Executive Strategies

Navigating Trends in Multinational Employee Data Management

Overview

In today's technology-driven, global marketplace — where more and more businesses are collecting and transferring personal data across national borders — employee privacy and data protection have become critically important.

Multinational organizations face complex data privacy compliance and management issues regarding their employees, former employees and job applicants. While many multinationals are working to make their human resource management systems operate at a global level, more and more countries are initiating privacy legislation that restricts the free transfer of personal information — including employee data — across national borders. Worldwide offshoring of business and IT processes increasingly places personal data and information in the hands of remote service providers. Complex global demands for stringent security and alarming rates of consumer identity theft and cyberterrorism contribute to the drive to keep sensitive information private and secure. In an environment defined by ever-changing multinational regulations, a demand for stronger corporate governance, constant technological innovation, and an emergent understanding of the financial implications of existing risk-mitigation controls, the management of employee data privacy and security takes on new importance.

"Governments and the private sector must work together to find appropriate ways to protect information privacy rights for consumers and producers around the world. " emphasizes Steve Christensen, director of Global Information Security and Privacy at Ceridian. "But many companies are beginning to recognize they need to apply the same levels of protection and flexibility to their own employee data. Now, as the demands for compliance give way to the costs of enforcement, is the time to talk about the next step."

The need for vigilant data management is more important than ever in the world of human resources (HR). Multinational employers must recognize the realities and challenges of accountability. Despite the security and protection offered by vendors and other companies that handle business data, enterprises may continue to find themselves at risk. Third-party providers are certainly protecting employee data within their means; however, full protection can only be provided by an individual's employer. A company may unintentionally or inadvertently infringe on an employee's data privacy by presuming that outsourcing offsets responsibility for data security and privacy. Every multinational organization is challenged to create, implement and sustain a responsive security governance model within its own walls.

Forward-thinking employers are particularly qualified to appreciate the challenges of data privacy and security. In a report from the 2004 HRO World Europe Conference in Brussels, *HRO Europe* magazine explained, "The regulatory reality remains that governments are far behind the technological security capabilities of HRO providers." As an HRO and multinational managed service provider, Ceridian is in a unique position to comment on the protection and management of employee data.

This executive briefing examines some of the emerging issues and trends a multinational organization may encounter in developing a privacy management structure strong enough to withstand existing employee privacy laws and flexible enough to comply with emerging global data privacy developments.

> "Data has become one of the most valuable assets an organization has and protecting intellectual property is becoming a business priority. The Internet makes it possible to distribute any kind of digital information, from spreadsheets to books, music and video, instantly and at virtually no cost. And since the Internet knows no borders, security and privacy is now a serious global issue. Governments and the private sector must work together to find appropriate ways to protect information privacy rights for consumers and producers around the world."
>
> Steve Christensen, Director, Global Information Security and Privacy, Ceridian

Global Perspective

Change is constant in the world of multinational data management. Developing — and maintaining — an effective privacy strategy requires the contemplation of a comprehensive global perspective, a thorough understanding of evolving concepts, and the ongoing observance of a complex and growing array of regulations.

Ten years ago, the European Union (EU) created an important catalyst for global data management change when it issued a new set of directives to safeguard personal data. The European Data Privacy Directive regulates the processing of personal data, including its transfer across national borders. In response, many other countries have been compelled to pause and examine their own privacy laws — stimulating a confusing array of new global regulations without clear direction on how to comply or the costs entailed. This transformation of the global privacy landscape, combined with the rapid evolution of e-business as the norm and an alarming increase in previously unimagined cyberthreats, has forced many companies to reevaluate their data security processes, policies and technology. The costs and consequences of a response to the growing array of demands have become significant.

"Multinational companies are facing a new HR privacy landscape that is in motion and employee-employer relationships that are changing," says Dr. Donald Harris, president of HR Privacy Solutions. "Knowing where the stress points are — where changes will affect policy and operations — is vital to a company's success."

"Multinational companies are facing a new HR privacy landscape... and employee-employer relationships that are changing. Knowing where the stress points are... is vital to a company's success."

Dr. Donald Harris,
President,
HR Privacy Solutions

Privacy concepts

Like regulations, concepts of data privacy can also vary from country to country and are best viewed through a flexible global lens. Definitions vary, but multinational employers may find it helpful to identify and adjust a baseline for a variety of terms, for example:

- *data privacy* — the rights related to an individual's "personal data."
- *personal data* — information from which an individual can be identified, whether directly (e.g., a social security number) or indirectly (e.g., a telephone number). Personal data is also sometimes described as the information carried on a business card: first and last name, physical address (home or otherwise), email address and telephone number.
- *sensitive personal data* — information such as racial or ethnic origin, religious or philosophical beliefs, political opinions, health or medical records, sexual orientation, trade union membership, criminal records, and other legally specified categories.
- *data processing* — any operation performed on personal data, from collection to manipulation, including storage.
- *data security* — the control and prevention of unauthorized access to and use of personal data.

