

Insights on IT risk

January 2011

Privacy trends 2011

Challenges to privacy programs in
a borderless world

Introduction

For years, the fixed boundaries of an office's four walls have, for the most part, enabled companies to manage the privacy of the data they keep. But in an era of anytime, anywhere access to information, these traditional boundaries are disappearing. It is a new world – technology-driven, ever-connected, globally extended and well beyond the scope of conventional privacy protection approaches.

In *Borderless security: Ernst & Young's 2010 Global Information Security Survey*, 81% of executives interviewed indicate that managing privacy and protecting personal data is very important or important to their organization. And no wonder: highly publicized incidents of data leaks or identity theft pose huge brand and reputation risks for businesses – a concern survey participants ranked even higher than privacy protection (84%).

As a result, executives are investing more money to protect the privacy of personal information – to respond to ever-increasing government regulation and enforcement and to stem the rising tide of risk. But are they spending it in the right places? With parts of the global economy still limping toward recovery, executives continue to ask this burning question as they search for the right balance between spending on privacy protection and taking appropriate levels of risk to manage costs.

One thing is certain: technological advances will only continue to accelerate, and organizations need to be ready. While governments are stepping up regulation and enforcement, privacy protection lacks international cohesion. It is a compliance patchwork with levels of consistency that vary from country to country and industry to industry.

Organizations do not have time to wait for global regulatory bodies to reach consensus. They need to take action now to proactively develop and implement enterprise-wide privacy protection strategies that match the organization's risk profile. By looking upon privacy strategies to drive regulation rather than the other way around, companies can meet today's needs and also anticipate tomorrow's challenges.





Regulations, laws and enforcement

Historically, enforcement of information protection legislation has lacked teeth. Today's regulators plan on changing that by expanding their reach and imposing tougher penalties. The US Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (the HITECH Act) is one such example. Under the HITECH Act, state attorneys general can investigate and take action against organizations for failing to secure protected health information. The year 2011 will bring additional clarity and detail regarding the provisions of regulations that address the online environment in many countries.

In the EU, the European Commission is in the process of updating the 1995 EU Data Protection Directive. Plans for strengthening enforcement include providing data protection authorities with the ability to investigate and sue organizations that do not comply,

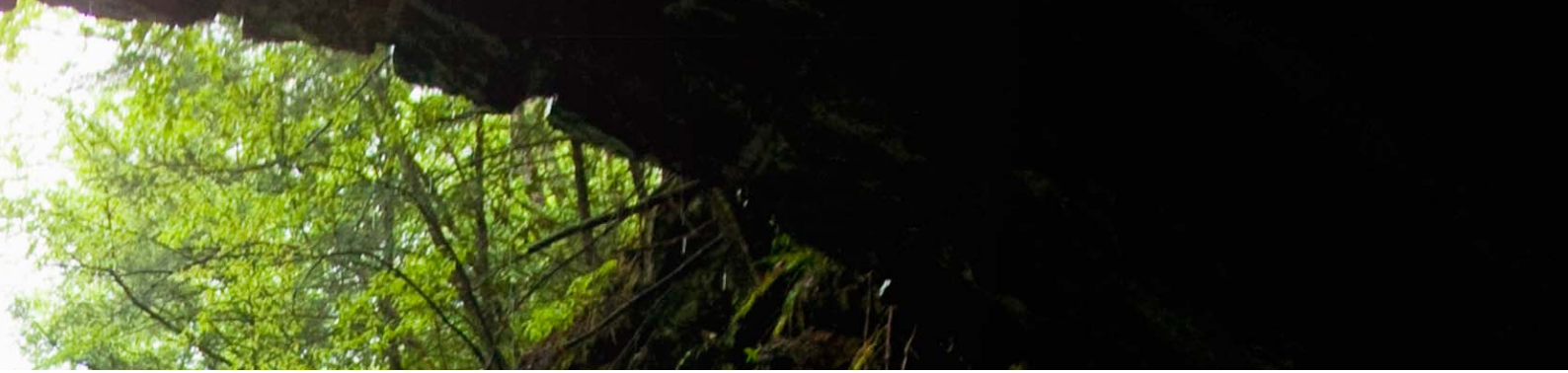
and for improving cooperation and coordination among member nations. In advance of the release of new regulations under the EU Data Protection Directive, several EU countries have been busy intensifying existing enforcement policies.

