jurisdictional regulations.

---

7 Ibid.
8 Ibid.
The business case for BCR

BCR is a set of internal guidelines or rules adopted by multinational organizations that defines global policies for transferring personal data within the same corporate group of entities, but across international boundaries — and particularly into countries that may not provide an adequate level of protection. Although momentum for BCR status has been building since its introduction by the EU in 2003, it is now reaching a tipping point, where it is becoming the obvious solution for many organizations, rather than simply another good option.

There are many reasons the time is right to adopt BCR status:

- With more than 40 BCR status applications already approved within the mutual recognition procedure, DPAs have significantly improved their cooperation. Accordingly, the review of BCR applications is now considerably shorter. It is possible to get an approval from the Leading Authority within eight months.
- BCR applications benefit from a strong support at national data protection authorities levels and at the EU Commission level. Viviane Reding, Vice-President of the European Commission, has presented BCR status as a toll to operate on a global scale, enabling “companies to transfer their data freely and safely — anywhere and in conformity with the law … potentially covering all kinds of business models: from a paper-based filing system to an intricate internal organization or the most complex cloud computing system.”
- BCR status is a very good data protection compliance package that enables consistency of data protection practices within a group.
- BCR status can serve as a marketing tool with clients because of the approval from public authorities.
- Since June 2012, data processing service providers have been able to apply for BCR status. This is a unique opportunity for service providers to offer trust and security to their clients interested in cloud computing solutions.

In the next five years, multinational organizations that have not sought BCR status will be viewed with suspicion — not a great place to be in a rapidly evolving and highly competitive global market.

---

Breach notification becomes a strategic imperative

In many jurisdictions around the world, breach notification regulations take a tactical rather than a strategic approach, focusing primarily on complying with the notification requirements rather than the risks that brought about the breach.

As the pace of technological evolution accelerates, such a tactical approach increasingly leaves individuals vulnerable to aggressive organizations seeking to create competitive advantage, or criminal enterprises looking to profit from unauthorized access to personally identifiable information.

In the US, Massachusetts has established policies that force organizations to take a more strategic approach to breach notification. In 2008, Massachusetts was one of 45 states to implement data breach notification requirements as part of protection legislation that governed the acquisition, management and disposal of personally identifiable information for its residents. In 2010, the state required that residents and the Attorney General (AG) be notified of any unauthorized access or use of the information an organization collects. Included in the breach notification regulation was a requirement by organizations that collect information about a resident of Massachusetts to develop a written information security program (WISP). Although mandatory, no one in the Massachusetts AG’s office ever demanded to see a copy of an organization’s WISP — until recently. The AG’s office is now requiring any organization that experiences a breach to produce a copy of their WISP. This requirement applies not only to organizations doing business in Massachusetts, but any organization that collects the personal information of a Massachusetts resident. The sweeping domestic, and potentially international, implications of the enforcement of this requirement means that organizations will have to think and act more strategically about breach notification.

Countries with a more federally comprehensive privacy approach, such as Canada, Australia and the EU, are beefing up their regulations around breach notification. Improved breach requirements in these countries further underscores the evolving role of the privacy regulator. As discussed earlier in this report, many privacy regulators increasingly find that collaboration and discussion with organizations under their jurisdiction is proving effective.

In the spirit of cooperation, leading organizations are already seeking to proactively prepare for issues before they arise. For example, some organizations are developing incident management plans that anticipate what may go wrong, so that if something does go wrong, they can react immediately. This includes having standing contracts with vendors that can provide call center, triage processing, communications and credit monitoring as soon as they are given a “go” signal. In fact, many vendors providing breach response services allow companies to establish master service agreements (MSAs) on a fee-for-service basis so that companies only incur costs when the MSA is enacted. Organizations that do not have MSAs in place lose valuable time when an incident does occur. Because MSAs are often sensitive in nature and have multiple requirements, there can be a lengthy legal review and negotiation process to ensure both parties are satisfied. Once the MSAs are in place, organizations need to constantly review their effectiveness, particularly after a breach to ensure an appropriate level of scope, clearly articulated roles and responsibilities, and most importantly, whether red flags are being escalated from the front lines to the right people within the organization.
Both sides of the Atlantic reconsider privacy

For almost two decades, a myth has been circulating that the EU’s approach to privacy and data protection is “stricter” than the sectorial approach the US employs. In my experience, both as a privacy lawyer and as Chief Privacy Officer for the U.S. Department of Homeland Security, the two regions’ approaches have more in common than the myth would suggest.

Both approaches to privacy are grounded in the concept of fair information practice principles (FIPPs). First proposed by a US privacy commission in the early 1970s, the FIPPs are internationally recognized, having been articulated and echoed in the US the European Union Directive 95/46/EC and the Asia-Pacific Economic Cooperation Privacy Framework.