"Every entity has an obligation to protect the private information they hold – either for customers or public citizens. And that means from threats big and small, external and internal."

www.theregister.co.uk

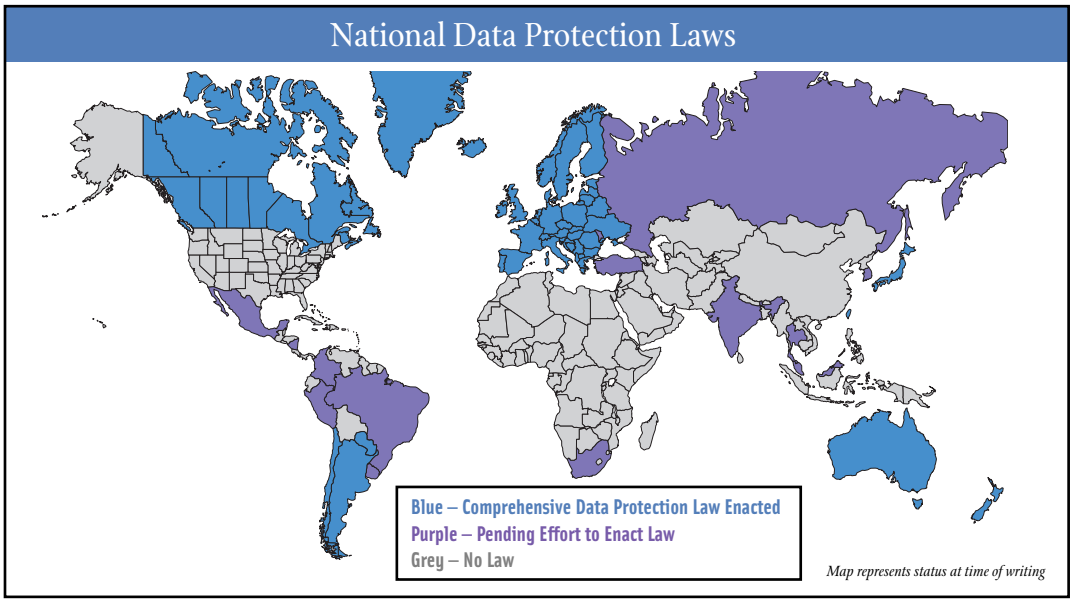
- *data subject* —the individual about whom personal data is collected.
- *data user* — the person who views and utilizes personal data.
- *data controller* — the person or entity, whether alone or jointly with others, (e.g., an employer) responsible for defining the purpose and the means of data processing. The data controller retains the responsibility of ensuring the data is collected and processed in accordance with the law and of assessing the adequacy of protection provided by data processors and handlers.
- *data processor* — an entity that uses clearly defined portions of personal information to provide a relevant value-add service.
- *data handler* — an entity, such as a records management service, that primarily houses and archives sensitive data offsite for protection and data recovery purposes.
- *data owner* — an organization or person who is housing information.

An awareness of various interpretations can be critical to a multinational organization's attempts to comply with global data protection policies. Two issues carry particular significance, especially in cross-border employee data transfers.

First of all, there are fundamental differences in the way countries look at the ownership of data. The concepts of *data subject* and *data user* are applied differently across the world. In Europe and Canada, where data privacy is considered a basic human right, the individual is usually referred to as the *data subject* and retains ownership rights. The *data user* has the responsibilities of a custodian for the protection of that information. In the United States, the prevailing concept is that once an individual provides personal information to an organization, the organization is the data owner, as well as the *data user.* U.S. firms often consider that the data they collect becomes their property and that they have the right, barring any sector-specific privacy legislation, to determine the use of it.

Secondly, because of these fundamental differences, there are important variations in the protection afforded to individuals in different parts of the world. For example, in the U.S. *sensitive personal data,* often regarded as information that could potentially be used for and against discrimination, is carefully protected by laws like HIPAA, Gramm-Leach-Bliley Act (GLB), and others. Globally, however, the EU Data Protection Directive sets more stringent rules that generally restrict any transfer of sensitive data.

Data protection policies around the world



Constantly evolving approaches to data privacy — each with its own set of requirements — complicate the ability of multinational companies to collect, process and transfer information regarding customers and employees. Multinational corporations must remain vigilant and nimble in their responses to different data protection and compliance demands around the world.