This year, Mexico, a significant outsourcing destination, joined about 50 other countries in adopting a broad privacy regulation that focuses on the private sector. The Federal Law on the Protection of Personal Data Held by Private Parties will impact many large US-based companies operating in Mexico.

Similarly, the EU found the data protection laws of Israel, an important outsourcing destination for the EU, provided an "adequate level of data protection" relative to the EU Data Protection Directive. This designation means that data between the EU and Israel can now move much more freely.

Questions to consider

- ▶ Have you stayed current with the regulations impacting your particular industry and the personal information your organization processes?
- ▶ Have you reviewed whether regulations have changed in the jurisdiction(s) where you operate?
- ▶ Have you assessed your compliance with applicable regulations recently?



Additional breach notification requirements

Breach notification goes beyond regulatory compliance. Its focus is on transparency, which has fundamentally altered how organizations approach privacy and data protection. Breach notification failures have resulted in reputational damage and attracted the attention of regulators. In the US, most states have adopted breach notification requirements that commonly address sensitive and financial identifiers. The HITECH Act introduced similar requirements for protected health information. And, while the US has been an early adopter of breach notification requirements, these types of requirements are increasingly taking hold in other places around the world.

In Canada, an amendment to the Personal Information Protection and Electronic Documents Act (PIPEDA) is making its way through the regulatory process and includes breach notification obligations. In the EU, a breach notification regulation for the telecommunications industry will come into effect in 2011. In addition, the EU's review of the Data Protection Directive is expected to result in notification requirements for all EU member countries. Some EU countries are adding their own breach notification provisions. In the UK, for example, regulators are working on a law that will force organizations to publicly acknowledge any data breaches to regulators and to inform those affected.

In Asia, Japan is leading the way with breach notification requirements that have been in place for several years. Much like in the US, the expense associated with such breaches can lead to a significant number of direct and indirect expenses for organizations operating there.

Breach notification cannot be discussed without raising the concern of the "insider threat." Individuals who are authorized to access and use information are increasingly found at the center of high-profile incidents. Such misuse of information may be due either to lack of awareness or to malicious intent. Training and awareness are key to addressing the unintended disclosure of information. Technical controls, such as tools for monitoring information traffic, can be of great help when addressing more malicious cases.

Data loss prevention (DLP) tools can also help by monitoring unintentional or intentional data leaks from within the organization. In 2011, we will continue to see the popularity of these tools increase as organizations look for a technical control to limit their breach exposure. However, it takes more than the purchase of a DLP tool to achieve effective monitoring of personal information to prevent loss. Adopting these tools requires appropriate consideration of the policy that will guide the extent of the tool's implementation (e.g., to stop a possible leak or just report it for a later investigation) as well as cross-functional leadership support and the necessary staffing to implement it.

Regardless of jurisdiction, organizations have to adapt to new requirements regarding breach notification. Whatever their reliance is on technical controls for combating the loss of personal information, organizations need to have effective programs in place to detect, address and resolve breaches. They also need to have open and transparent communication plans to inform those affected when their data is compromised.

Questions to consider

- ▶ Have you developed and implemented an incident response plan for handling breaches of personal information?
- ▶ Have you identified the relevant breach notification requirements in your industry and jurisdiction(s) of operation?
- ▶ Have you looked into the adoption of a DLP tool or using DLP services to monitor your organization's network for possible loss of personal information?



Governance, risk and compliance (GRC) initiatives

Organizations have been investing heavily in GRC initiatives for years. But in the wake of the worst economic crisis since the Great Depression, some reports are suggesting that financial institutions alone were spending up to US\$100 billion on mitigating risks in 2010.

