

*Intensive risk, elusive value*  
A Risk Intelligent executive's  
guide to security and privacy





# Who should read this paper?

If you are a c-suite executive or board member who has seen media reports on the latest security or privacy breach and has wondered, "Could this happen to us?," this paper is for you.

If you are a non-IT professional with significant governance or executive management responsibilities, and if you have a nagging feeling that your organization might not be entirely on top of its security and privacy issues, this paper is for you.

If you are an IT executive who needs some logistical and logical support to help align thinking and bring the rest of the organization up to speed on security and privacy, this paper is for you (to personally pass along to others who may benefit from it).

If you fit any of the categories above, and if you are trying to decide whether it makes more sense for your organization to reinforce the locks or open the cage on your data, information, and intellectual property assets, this paper may provide the key you are looking for.



# Part one: Understanding the present

## Us and them

People in hypnotic, near-death, or spiritual states sometimes lose their ability to identify where “self” ends and “non-self” begins.

The same phenomenon may apply to your organization. Between outsourcing and offshoring, supply chains, alliances, partnerships, and other intertwined arrangements, the very definition of the enterprise has changed.

You may outsource your payroll, human resources, warehousing, manufacturing, or order fulfillment. In doing so, you are exposing vital data, from the personally identifiable information (PII) of your employees to the intellectual property secrets of your products.

Even your customers, at one time the embodiment of separateness, are now caught in the identity crisis: you share their data; they share yours.

The new reality: There is no “us” and “them” anymore. There is only “us.”

This blurring of boundaries can have profound implications for your organization. Data and information, the crown jewels of your enterprise, can no longer be defended in the manner of a moated castle, with security measures applied around the perimeter. Today, the moat has been drained, the walls toppled, and the assets scattered across the countryside.

A new world with no borders and virtual companies presents some thorny questions:

- What new risks were introduced when the walls came down?
- How do you protect your assets when they are no longer in one place?
- What is even worth defending?

Clearly, we are operating in a new environment. The rules have fundamentally changed. Unfortunately, many companies have not adapted; yet adaptation will be a critical success factor.

Business as usual is business at risk.



# Migration and mutation

With all manner of intellectual property convertible to ones and zeros, it's no wonder that defending the enterprise has become more difficult than ever.

Information moves freely and gets replicated, combined, and modified along the way. Every day, countless terabytes of data are transferred from corporate servers to laptops, USB drives, and smart phones. Information gets absorbed into spreadsheets; copied into databases; pasted into emails. It gets transmitted wirelessly; it migrates outside of corporate networks, VPNs, and other controlled environments; and it gets stored — properly and improperly.

The risk can vary, depending on multiple factors, including data distinguishability (how easily the data can be tied to a particular individual), the context of use, and its location and access.

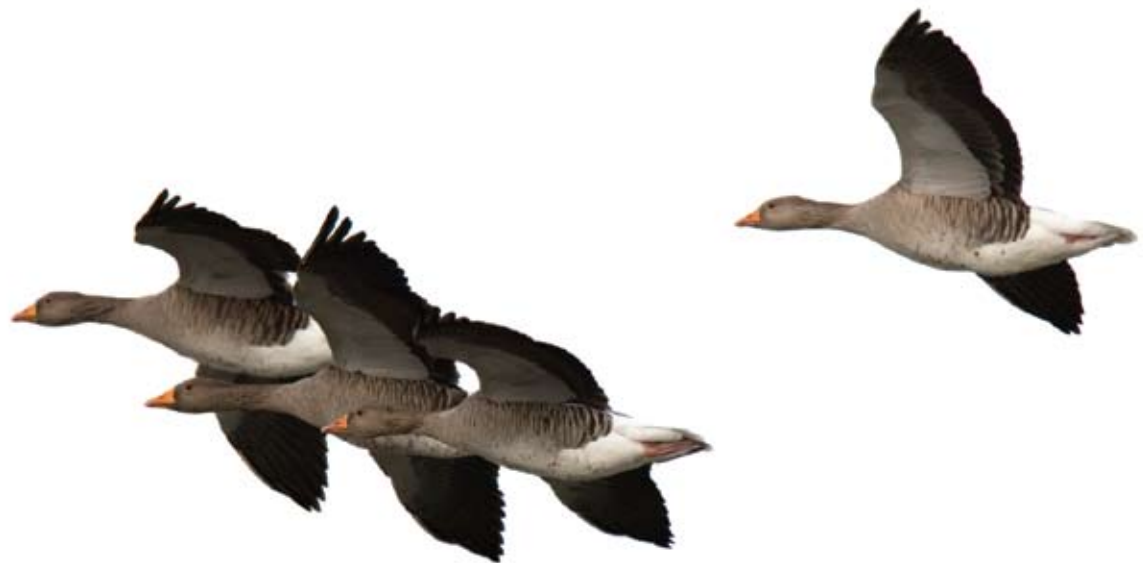
Consider, for example, the threat posed by data aggregation. Normally, a single record in a single data set — say, a person's name — carries little risk. But when that name becomes associated with another piece of information — like an account number or social security number — the risk level rises appreciably.