European Union Directive

When the European Commission adopted Directive 95/46/EC (the "EU Directive"), it set an important world standard. The basic provisions of the EU Directive ensure that personal data must be processed fairly and lawfully, collected and possessed for specific legitimate purposes, and kept no longer than necessary. Significantly, the EU Directive restricts the processing of sensitive data and prohibits data transfers to any country lacking an "adequate level of protection" as determined by the EU. As a result, any business that outsources data to countries with less-than-robust privacy and security policies can risk the loss of European customers. "Nine years after the passage of the EU Directive, uncertainty about achieving compliance with legal restrictions on international data transfers can still be a barrier to international commerce. Restrictions can be particularly costly for multinational companies that frequently need to transfer data between different corporate groups." (*International Chamber of Commerce*)

"Nine years after the passage of the EU directive, uncertainly about achieving compliance with legal restrictions on international data transfers can still be a barrier to international commerce."

International Chamber of Commerce

United States

With no national privacy legislation, the U.S. has developed data privacy and protection practices for specific industries and practices, while relying primarily on employer self-regulation for others. Several key regulations carrying implications for employers are in place in the U.S., including:

– The U.S. Patriot Act is a comprehensive piece of legislation passed with the aim of combatting terrorism, including cyberterrorism. Among other things, the Act expands U.S. law enforcement agencies' ability to access personal records. This has made it highly controversial, especially outside U.S. borders where some global corporations fear U.S. law

enforcement agencies will use the Act to access personal employee information more aggressively than would be allowed under local laws. However, there are many reasons to believe that U.S. law enforcement will continue to rely on other longstanding laws — obtaining court orders to access individual information, and working directly with employers regarding any potential internal threats of cyberterrorism.

– Sarbanes-Oxley (SOX), passed to protect investors from fraudulent accounting activities, has required substantial use of personnel, technology and financial resources in publicly-held U.S. businesses. Many subsidiary operations of U.S. companies in other countries are unaware that they too must comply with requirements of the act — such as auditing and monitoring of material compensatory changes globally.

– Other legislation — such as The Health Insurance Portability and Accountability Act (HIPAA), which mandates standards for the use of protected health care data; Gramm-Leach-Bliley Act (GLB), which requires financial service providers to disclose privacy policies to their customers; and individual state initiatives, like those in California requiring the removal of Social Security numbers from printed documents — has also required expenditures on new processes and audits, investments in software, and internal and external resources to ensure compliance.

Canada

The Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's most significant data privacy and security legislation. Designed to protect personal information held by private sector companies, it is recognized by the European Union as providing "adequate data protection" and allows Canadian businesses to seamlessly do business with the EU. Initially PIPEDA applied only to federally regulated private sector organizations but since 2004 it applies to any organization that collects, uses or discloses personal information in the course of a commercial activity within a province, whether or not federally-regulated. Employee and consumer data are also protected by provincial private sector laws where they exist. The Public Safety Act of 2002 contains key provisions, similar to the U.S. Patriot Act, that increase Canada's ability to protect its citizens from terrorist acts and includes an amendment to PIPEDA permitting organizations to collect and use personal data without an individual's knowledge. Like the EU, the Canadian regulatory environment attempts to create a minimum standard that is applicable in all circumstances, with some sectoral or regional laws exceeding the protection of the minimum standard.

Other global organizations and legislation

Around the world there are many other important groups and governments instituting new privacy legislation. A few examples include: Asia-Pacific Economic Cooperation (APEC), a U.S.-style self-regulation framework that encourages the development of appropriate information privacy protection to ensure the free flow of information in the Asia-Pacific region; the Hong Kong Personal Data (Privacy) Ordinance, which protects personal data and establishes the free flow of personal data to Hong Kong from countries that already have data protection laws; and the Law of the Russian Federation on Informatization [sic] and Information Protection, which does not have a central regulatory body for data protection but lists a code of fair information practices on the processing of personal information and forbids the use of personal information to "inflict economic or moral damage on citizens."

Despite the emergence of a growing array of global regulations, many national policies include the same basic principles of data protection and repeat the same security and privacy themes, using different words and regulatory bodies. In the muddy waters of ongoing legislative and technological change, governments and multinational organizations are developing a variety of responses in their attempts to find the way to a sound security program.

Responses to data protection policies

As the U.S. Department of Commerce explains, "While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union."

European Union (EU)	United States (U.S.)
The EU relies on *comprehensive* legislation that establishes that certain basic privacy rights be afforded citizens of the EU, requires creation of government data protection agencies, and in some cases, requires registration of data processing notices with those agencies or prior approval, before personal data processing may begin.	The U.S. uses a sectoral approach that relies on a *mix* of legislation, regulation and employer self-regulation, with no national data privacy legislation.

While the EU Directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions, some significant progress has been made. The following describes some of the options multinational employers are pursuing as they attempt to comply with global privacy directives.

Safe Harbor

Unfortunately, Safe Harbor has not proven to be the "silver bullet" of EU compliance for U.S. multinationals. Not all U.S. companies are eligible; only EU data *entering* the U.S. is protected (preventing U.S. headquarters from distributing relevant business data to key executives outside the U.S.); non-EU data is not addressed; and Safe Harbor subjects a company to increased liability under the jurisdiction of the FTC.