In an Ernst & Young survey of 567 organizations across Europe, the Middle East, India and Africa in 2010,¹ 69% of participants indicate that they are highly reliant on their GRC activities as a safeguard against failure. And yet, 67% of respondents suggest that more work is needed to enhance their GRC functions.

From a technology perspective, the market for GRC tools continues to develop and offer risk management solutions, and more specifically, solutions for managing privacy. In 2009 and 2010, technology heavyweights entered the GRC market. However, few vendors offer a full GRC solution, and even fewer offer sophisticated or easy to use modules for privacy management. This is partly due to the complex nature of the requirements and partly due to the difficulty involved in automating key privacy-related updates. But while the giant GRC technology firms may still be finding their feet when it comes to privacy management, some boutique software companies, seeing a gap to fill, are entering the market. These smaller firms are aggressively exploring ways to automate regulatory and policy mapping, incorporate a framework for integrated compliance and risk assessments, and provide the ability for multiple users to

update a common roster that identifies where an organization's data resides. In 2011, we expect technology firms large and small to produce new modules that will attempt to better integrate privacy into control monitoring.

GRC tools, however, should not be seen as a one-dimensional solution for managing risk. Often, organizations need to completely transform their risk functions. In 2011, we expect to see progressive organizations take an integrated approach that aligns risk and strategic business objectives. This means shifting GRC investment to focus on the risks that matter, and looking across the enterprise to identify compliance control redundancies. From there, organizations may wish to consider compliance convergence, which streamlines controls horizontally rather than vertically within the organization. Convergence of control activities will reduce audit fatigue and the strain that repeat audits put on resources. It may also produce the much-needed cost efficiencies many budget-conscious organizations still seek.

As organizations endeavor to implement a risk transformation program to improve GRC performance, privacy professionals need to make sure they have a seat at the table to ensure that privacy concerns remain a top priority for risk leaders and an integral part of any comprehensive GRC solution.

Questions to consider

- ▶ Have you considered different approaches for continuously monitoring key aspects of your privacy program?
- ▶ Have you assessed GRC solutions that offer a wide range of monitoring areas, including privacy?
- ▶ Have you asked your current GRC vendor for updated modules to help monitor risk and compliance related to the use of personal information?

¹ *The multi-billion dollar black hole – Is your governance, risk and compliance investment being sucked in?*, Ernst & Young's survey of 567 companies in Europe, the Middle East, India and Africa, conducted in the second quarter of 2010.



“Cloud computing has enormous social and economic potential. It can help businesses save money and create jobs. It can help governments increase efficiency and better serve their citizens. And it can help schools better educate their students. However, privacy concerns remain a significant impediment to the adoption of cloud computing for many potential customers. To ensure that society can maximize the benefits of cloud computing, removing the blockers around privacy is critical. Cloud service providers can start by building customers’ confidence in the cloud. They can do this by demonstrating an inherent respect for privacy that is embodied in transparent business practices and a commitment to accountability.”

Brendon Lynch, Chief Privacy Officer, Microsoft

Cloud computing

While cloud computing may be on the rise, many organizations still have reservations about the inherent data privacy and security risks associated with using cloud providers. In our 2010 Global Information Security Survey, only 23% of participants indicate that they currently use cloud computing-based delivery solutions. A further 55% say they have no plans to use cloud computing in the next 12 months. But this will change quickly – according to a 2010 Gartner research publication, by 2014 less than 10% of companies will see privacy concerns as a reason not to join the cloud.²

The major attractions of cloud computing are cost and flexibility. As some global economies struggle to recover, organizations are looking for more ways to streamline operations and save money. Cloud computing can be a huge cost-saver. It is particularly attractive to small- and medium-size businesses that use it to stay competitive.

But with cloud use comes responsibility. Organizations need to have robust vendor risk management, including third-party reporting capabilities that address data privacy risks. For example, cloud services located in different geographies raise regulatory challenges as personal information travels across jurisdictions.