In many countries, privacy laws and regulations are based on combinations of data, not one piece of data in isolation. Organizations get into trouble when they don't safeguard against, for example, the ability of an employee to extract and combine data from various sources like a customer master file, an account transaction database, and a medical insurance report. When that happens, relatively harmless data can suddenly morph into a significant threat.

## Data and information: The difference

Although we use the terms "data" and "information" interchangeably in this document, there is, in fact, a difference.

- Data = technical/lowest level of abstraction
- Information = transformed data/middle level of abstraction
- Knowledge = business intelligence/highest level of abstraction



# The half-asset approach

---

At a time when knowledge is supposedly king, information abuse and neglect actually rules the kingdom. Many organizations don't tag, identify, inventory, or classify their data — or do so haphazardly.



Imagine that your company buys a large office building, with more than double the square footage needed to comfortably accommodate your workforce. You have to service the debt on this unnecessary floor space. You need to maintain it, secure it, and pay taxes on it. You derive no benefit from owning the extra space, but you pay handsomely to do so.

Such a move would be sheer folly, right?

Surprisingly, many organizations find themselves in an analogous situation in terms of their data. We postulate that up to half the information assets that companies maintain and defend are not wanted, needed, or used.

This superfluous data carries a significant price tag for collection, storage, and maintenance. More importantly, it carries huge potential costs in terms of legal responsibility and accountability. Many companies have paid dearly — in currency and reputation — for the misuse and loss of data that they never needed or used in the first place. Consider the recent case involving a global financial services company: backup tapes that were stolen contained data of marginal value to the company — but potentially great value to the thieves.

On the other hand, many digital assets that organizations possess do have intrinsic value. The problem is, most don't know the difference. At a time when knowledge is supposedly king, information abuse and neglect actually rules the kingdom. Many organizations don't tag, identify, inventory, or classify their data — or do so haphazardly. They fail to handle it properly in terms of storage, management, retention, retrieval, or destruction. They don't exploit its inherent value, nor do they mitigate its latent risk. They have a limited understanding of whether what they possess is worth keeping and defending.

In other words: Many companies don't know their assets from their elbows.

# The people paradox

Where does your biggest security risk lurk? Contrary to lurid media reports, the primary threat isn't hackers, hurricanes, or terrorists. It's actually the people within your "trusted" circle — your employees and your extended enterprise of contractors, customers, partners, and affiliates.<sup>1</sup>

The threat is not limited to fraud. Indeed, the bigger problem is relatively mundane: your employees and contractors are human. And, like all humans, they are prone to error and carelessness, fatigue, boredom, and distraction. They are susceptible to phishing and other social engineering attacks. As noted in a recent Deloitte global security survey, "breaches are as much a result of inadvertent and careless behavior as they are of malicious intent."<sup>2</sup>

Additionally, some people with IT system access don't understand the restrictions, rights, and obligations associated with data, so they routinely pass information to others in the organization — who may not have the same permission rights — creating data leakage. This phenomenon is, in essence, a "helpfulness" issue — great intentions leading to bad outcomes.

To help solve the people problem, many companies impose computer network access-level restrictions under the premise that you can't misuse data that you can't access. Yet the routine personnel activities of hiring, promotion, and firing can present complications. For example, as people change job functions, they often gain new access rights without ever relinquishing their old permissions. As a result, those with extended tenure at an organization eventually accumulate extensive, unmonitored privileges.

The Deloitte security survey<sup>3</sup> noted that controlling access requires vigilance and diligence that is sometimes lacking: "As simple as [access management] sounds in theory, in practice, it is not. Given changing job responsibilities, a more mobile workforce, employee turnover, and corporate reorganizations and mergers, this is a tall order." The survey additionally notes that auditors and regulators have shown a keen interest in this area.

In short, you are faced with a security paradox: People are simultaneously your greatest asset and your greatest risk.

---

Where does your biggest security risk lurk? Contrary to lurid media reports, the primary threat isn't hackers, hurricanes, or terrorists. It's actually the people within your "trusted" circle — your employees and your extended enterprise of contractors, customers, partners, and affiliates.



<sup>1</sup> For more information, see "Building a Secure Workforce: Guard Against Insider Threat," Deloitte Development LLC, 2008. Available at <http://www.deloitte.com/dtt/article/0,1002,sid%253D7021%2526cid%253D225950,00.html>.