One way for U.S. companies to accommodate the EU Directive is via the "Safe Harbor" framework. The U.S. Department of Commerce and the European Commission developed Safe Harbor to help U.S. companies establish privacy processes that meet the EU requirements so personal data flows in their business models would not be interrupted and so, in most cases, claims brought by EU citizens against them would be heard in the U.S.

Safe Harbor was originally intended to provide a simple and cheap means to adequately comply with the EU Directive. However, it only addresses EU data entering the U.S., and the reality is that the rate of adoption by U.S. companies has been less than anticipated.

To be eligible, U.S. companies must be subject to the jurisdiction of the U.S. Federal Trade Commission (FTC) or U.S. Department of Transportation. This excludes many financial services companies (e.g., banks, insurance and credit unions) as well as telecommunications and not-for-profit organizations. As a Safe Harbor participant, a U.S. company may be subject to enforcement by both in-country Data Privacy Authorities (DPAs) and the FTC. Additionally, a Safe Harbor organization must annually file a certification form stating compliance with regulations with the Department of Commerce.

The European Commission issued a report in October 2004, noting that only a "substantial minority" of companies have adopted Safe Harbor. Of all the corporations doing business in the U.S., the Department of Commerce's latest count of "current" Safe Harbor participants is still well under 800 companies.

At the Third Annual Privacy and Data Security Summit, lawyer Becky Burr observed that, "While operating under the Safe Harbor increases company liability, it does not afford better protection for European employees." This leaves U.S. multinational organizations questioning why they should spend more money to subject themselves to additional scrutiny and potential increased liability while their EU subsidiaries have no true guarantee of protection of employee data. Many enterprises are examining other options.

Model contracts

Model contracts offer an alternative to Safe Harbor for employers who need to transfer personal data outside the EU. These contracts stipulate the conditions under which data transfer can take place and have been approved by the EU.

Model contracts impose a contractual obligation on the parties transferring data to process that data in accordance with EU protection principles. This allows personal data from the EU to be transferred to countries that do not meet the EU adequacy requirement. Ultimately, the European company is responsible for ensuring that transfers are consistent with local law and that the company provides sufficient data security and integrity guarantees (the U.S. side may be a controller too). In most cases, the European controller will be liable to the data subject any for misuse of personal data, even when the processor is responsible for a potential violation. As Becky Burr has pointed out, contract provisions are enforceable against a U.S. processor even when the European controller has disappeared or ceased to exist as a legal matter.

While model contracts offer a promising solution to EU compliance, the option is still a work-in-progress. At the time of this writing, fewer than 10 of the 25 countries in the EU have adopted model contracts. In late December 2004, after four years of negotiation, the EU approved a new set of clauses submitted by a coalition of business associations, including the International Chamber of Commerce (ICC) and the Confederation of British Industry (CBI). The new clauses, dubbed "Set II," form a more commercially flexible solution, including new guidelines on liability, security measures, audits, enforcements and use. Adoption of the clauses, which are subject to a three-year review, is without prejudice to national provisions, and all countries in the EU have their own national law in this area.

ISO 17799:2000 Code of Practice for Information Security

The International Organization for Standardization (ISO) is a non-governmental body and the world's largest developer of standards to help measure, manage and reduce risk. The network, which encompasses the national standards institutes of 150 countries, specifies internationally-recognized requirements for state-of-the-art products, services, processes, materials and systems, and for good conformity assessment, managerial and organizational practice.

ISO17799:2000 is the outcome of the collaborative effort to evolve the British Standard BS7799 as the common "security language" among ISO members. Continual enhancements resulted in the BS7799 Part 2, which combines the baseline ISO code of practice with a risk management approach and, in essence, adds specifications on how to apply the ISO17799 for information security management systems.

Rather than attempting to set rigid standards that could not possibly apply to every conceivable scenario, BS7799 provides a baseline of "common sense" controls with additional guidelines that can be applied based on risk within an organization's business environment.

This best practice has grown into an industry de facto standard, and has actually been adopted as the national standard for the Australia, Denmark, the Netherlands, New Zealand and Sweden. However, it is important to note that the Code's primary focus is on data security rather than data privacy.

Binding corporate rules and codes of conduct

Binding corporate rules (BCRs) are defined by the ICC as "a set of rules adopted within a particular company or corporate group that provide legally-binding protections for data processing within the company or group. They offer a more holistic approach to providing a legal basis for global data transfers." They are not yet approved by the EU as providing adequate protection for the purposes of onward transfer and, at the time of this writing, are under review by a European Commission Working Group.

Uncertainties remain about the legal enforceability of BCRs in some jurisdictions. They still lack a streamlined approval mechanism and require the need for consent from individuals whose data is being transferred. But a recent ICC survey suggests that governments and businesses should work together to eliminate these uncertainties, stating that, "There is a wide variety of legal principles which may lead to legal enforceability of BCRs. BCRs are therefore a realistic mechanism for providing a legal basis for data transfers in many jurisdictions around the world."