Today in the US, it's easier to subpoena or otherwise compel the release of information when it is held by a third party (such as a cloud provider) than its original owner. And then there are laws such as the PATRIOT Act, which for some specific purposes allows the government to gain access to personal information residing in a third-party cloud provider without the knowledge of the information owner or data subject.

Further, as more companies choose to use a third-party cloud provider in 2011, they need to outline specific requirements that enable them to meet their privacy regulatory obligations. Before moving data to the cloud, organizations should analyze their data and develop policies that address both the risks associated with sensitive data and regulatory requirements.

Policies should include how soon the cloud provider needs to alert the organization of a suspected breach so that the organization can notify relevant regulatory bodies and individuals. Organizations will also want to be clear about retention periods, where the data can or cannot be transferred, logging of access by cloud administrators and the ability of other parties to access the data for market research or other secondary activities.

Questions to consider

- ▶ Have you conducted a risk-based review of what business processes and related personal information are needed before a move can be made to a cloud environment, and what varying levels of protection and control they require?
- ▶ Have you reviewed what contractual and regulatory limitations may exist over the use of a cloud provider, including questions surrounding geographic location, data retention and security?
- ▶ Have you explored your ability to monitor the adherence of your cloud providers to the terms set in your agreement with them, including the protection of personal information?

² “Predicts 2011: Enterprises Should Not Wait to Find Solutions for Business-Critical Privacy Issues,” Gartner, 8 November 2010, © 2010 Gartner, Inc. and/or its Affiliates.



Mobile devices

Laptops, cell phones, smart phones and tablets: in today's wireless world, there is an array of mobile devices that employees can use to stay connected to the office without stepping foot in the building. This kind of mobility offers huge opportunities for organizations to enhance productivity. But there are risks. Portable media lead to portable personal information. In 2011, we expect increased regulation that directly addresses protecting personal information on mobile devices, and the sensitive information revealed by geo-location tracking of mobile devices.

Geo-location

Technology advances are increasingly enabling organizations to identify the physical location of a device, as well as the person using it. In terms of privacy, organizations need to understand where to draw the line in using location data.

On the employee level, organizations can keep track of their workforce, comparing where their employees are at any given time versus where they are supposed to be. On the customer level, organizations can offer marketing programs that are based on immediate location.

If organizations decide to use physical location to track employees or reach out to customers with special offers, transparency is paramount. Employees need to know what the policies are regarding geo-location and what tools they may have at their disposal to shield their privacy by choosing how much information they share on the device. Customers must have the opportunity to provide informed consent before allowing any organization to track their location.

Encryption

Traveling data means understanding and adhering to state, federal and international privacy regulations that will vary from one jurisdiction to another. Some emphasize the encryption of personal information on mobile devices (e.g., the State of Massachusetts in the US). But, in most cases, hard drive encryption is only useful when a mobile device is lost or stolen and it is in the "off" or "hibernation" mode. It doesn't protect against hackers, nor does it necessarily protect information that is being backed up. Encryption is an effective tool for protecting some data, but it is not preventing attacks and it is likely not addressing your organization's top security risks.

Training and transparency

The benefits to organizations and employees of being able to work in different locations and in different time zones (think telecommuting) bring increased responsibility for protecting the personal information employees use for work. Employees and organizations alike need to understand and respect the limitations and technical controls of mobile devices. When employees use personal devices for work, organizations may be able to apply technical controls (e.g., require a download of a certain load set before allowing a personal device to connect to the firm's network) that provide visibility into various content and activities on those devices.

However, where should the organization draw the line in terms of infringement on personal privacy? Organizations need to ensure that they have specific policies regarding the use of each mobile device issued, and the extent to which personal devices used for work purposes may be monitored. Organizations should clearly communicate to employees what information is being monitored, how it is being monitored and the consequences for not adhering to mobile device policies.