In contrast to the United States’ sectorial approach to privacy protections and legislation, the EU frequently adopts an umbrella approach, in which broad standards or principles are easily promulgated, but often require the creation of exceptions or derogations to apply the standards. The US can be more agile and specific in its legislation, but may appear more reactive to high-profile privacy violations.

There has been significant recent activity on both sides of the Atlantic on fine-tuning privacy regimes. The EU has released a draft Data Protection Regulation to update its 1995 Directive; the Obama Administration has supported a “consumer bill of rights,” self-regulatory initiatives and potentially privacy legislation. The EU’s process will take years, and the end result will likely not look like the current product. Similarly, the legislation process in the US may take a long time, but with President Obama’s re-election, privacy legislation may receive renewed attention in the next Congress.

One thing that is certain — regardless of the result of both privacy reconsiderations, the FIPPs are still very relevant to the privacy process. In the end, the EU approach will probably be broader with a series of “derogations” — exceptions — while the US approach will be more narrowly tailored, trying to address some discrete issues. With that said, there will likely more additional international harmonization of privacy harm analysis as the topic of privacy in the 21st century evolves.
Privacy by Design (PbD) needs regulation to gain traction

It has been more than two years since privacy commissioners gathered at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem, Israel to discuss and endorse the concept of PbD. In that time, regulators around the world have lauded PbD as a standard that all organizations should adopt.

Yet few regulators or government lawmakers have mandated its use through regulation or legislation and few organizations have sought to adopt it of their own accord. For PbD to gain traction with organizations, it needs that regulated mandate.

Until PbD becomes a regulated standard, organizations will continue to operate upon the principles established during the early days of the internet. That is, to take advantage of the free online services an organization provides, consumers must be willing to give up some of their personally identifiable information and privacy. However, as technology evolves, consumers are giving up more and more of their personally identifiable information, often without even knowing it.

As such, it is increasingly incumbent upon organizations to take greater care and responsibility for the data they are collecting. This includes not only the organizations doing the collecting directly, such as the application and software companies, but also all of the corollary organizations, such as infrastructure companies and device or operating system manufacturers. Every organization that touches consumer data should be accountable for managing the privacy of that data. PbD would enforce that accountability.
Changes to the role of the European DPA under proposed changes to the EU Directive on data protection

On 25 January 2012, the EU Commission proposed an ambitious and comprehensive reform of the 1995 data protection rules. The proposal is building on the principles of the previous directive but ensures a higher level of protection for the users, particularly in the online world.

One of the key changes in the reform is the setting up of the “one-stop shop” and consistency mechanism. Companies will have to deal with a single DPA in the EU country where they have their main establishment.

The proposal ensures consistency among supervisory authorities by two mechanisms:

1. It sets out a cooperation and mutual assistance regime, in cases where more than one DPA has an interest in supervision. This will be the case for instance, when data subjects from more than one Member States have lodged complaints.

2. It creates a consistency mechanism through the European Data Protection Board (EDPB) that has the competence to deliver opinions on cross-border matters. The EDPB’s opinions, however, will not be binding for the lead DPA.

The EU Commission’s proposal is currently under scrutiny by the European Parliament. As the draftsperson of the Committee on Legal Affairs, I am very much in favor of the one-stop shop mechanism that will boost the EU single market, reduce red tape and administrative costs for companies and facilitate the free flow of data in Europe.

However, more must be done. A clearer definition of the main establishment is needed and the same criteria should apply to both controllers and processors. The cooperation and mutual assistance regime should be strengthened and in the consistency mechanism we must find the right balance between the powers of the EU Commission and those of the EDPB and national DPAs.
Conclusion

Our ever-deepening foray into digital is transforming businesses in ways we have not seen since the onset of the industrial revolution. It is opening doors to a world of opportunity – and tremendous risk to privacy. Privacy regulators are doing everything they can to keep up, but as the technology’s evolution accelerates its pace, regulators continue to fall behind.

Regulation remains a useful tool to improve privacy protection. However, privacy regulators will have to make a fundamental shift from compliance officers to strategic advisors. They will have to work with organizations to facilitate stronger decision-making when it comes to privacy management.

On the business side, organizations need to be more accountable. If organizations are unwilling to integrate privacy into IT transformation initiatives, as PbD suggests, regulators should be looking to mandate it.

The digital ecosystem is still young and many organizations have yet to fully grasp not only the opportunities, but also the responsibilities that come with operating in a digital environment. Organizations and regulators alike need to appreciate the governance role they must play in safeguarding personal information and serving as examples that the rest of society can follow.
About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young’s Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 25,000 Advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential, you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

The views of third parties set out in this publication are not necessarily the views of the global Ernst & Young organization or its member firms. Moreover, they should be seen in the context of the time they were made.

© 2013 EYGM Limited.
All Rights Reserved.

Contact details of our Risk leaders

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

EMEIA

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

Asia-Pacific

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

Japan

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