A c*ode of conduct* may be an acceptable alternative to a BCR. It can be a single document or an organization-wide set of documents explaining how personal information should be treated, particularly within a certain business sector. EU authorities are also beginning to consider business codes of conduct as viable options in the handling of personal information.

Codes of conduct could potentially offer multinationals a method for tailoring a global privacy solution to their individual operations and business risks, while clearing regulatory hurdles for international transfers of personal information. The key benefit of binding corporate rules and codes of conduct is their potential efficiency as EU-wide mechanisms.

Regardless of the options multinational employers choose in their response to data protection policies, most forward-looking organizations are keeping a weather eye on the major trends that are emerging in global employee data protection and management.

Trends

Against the background of evolving data management concepts and terminology, global privacy regulation, and compliance options, there are several recognizable trends emerging that seem likely to influence multinational employee data management in the near future.

1. Increased threat monitoring

"Not only is cyberterror a potential threat, but many experts believe that terrorists are using technology to commit crimes such as identity theft to help fund terror operations."

SHRM 2004-2005 Workplace Forecast: A Strategic Outlook

As organizations pool employee information from numerous global locations, the risks of merging data from multiple databases are exacerbated. The threat of unauthorized external access poses a well-recognized threat to company-level data security. The 24/7 nature of the Internet leaves corporate data constantly vulnerable. In recent years the news has been filled with stories of attacks on business networks as devastating computer viruses and "worms" have been unleashed around the world, often by exploiting vulnerabilities in widely used operating systems.

Combatting cyberterrorism will require international cooperation to ensure that cybercriminals are identified and punished, regardless of their location. International law enforcement is necessary to combat threats to businesses as well as national security. In the meantime, as the Society for Human Resource Management (SHRM) realistically points out in its 2004-2005 Workplace Forecast, the complex challenges of developing a global enforcement infrastructure make it paramount for individual businesses to "develop greater awareness of how to protect their own data and technology from attack."

Organizations face more than external attacks on their networks and Web sites. Many companies have begun to recognize a widening range of new internal liabilities and risks to data security and privacy that are inherent within their employee base, including:

- cell phones with audiovisual recording features that subject a company to the potential of having proprietary information recorded and "leaked."
- lost or stolen laptops, personal digital assistants (PDAs) and USBs containing company data.
- abuse by former employees have not been promptly removed from a computer system.
- use of wireless networks outside a company's firewall.
- downloading of applications that are not secure (e.g., personal software or games).
- potential lawsuits from current and former employees and Works' Councils when personal sensitive data is compromised.

2. Improved technology

Although Gartner has stated that secure corporate data management initially suffered from a "lack of robust, accessible technology solutions," the technology marketplace is responding

Even when helpful technologies exist, they are not always implemented.

"A recent survey by the Enterprise Strategy Group, a research firm in Milton [MA], found that the majority of companies don't encrypt their backup files. Jon Oltsik, a senior analyst for the group, said recent data-security problems are causing many companies to begin taking encryption more seriously."

Boston Globe, 5/2/05

quickly to growing threats by developing a wide range of new solutions — services and applications, privacy management practices, data minimization techniques, security technology, privacy violation detection, verification and certification.

As new technologies develop, some companies are choosing to implement "a multifunction security management system. ... A common security architecture for both wired and wireless networks so that firewalls, antivirus software, intrusion-detection systems, authentication, virtual private networks, access and authorization will be integrated with management tasks for bandwidth, devices and users." (www.computerworld.com, 12/13/04)

According to SHRM/eePulse collaborative research done a year after the attacks of September 11th, the majority of employers changed security policies in the aftermath of the event. "Employers are likely to continue to redesign their security measures as new threats arise. Technological advances could have a strong influence on the types of security measures implemented, while information management systems that aim to ensure employees do not pose a security threat could become more common for some types of organizations."

3. Escalating global regulations and enforcement

The intricacies of global legislation around data privacy and security have been well documented. As companies seek to establish policies that will comply with regulations in all operating countries, the complexities of compliance — and the potential costs of noncompliance — increase.

There is no doubt that U.S. awareness of the vulnerability of corporate data security and the risks of non-compliance has been heightened.