Questions to consider

- ▶ Have you considered both the advantages and risks associated with using mobile device geo-location information for your operations?
- ▶ Have you assessed what level of encryption (or combination of levels) is merited to protect personal information in the common work settings of your organization?
- ▶ Have you reviewed your privacy policies recently in light of your organization's use of mobile devices?



Increased investment

Organizations understand the significance of data protection. They are increasing their investment around personal information, in part because of regulation, but also because of increasing risks. In 2011 we will see an increase in privacy and data protection investments that will focus on two issues: program initiatives and technical controls.

Organizations will once again review their governance structure through a privacy and security lens. They will launch new privacy programs, including updated policies, new procedures and awareness programs, and will recruit talent accordingly. Reacting to the global economic downturn, many organizations reduced compliance and risk management positions. As organizations start to rebound economically, and as privacy risks increase, organizations will

start to re-invest in related positions. The increased use of tools to protect privacy, such as DLP solutions, will also require appropriate staffing to monitor and respond to technology alerts.

In terms of technical controls, 2011 promises more spending in this area as organizations rely more heavily on controls to manage personal information. Tracing the web, with brand risk management in mind, is yet another area of investment for organizations in 2011 as employees and customers increasingly interact with (and discuss) organizations, products and services. In addition to the GRC and DLP technologies mentioned in previous sections, organizations will continue to invest in internal monitoring solutions to monitor inappropriate activity by insiders who use – and may be abusing – personal information.



“In health care, privacy goes back thousands of years to the Hippocratic Oath. The health care profession realized, even then, that the ability to provide care to individuals requires that the interactions between physician and patient remain confidential. Privacy enables trust, and trust is at the core of providing care. If that trust is absent, there can be negative consequences to the health of a patient, as they may not seek the treatment they need.

Unlike breaches in other industries, where you may be able to reimburse an individual after a breach, it is not possible to compensate an individual for an irreversible breach of their privacy. Trust is eroded.

Historically, the health care industry’s focus has been on regulatory compliance. The notion of security as a discipline that is separate from compliance is still relatively new. But as health care increasingly relies on technology as a means of providing care, security needs to mean more than basic guidelines on password length and not inappropriately sharing information.

The growing reliance on technology exposes the health care industry to new threats that go beyond those that have traditionally been a concern to health care. New and rapidly evolving technologies have also increased the stakes in that a breach may now involve thousands of records. Continuously adapting to changing threats and evolving technologies to manage risk and ensure patient privacy is the challenge we face in health care.”

Patrick Heim, Chief Information Security Officer, Kaiser Permanente

Questions to consider

- ▶ Have you assessed your budget needs in light of the evolving risk and compliance landscape?
- ▶ Have you reviewed the necessary positions for effective governance over your privacy and data protection activities?
- ▶ Have you consulted with your organization’s privacy professionals regarding the investment in technology to monitor the use (and possible abuse) of personal information?



More privacy assessments

Protecting personal information needs to be a never-ending focus for organizations. Internal auditors are increasingly challenged to identify and assess controls to minimize the risk of data breaches. According to our 2010 Global Information Security Survey, 54% of participants are already using internal auditing to test controls as a means of controlling data leakage of sensitive information. In 2011, we expect that number to increase.

In the past, internal audits have had a fairly broad focus. In the future, internal audit departments will begin to identify specific parts of their organizations to conduct deeper privacy audits. This may include reviewing the effectiveness of the monitoring of the possible exposure of personal information. Concerns over abuses of personal information by employees, whether intentional or unintentional, make privacy an area of risk that internal audit cannot ignore. Such audits address the effective use of technical controls to monitor activities and the use of personal information in databases, repositories and the organization's network. Audits

of guidance and training should also be performed, as incidents involving personal information may result from a lack of awareness rather than the intent to cause harm.