<sup>2</sup> "Protecting What Matters: The 6th Annual Global Security Survey," Deloitte Development LLC, 2009. Available at <http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html>.

<sup>3</sup> Ibid.

# Fire trucks vs. smoke detectors

It's as predictable as the flu season: When the media reports another security or privacy breach, executives suddenly get motivated. They quickly assemble the brain trust. They demand reports. They seek assurances. "This can't happen to us, can it?"

The short answer is, "Yes, it can." According to a recent survey from the Ponemon Institute<sup>4</sup>, data breaches cost U.S. organizations an average of \$6.65 million per incident in 2008. Deloitte's research, conducted in collaboration with the Ponemon Institute, indicates that 32.1 percent of respondents report more than 20 incidents per year; 45.5 percent report more than 5 incidents; and 5.7 percent report 1-5 incidents.<sup>5</sup> As the data suggests, the costs can quickly add up.

Consider, for example, the major data loss recently suffered by a multinational company. To deal with the event, they sent postal notifications to several million customers whose personally identifiable information had been compromised; they purchased several months of credit report monitoring for each affected consumer; they paid significant legal fees; and they suffered unquantifiable but likely significant customer losses and reputation erosion.

All of which makes procrastination and passivity hard to fathom. Most executives are motivated and proactive when it comes to increasing revenue, attracting talent, and pursuing growth opportunities. Yet, within the security and privacy realm, many of these same executives wait for an external event — be it a spectacular crisis or a more routine regulation — before taking action.

Companies that deal with hazardous waste would never contemplate waiting for an accident before investing in safety measures. Farmers don't wait for their crops to be decimated by insects before applying pesticides. Yet in regard to security and privacy, many organizations still summon a fire truck rather than install a smoke detector.

---

Many executives wait for an external event — be it a spectacular crisis or a more routine regulation — before taking action.



<sup>4</sup> Ponemon Institute, "U.S. Cost of Data Breach Study," 2009. Available at [www.ponemon.org](http://www.ponemon.org).

<sup>5</sup> "Enterprise@Risk:2009 Privacy & Data Protection Survey," Deloitte Development LLC, publication pending.

# Part two: Envisioning the future

## The promise of the information age

In an ideal world, organizations and individuals enjoy the seamless delivery of high-quality information, transmitted safely and securely wherever, whenever, and to whomever it was deemed valuable and needed. This network would help create better informed, more productive people, and would enable the trusted, efficient, and effective delivery of products and services.

This is the promise of the information age, as yet unrealized, but attainable. What will get us there? A few prerequisites:

- An international framework that accounts for rights and obligations associated with information assets.
- Implementation of appropriate laws, regulations, and industry standards.
- Effective and efficient risk management approaches.
- Efficient use of information management resources.
- Accurate inventory and valuation of information assets.
- Sufficient investment in information technology based on this valuation.
- Availability of proven, accepted solutions that enable the safe delivery of information.
- Proactive mitigation and management of threats that are increasingly targeted and sophisticated.



# Part three: Building the bridge

## Forge the missing links

---

Policy and day-to-day operations must be inextricably linked, blended in a practical manner. Increasingly, regulators (and jurists) will accept nothing less.

How do some companies deal with privacy issues? Simple: A staff lawyer drafts a privacy policy and throws it over the transom. Follow-up? Training? Monitoring? Often it just doesn't happen.

How do other organizations handle security concerns? Similarly: They dump it into the lap of the IT group. Collaboration? Consultation? Coordination? Sometimes it simply doesn't occur.

These are not failures of intention, but of connection. Missing is a link between policies and operational reality. Rules are drafted to satisfy a regulatory or legal requirement, with scant consideration given to the business needs of the organization. The result? Policies that are unworkable and unenforceable. Or, perhaps even worse, irrelevant.

To be truly effective, security and privacy must transcend policy-making and become everyone's issue. Threats and opportunities must be broadly understood; priorities and shared responsibilities communicated; the message transmitted to stakeholders up, down, and across the core and the extended organizations.

The board and c-level executives have crucial roles to play, because direction is set from the top down. Unfortunately, recent trends suggest that support and involvement at this level may be waning. According to the Deloitte security survey, the current "financial turmoil has forced executives in North America to start de-prioritizing security initiatives ..." The survey showed "a significant drop in 2008 in the number of respondents who feel that security has risen to executive management and/or the board as a key imperative (63% in 2008 versus 84% in 2007)."<sup>6</sup>

These missing links must be restored. Organizations can no longer just write a policy and think they are done. Rather, policy and day-to-day operations must be inextricably linked, blended in a practical manner. Increasingly, regulators (and jurists) will accept nothing less.