In April 2005, data broker LexisNexis said that, "personal information may have been stolen on 310,000 U.S. citizens, or nearly 10 times the number found in a data breach announced [the previous] month. An investigation by the firm's Anglo-Dutch parent Reed Elsevier determined that its databases had been fraudulently breached 59 times using stolen passwords, leading to the possible theft of personal information such as addresses and Social Security numbers." (*Reuters*)

The report followed weeks of similar high-profile news stories of security breaches at other large enterprises, including the Bank of America, MasterCard, health care heavyweight San Jose Medical Group, payroll handler PayMaxx and data broker ChoicePoint. "Whatever the specific legal fallout...the bigger effect may be its exposure of the patchwork of sometimes conflicting state and federal rules that govern consumer privacy and commercial data vendors.... State and federal regulators and lawmakers have started calling for an updating of those rules, which never envisioned the current power of data gatherers to amass and distribute vast digital dossiers on ordinary citizens." (*NY Times*, 2/24/05)

The potential repercussions from misplaced or stolen personal data has particular resonance in multinational organizations, which face the additional complexities of international data privacy regulations. In multinational organizations, employee data may be handled domestically within multiple borders but may also be passed through a single point in shared services. Exposure to risk is exacerbated by more employee data to protect, more exposure to multiple country regulations, and more potential retribution for noncompliance.

In May, 2005, Time Warner Inc., one of the world's largest media companies, reported that Iron Mountain, the world's largest data-archiving company, had misplaced unencrypted computer data tapes with the personal records of 85,000 current Time Warner employees, plus another 515,000 people who formerly worked for the company, some outside contractors, and some dependents of Time Warner employees. The New York Times reported that "Time Warner is offering to pay for one year of credit monitoring for all affected individuals" and also said Time Warner would begin encrypting its backup tapes.

The New York Times

But "compliance" is no longer a trend; it is a standard. In the spotlight of continuing news stories and renewed government focus, the stakes have been raised. As Paul Proctor, vice president of Security & Risk Strategies at META Group (now part of Gartner, Inc.), said during a Web cast on risk management and data protection trends, "Last year was the year of compliance, *this* is the year of enforcement."

4. New justifications for security needs

Under the current economic conditions, liability is a key driver in corporations; security is not just an IT issue anymore.

The complications and costs of complying with Sarbanes-Oxley, particularly in U.S.-headquartered companies whose multinational operations must also comply, have already made many corporate executives painfully aware of the need to protect their consumers' data. Now they are realizing their employee data must be protected just as carefully.

Effective security initiatives require funding. But in today's world, effective employee data management impacts more than just the quantifiable ROI of data protection. Corporate data management has migrated into the world of risk assessment and is now motivated by protection as well as profit — keeping intellectual property and employee data safe from compromise, insuring protection for valuable company data, and defending the enterprise from lawsuits for negligible conduct.

"Deciding which assets need the most protection, and determining the appropriate balance between cost and risk, are strategic decisions that only senior management should make. Furthermore, security almost inevitably involves inconvenience. Without a clear signal from upstairs, users will tend to regard security measures as nuisances that prevent them from doing their jobs and find ways to get around them." (*The Economist,* 11/01/02)

5. Corporate approach to security strategies and policies

In some companies, especially those with forward-thinking executives, the need for security is driving new links between IT and business strategy, uniting risk mitigation with corporate context.

More and more multinational organizations are beginning to understand that their data privacy policy impacts their business strategy as well as their IT processes. The location and management of cross-border call and data centers; the prevalence of mergers, acquisitions and partnerships; and the administration of sales and marketing activities that stretch across multiple borders all have significant implications for corporate data privacy policies.

Some successful multinationals support the need for high levels of data privacy by instituting a team approach to policymaking. Others go a step beyond, formalizing their collaborative approach by creating structures and processes that support continued sharing among team members. These organizations approach risk management with a cross-functional team that

"Digital security, once the province of geeks, is now everyone's concern. But there is much more to the problem – or the solution – than mere technology.... Deciding which assets need the most protection, and determining the appropriate balance between cost and risk, are strategic decisions that only senior management should make."

The Economist, 11/01/02

stretches across the enterprise and works together to set a policy, monitor and enforce its tenets, and propose changes as the environment evolves. Rather than having each business unit separately tackle policy and compliance, the group approach can add substantial business value by supporting best practices at minimal additional cost.

Because a solid security program involves business continuity, legal contracts, information security, business partners, insurance, corporate culture and privacy, cross-functional security teams often include a CEO or CFO, as well as representatives from legal, finance, IT, marketing, HR and risk management. In some cases, the team is lead by a security or privacy officer, usually from IT or risk management. In others, data protection becomes its own department. (Hewlett-Packard has a Chief Privacy Officer, for example, and IBM has a Director of Corporate Security Strategy who is responsible for developing an overall roadmap for IT security products, services and partnerships.) As roles change, the budget for security in some companies may appear to shrink. In many cases however, the investment of resources is simply being handled differently within the organization.

6. Employees as assets in risk management

The greatest security risk facing large companies over the next 10 years may be the increasingly sophisticated use of social engineering to bypass IT security defenses. Social engineering is the manipulation of people, rather than machines, to successfully breach the security systems of an enterprise.

"People, by nature, are unpredictable and susceptible to manipulation and persuasion. Studies show that humans have certain behavioral tendencies that can be exploited," Rich Mogull, Gartner research director for information security and risk, told *Information Technology Europe,* "We believe that social engineering is the single greatest security risk in the decade ahead."