The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) Privacy Task Force's Generally Accepted Privacy Principles (GAPP) describe a comprehensive framework developed to allow the auditing and development of privacy programs. The GAPP help management develop effective policies to address privacy risks. They are gaining widespread recognition and use in the design, measurement, monitoring and auditing of privacy programs. In 2011, organizations will be able to use a newly developed maturity model to assess themselves with incremental improvement in mind. In addition, beginning in mid-2011, changes to reporting standards for service providers will allow organizations to include the GAPP criteria in the report they receive from their auditors.

Questions to consider

- ▶ Are there or should there be any privacy internal audits planned for 2011?
- ▶ Does the internal audit group in your organization have access to professional training about privacy risks?
- ▶ Have you reviewed the GAPP and their possible use in assessing and further developing your privacy program?



Service provider reporting standards

Even an organization with the most robust privacy practices and controls cannot comply with its privacy commitments if its service providers do not also have equally robust practices and controls. In our 2010 Global Information Security Survey, 41% of participants indicate that service providers and outsourcing rank among their top five areas of IT risk.

As a result, many organizations desire or require their service providers to obtain an independent assessment of their privacy and security practices. Often, organizations seeking such an assessment have been making do with reports performed in accordance with Statement on Auditing Standards No. 70 (SAS 70) reports, although these reports are not intended to address privacy, or even security for the most part.

The AICPA is in the process of issuing new guidance on service organization controls (SOC) reporting (SOC 2, *Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy*), which will allow service providers to report on their privacy and security controls.

A report prepared using this guidance will provide:

- ▶ A description of the service provider's system regarding the privacy and security of personal information throughout its life cycle

- ▶ A description of its system by management of the service provider, and an assertion of the effectiveness of its controls and its compliance with its privacy commitments in accordance with GAPP
- ▶ An auditor's opinion on the fairness of the description of the system, effectiveness of controls and compliance with privacy commitments based on GAPP
- ▶ A description of the tests performed by the auditor to arrive at its opinion, and the results of those tests

This new report will provide transparency and insight into the privacy and security practices of service providers, permitting them to demonstrate that they have effective privacy and data protection practices in place. Many leading service providers are eagerly awaiting this new guidance and their customers are anticipating its release even more.

Expect 2011 to bring an increased interest in and new discussion about independent assessments of privacy and security practices. Service providers should become familiar with this new guidance, the principles and criteria of GAPP and the controls necessary to address them. Service providers and their customers can follow the development of this guidance at <http://www.aicpa.org/InterestAreas/InformationTechnology>.

Questions to consider

- ▶ Have you been relying on your service providers' SAS 70 report as a privacy and security monitoring mechanism?
- ▶ Have you discussed with your service providers the controls over the use of personal information that you expect to see covered in the new reports?



Privacy by Design

Privacy by Design gained international recognition with the signing of the Privacy by Design Resolution at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem. The resolution is intended to help preserve privacy into the future.

The concept of Privacy by Design is not new. Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, has been championing the idea since the 1990s. The model offers a different approach to the security versus privacy conundrum. Rather than sacrificing one for the other, the concept of Privacy by Design suggests that organizations should design a system that protects both. Instead of treating privacy as an afterthought, Privacy by Design offers a proactive and prescriptive response that is entrenched into the very fabric of the organization.

The resolution ensures that privacy becomes an essential component of privacy protection by embedding it into new technologies and business practices from the beginning. The resolution also encourages organizations to adopt Privacy by Design principles as a fundamental means of operation. On a government level, it invites data protection and privacy commissioners globally to promote Privacy by Design and to incorporate its principles in future privacy policy and legislation in their jurisdictions.

In 2011, expect Privacy by Design to be increasingly openly debated by organizations as new products and services are discussed. The concept will further elevate the important role privacy professionals play in their organizations. It will also help increase their involvement with the initial operational considerations – those that influence the direction of the organization.



“We live in an era of enhanced surveillance: data mining, behavioral profiling, targeted and discriminatory practices and cloud computing. If we want to preserve the privacy that so many of our freedoms rest upon, beyond the next decade, we need to commit to a new approach, and we need to do it now.”

Dr. Ann Cavoukian, Information and Privacy Commissioner, Province of Ontario, Canada

Questions to consider

- ▶ Have you considered Privacy by Design as part of your system development life cycle (SDLC) and process development life cycle (PDLC)?
- ▶ Do privacy professionals in your organization play a mandatory and integral part in the early consideration of the business developments and changes that may impact both employee and customer personal information?



Social networking

There is a new generation of workers and customers who have never known a world without the internet, social media or around-the-clock access to information. They have different expectations of their work environment – expectations that blur the lines of personal, professional and commercial communication.

On an individual level, stories about social networking profiles scuttling job opportunities are legendary. Once pictures or status updates are posted, the internet makes them accessible forever. Social networks challenge the privacy concept of the right to be forgotten. Despite the development and growth of privacy regulations, regulators find it difficult to accurately capture the particular challenges that come with sharing personal information on social networks. Many of the actions taken by regulators regarding social networks have been directed at challenging their current practices and requiring certain changes to those practices. The right to be forgotten has yet to be addressed.

In the workplace, there are a host of issues about which companies need to be clear. They need to be transparent about their expectations of employees' behavior on social networking sites (as applicable to the organization) and whether such activities may be monitored and used to discipline them. Recruiters should have policies about whether and how to use social networks to mine for information on candidates and should communicate those intentions clearly when candidates come in for an interview.

Commercially, some organizations are creating a presence on social networks to promote products and services and to communicate directly with their customers. But when an organization creates a profile for this purpose, how does it define and communicate its privacy practices for the information it collects? And how should employees who communicate with customers on an individual basis use the additional personal information available to them from their customers' profile? These are all questions companies using social networks as a sales or promotion tool should be asking. Organizations also need to be aware that social media sites can be abused for fraud purposes and that the information that is collected by the site is not in the control of the organization and will likely end up "living" longer than the organization intends or expects.

In 2011, whether organizations use social networks to reach out to customers or to communicate with (or monitor) employees, policies and training are key. It is important that organizations develop and communicate thoughtful policies that address interactions among customers, employees and job candidates. Merely disabling social network use in the workplace is not a sustainable solution. The reliance on these policies is especially paramount in an environment where regulatory requirements do not easily align with technology and its common uses. Awareness campaigns and training must accompany the policy changes.

Questions to consider

- ▶ Have you considered the possible privacy risk and compliance challenges before using social media sites for commercial purposes?
- ▶ Have you brought together your compliance and HR groups to discuss the approach and policies to follow regarding the personal information on social media sites of employees and job candidates?
- ▶ Have you clearly communicated your expectations to employees regarding their communication on social networking sites where they are identified with your organization, or otherwise interact with colleagues or customers?



Evolving privacy professional expectations

With the ever-increasing scrutiny on privacy protection, it is no surprise that the privacy profession is evolving well beyond the position of the chief privacy officer. Organizations with privacy offices are recruiting and training privacy professionals to focus on specific areas of the business. Moreover, far from being a dead-end role with an unclear career trajectory, privacy positions are playing a pivotal role within the organization.

In 2011, organizations will increase their hiring of privacy professionals, reversing the head count loss privacy offices experienced during the economic downturn. Organizations will have a better understanding of the complex nature of privacy protection and their need to do a better job of managing the associated risk and compliance obligations.

Several organizations are improving the privacy function by merging information security, privacy and other functions (HR, legal, sourcing) into virtual information risk governance organizations, which take

a more holistic approach to data protection. This also encourages more proactive compliance with privacy requirements, rather than attempting to inject privacy after the fact.

Beyond professionals that solely focus on privacy, many positions that impact the organization's use of personal information will become increasingly savvy about privacy risk and compliance matters. In 2011, we will see individuals in areas such as IT, audit, legal and marketing add privacy to their skill sets.

To accommodate that growth, individuals seeking privacy certifications will rise in 2011. For example, Ernst & Young in the US has added Certified Information Privacy Professional (CIPP) as one of the professional certifications an employee may earn to be promoted in our Advisory Services group. In 2011, this and other certifications will become more professional, allowing individuals to be certified in focused areas, such as jurisdictional regulation, IT or industry-specific privacy requirements.