But just as employees can present a potential risk to data security, they can also become a valuable asset. How? Through human capital management that creates and sustains a healthy corporate culture, with actively engaged employees who understand and are fully involved in corporate security policies.

Formal codes of conduct may form the basis of a security policy, but in conversations about ethics and risk management, corporate culture proves central to the discussion. In addition to threat monitoring, technological innovation, careful compliance, and cross-company security codes and policies, some multinational businesses support data privacy to the fullest by positioning employees as individual stewards of ethics and creating cultures that support, encourage and reward attention to individual privacy, trust and respect.

> "Successful corporate leaders must therefore strive to do the right thing, in disclosure, in governance, and otherwise in their businesses. And they must instill in their corporations this attitude of doing the right thing. Simply complying with the rules is not enough. They should, as I have said before, make this approach part of their companies' DNA. For companies that take this approach, most of the major concerns about compliance

disappear. Moreover, if companies view the new laws as opportunities — opportunities to improve internal controls, improve the performance of the board, and improve their public reporting — they will ultimately be better run, more transparent, and therefore more attractive to investors."

SEC Chairman William H. Donaldson,
National Press Club, July 2003

7. Data privacy as an ongoing process

Successful multinational corporations encourage a continuum view and treat data privacy as an ongoing process.

Even with strong policies, careful protection and supportive corporate culture in place, the job is not finished. Data privacy and security risks and regulations are constantly evolving. Multinational organizations must constantly evolve their data management as they seek to reduce risk, lower costs and increase predictability.

As Forrester Research analyst Michael Rasmussen pointed out in November 2004, "Achieving compliance is not an elusive impossibility or part of some secret society to which you do not belong. While technically oriented people may get lost in legalese during the struggle to reach compliance, compliance programs can be successfully implemented if approached correctly."

It's not always an easy task. Communicating the intricacies and importance of privacy to an entire organization can be overwhelming. As one legal consultant said, "Our clients send their IT staff to these data privacy conferences and they hear all these technical presentations around security and privacy — and they say to themselves, 'Drat, we don't do *anything* like that.' It can be quite disheartening. I urge a continuum view of data privacy."

The increasing external and internal threats to secure data management may require an ongoing multi-pronged solution — a safety net woven partially from successful data protection policies, stronger international enforcement of data privacy and security laws, continuous monitoring, and protection from evolving technologies.

Successful multinational corporations encourage a continuum view throughout the entire organization and treat data privacy as an ongoing process. Forward-thinking enterprises will continue to check themselves against existing benchmarks and keep moving forward on an ongoing agenda of data privacy and security initiatives. By recognizing that data management is more than a tangential concern, a set of written policies, or a one-time effort, and by looking beyond the volumes of regulatory manuals, and striving to nourish a culture of compliance, multinational organizations may be well positioned to take advantage of the opportunities for growth.

Ceridian's global security strategy

Who is Ceridian?

First company to provide businesses with payroll outsourcing services (1932)

Serves over 110,000 businesses and their 25 million employees worldwide

Offers payroll and human resource solutions in over 40 countries

Serves 338 of the U.S. Fortune 500

Serves 259 of the *London Financial Times Global 500*

One of the 50 Best Employers in Canada, *Report on Business Magazine*

Recognized by *Forbes* in the "Best of the Web" *Annual B2B guide* (2003, 2004)

Largest payroll outsourcing provider in Canada and the U.K. and the second largest in the U.S.

Largest provider of services for: work-life/EAP, FSA, QDRO,COBRA/HIPAA and stand-alone tax filing in the U.S.

Eighth largest 401(k) service provider

At Ceridian, security is serious business. With over 9,500 employees worldwide, Ceridian is a leading information services company serving businesses and employees in the United States, Canada and Europe.

As a multinational information services and human resources outsourcing company, Ceridian is at the forefront of employee data management. With its suite of innovative managed business solutions, our Human Resource Solutions serve more than 20 million employees, or 18 percent of the workforce in the U.S.; over 17 percent of about 2.6 million employees in Canada; and 7 percent of the workforce in the United Kingdom. Ceridian serves about 7 percent of the workforce. Ceridian's multinational payroll outsourcing solutions serve workforces in more than 40 countries, with plans to exceed 50 countries by the end of the year.

As a trusted business partner, Ceridian believes that maintaining the confidence of our customers is paramount. Rather than reacting to the starts and stops of political legislators around the world, we have taken a forward position to establish a comprehensive, multi-pronged, flexible global strategy that supports data security, privacy and protection within our businesses.

Comprehensive "top down" approach

Ceridian's commitment to the highest standards of information security practice starts at the top with senior management and extends to every part of the organization. All Ceridian business units are committed to appropriate standards and we are rigorous in our attention to complete corporate compliance with information security policies. Our goal is to utilize information security as one way to offer our customers world-class service, help our customers meet regulatory requirements, and demonstrate our high ethical standards.