"As the privacy profession evolves, I expect we'll see continued focus on regulatory risk and information technology, but perhaps with an added dose of ethics and social responsibility added in. No longer will this be a role of just lawyers advising IT professionals or tech experts challenging regulatory norms. Collaborative technologies are challenging our notions of what is 'good' – what is good for our children, our communities, our society – in terms of how much information we share and keep indefinitely. We need responsible leaders, in corporations, the government and civil society, to address these questions."

Nuala O'Connor Kelly, Senior Counsel, Information Governance & Chief Privacy Leader, General Electric; Chairman of the International Association of Privacy Professionals Executive Committee

Questions to consider

- ▶ Have you considered specific positions in your organization that can benefit from additional training and certification in privacy?
- ▶ Have you identified specific certification requirements for professionals handling personal information in marketing, IT, internal audit, compliance and legal in your organization?



Conclusion

In an increasingly borderless operational environment, protecting personal information is paramount. Mobile communication, social networking and cloud computing have erased the boundaries of the traditional corporate environment. They have also created a number of new privacy risks for organizations and employees alike.

Regulators have taken notice. The year 2011 promises to usher in a host of new regulations and enforcement capabilities to see that organizations comply. But, as the new breach notification regulations coming into effect in various jurisdictions around the world highlight, privacy protection is no longer a compliance exercise. Organizations that ignore the importance of protecting personal information from outside – or inside – will suffer more than financial penalties. They may also see their reputation damaged and their brand negatively impacted.

Regulation and risk are the two primary reasons we will see organizations increasing their investment in privacy. They will be spending money to hire highly skilled certified privacy professionals and will invest in technical controls that monitor and manage external attacks and leaks from within.

As we enter 2011, a fundamental shift in how organizations approach privacy may be in order. Protecting personal information can no longer be an afterthought that is bolted onto an existing privacy or security program. As Privacy by Design suggests, it needs to be a series of much-needed policies that embed privacy protection into new technologies and business practices at the outset. The focus on privacy will enhance the business performance of leading organizations.

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 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 20,000 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 as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2011 EYGM Limited.
All Rights Reserved.

EYG no. AU0730



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

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor. The opinions of third parties set out in this publication are not necessarily the opinions of the global Ernst & Young organization or its member firms. Moreover, they should be viewed in the context of the time they were expressed.

www.ey.com

About Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers and more focused and faster in responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective IT risk management helps you to improve the competitive advantage of your IT operations, by making these operations more cost efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. 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.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contacts

Global

Norman Lonergan (Advisory Services Leader)	+44 20 7980 0596	norman.lonergan@uk.ey.com
--	------------------	--

Advisory Services

Robert Patton (Americas Leader)	+1 404 817 5579	robert.patton@ey.com
---	-----------------	--

Andrew Embury (Europe, Middle East, India and Africa Leader)	+44 20 7951 1802	aembury@uk.ey.com
--	------------------	--

Doug Simpson (Asia Pacific Leader)	+61 2 9248 4923	doug.simpson@au.ey.com
--	-----------------	--

Naoki Matsumura (Japan Leader)	+81 3 3503 1100	matsumura-nk@shinnihon.or.jp
--	-----------------	--

IT Risk and Assurance Services

Bernie Wedge (Americas Leader)	+1 404 817 5120	bernard.wedge@ey.com
--	-----------------	--

Paul van Kessel (Europe, Middle East, India and Africa Leader)	+31 88 40 71271	paul.van.kessel@nl.ey.com
--	-----------------	--

Troy Kelly (Asia Pacific Leader)	+852 2629 3238	troy.kelly@hk.ey.com
--	----------------	--

Masahiko Tsukahara (Japan Leader)	+81 3 3503 2900	tsukahara-mshk@shinnihon.or.jp
---	-----------------	--