Information assets, including all data stored on or traversing the Ceridian network, are considered the property of Ceridian or our customers and are treated with the same level of care we expect from our business partners.

Information security framework

Ceridian businesses utilize the concept of "Least Privileged Access" and a common security framework in their approach to information security. Under "Least Privileged Access" guidelines, employees are only given access to information they need on a routine basis to perform the duties detailed in their job descriptions, helping to ensure the security of customer data.

Ceridian's common security framework draws from an international standard (ISO 17799:2000) and serves as a common foundation, presenting guidelines on the policy requirements each business unit must embrace to meet corporate business and regulatory requirements.

Corporate commitment

At Ceridian, security is serious business. It is the responsibility of every employee, contractor and consultant to learn and adhere to Ceridian's information security policies. We stress the necessity of ensuring compliance with legal and regulatory requirements, maintaining corporate credibility, and meeting our customers' demands for information asset protection.

Each business unit shares in the responsibility for protecting information assets. Specific personnel in each unit are assigned overall security responsibilities including complying with local (country specific) regulations and communicating with Ceridian's corporate security group. Each business is also responsible for documenting information security policies, communicating those policies, and enforcing them. Policies apply to "normal" day-to-day activities and include provisions for handling exceptions.

Ceridian combines this overall corporate governance of data security, privacy and protection to myriad inter-company transfer policies, audit processes, pre-employment screening and policies, employee training, and a corporate code of ethics with clearly defined sanctions for violations.

Conclusion

"In many enterprises and global networks, concerns for information and process security affecting data will likely dominate corporate agendas for years to come."

Deloitte & Touche and the Office of the Information and Privacy Commissioner of Ontario

As privacy and security threats, technology, and demands for compliance increase, multinationals are responding by linking data management to business strategy, employing an ongoing collaborative approach that stretches across the business.

In order to successfully navigate the trends of multinational employee data management, corporations must maintain a global perspective; carefully monitor evolving privacy concepts, technologies, and protection policies; and develop a vigorous privacy management structure that can thrive in an environment of complexity, ambiguity and change.

External and internal threats to secure employee data management are increasing and will continue to increase. Technology is changing just as quickly, and the challenge to identify and implement successful new data protection solutions is ongoing. An expanding array of global data privacy policies and high-profile cases of misplaced and stolen personal data combine to point out the growing complexities of compliance and enforcement.

More and more C-level managers are identifying the strategic need for risk assessment and management. New security strategies are linking data management to business strategy, and many multinational enterprises are taking a collaborative, team approach that reaches throughout the entire business. Employees, who might be considered risks to secure data management, can instead become assets with the help of effective human capital management and a strong corporate culture that supports security policies.

Leaders of many multinational businesses are leveraging these trends and implementing strategies that allow them to meet the demands for data privacy protection with creativity and confidence. It is an ongoing process, and only those who begin with a sound program and remain flexible will succeed.

"Companies will achieve sustained success and cost effectiveness in information security and privacy protection by developing flexible strategies. Flexible means adapting fundamental principles, standards, and technologies to your own environment and priorities. It also means treating this approach as an ongoing process, requiring review, fine-tuning, update, and, in some cases, major reconstruction." (*Deloitte & Touche*)

Resources

In addition to sources already cited, this briefing is drawn from information and opinions expressed in multiple sources — interviews, publications, new articles, Web casts, Web sites and white papers — including:

Gartner, Inc.

Forrester Research

International Chamber of Commerce (ICC)

Society for Human Resource Management (SHRM)

Deloitte & Touche, *Security and Privacy – Peeling Back the Layers*

META Group, Inc., *Top Five Risk Management & Data Protection Trends for 2005*

U.S. Department of Commerce

HR Privacy Solutions

The Economist

HRO Europe

The New York Times

The Boston Globe

The Register

J. Beckwith ("Becky") Burr, Wilmer Cutler Pickering, Hale and Dorr

Third Annual Privacy & Data Security Summit

International Association of Privacy Professionals

www.privacyassociation.org

www.privacyexchange.org

www.pandab.org

www.informationshield.com

www.parl.gc.ca

www.iso.org

http://web.ita.doc.gov

Ceridian is changing the world of work by enabling companies to be free to succeed in their core business through its suite of innovative managed human resource solutions that include payroll and compensation, staffing, compliance, HR administration and employee effectiveness. Ceridian Corporation (NYSE: CEN) is an information services company serving businesses and employees in the United States, Canada and Europe. For more information about Ceridian's comprehensive array of human resource solutions, visit www.ceridian.com/multinational or call (800) 729-7655.

CERIDIAN 3311 E. Old Shakopee Road Minneapolis, MN 55425 800-729-7655 www.ceridian.com/multinational