<sup>6</sup> "Protecting What Matters: The 6th Annual Global Security Survey," Deloitte Development LLC, 2009. Available at <http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html>.

# Resolve the IT conundrum

During the last few years, many IT departments have found themselves in a no-win situation in terms of security and privacy. Two factors contributed to the current conundrum:

First, technology folks are burdened by the widespread misconception that security and privacy is primarily an IT problem. According to the Deloitte survey of top executives at Fortune 1000 companies, 9 out of 10 respondents expressed this viewpoint.<sup>7</sup>

Second, IT is hampered by unrealistic expectations: Since security and privacy is perceived as exclusively an IT problem, many believe IT should singlehandedly provide the solution.

This is a dangerously limited view. Imagine if similar thinking governed, say, the human resources department. At most companies, employment policies and paperwork are handled by HR. But out of logistical necessity, day-to-day supervision, performance evaluations, work assignments, and other responsibilities must be carried out by others. Without the engagement of the full organization, HR simply could not function properly.

So too with security and privacy issues. The area has grown substantially more complex in recent years, necessitating a multidisciplinary approach that has various groups working in concert. The CIO<sup>8</sup> can take a leadership role, but must work closely with the legal, compliance, HR, and other functions, as well as business unit heads.

At its core, security and privacy is a business issue, not a technology issue, and if you focus primarily on technology, progress will be painstaking. On the other hand, if you look at security and privacy as a business problem, a customer problem, or a stakeholder problem, then consensus, collaboration, and solutions will be much easier to come by.



<sup>7</sup> Ibid.

<sup>8</sup> For more information on the CIO's role, see "The Risk Intelligent CIO: Becoming a Front-Line IT Leader in a Risky World." Available at [www.deloitte.com/RiskIntelligence](http://www.deloitte.com/RiskIntelligence).

# Gain visibility

Shine a light on your information by developing a data inventory. Initiated *before* your next adverse event, a data inventory project can be completed on your own terms, without duress.



This question might not keep you awake at night — but perhaps it should: Do you know where your data is?

Unfortunately, many executives have little visibility into corporate information assets. They don't know who's accessing and modifying it; nor whether it's properly archived and secured.

Being in the dark can be dangerous if your organization is hit with a lawsuit. In the U.S., rules that were modified in 2006 govern discovery of information by both sides. Litigants must quickly come to the table with a list of sources of potentially relevant information. If your organization has a sprawling IT infrastructure, inventorying your email, file sharing, transaction systems, portable drives, and the like may prove logistically impossible under a court-ordered timeframe.

So shine a light on your information by developing a data inventory. Initiated before your next adverse event, a data inventory project can be completed on your own terms, without duress.

And the corollary benefits can be significant. You can:

- develop a full understanding of your data assets
- assess true risk and net value
- strengthen protections or loosen restrictions, as warranted
- map your asset inventory to applicable laws, regulations, and market expectations.

You'll likely need a point person for the effort. Some large organizations appoint a chief data officer (CDO) to oversee the task.<sup>9</sup> Companies that don't have the luxury of a CDO may enlist internal audit, information systems, or pull another employee from their normal duties.

The goals are simple, even if the process is painstaking. The team will examine data structures and management practices; inventory existing information; assess and assign risk and value. It will determine how you handle your own data, along with that of your customers and vendors. It will examine your data gathering and retention practices. It will answer the questions: Why are we collecting this data? What are we doing with it? Are we gathering superfluous or unnecessary information that represents potential risk without the opportunity for reward?

<sup>9</sup> The position of chief data office is still a relatively rare, but growing, role in larger organizations. For more information on this trend, see "The Role of the Chief Data Officer" at [http://www.deloitte.com/dtt/cda/doc/content/us\\_consulting\\_ti\\_roleofchiefdataofficer\\_250108.pdf](http://www.deloitte.com/dtt/cda/doc/content/us_consulting_ti_roleofchiefdataofficer_250108.pdf).

# Embrace data's dual nature

If your job title begins with “chief,” you should think about the information your organization controls in two ways:

- (1) how to harness it to grow the business
- (2) how to prevent it from harming the business.

This bifurcated view is required because data is simultaneously the most overexposed liability and underexploited asset in the entire enterprise.

Your liability is potentially immense. Consider: Who owns your data? Who has access to it? What controls are in place? What would be the impact to your organization if it got into the wrong hands? Are you spending enough to maintain and protect it?

At the same time, data value is invariably underappreciated. What data assets are you sitting on? Do you understand their true worth? Are you maximizing your return on your investment? Are your efforts to safeguard it commensurate with its value?

These opposing views create dynamic tension that must be resolved: between a Fort Knox and a laissez faire approach; between security professionals who want restriction and businesspeople who want liberation; between squashing the value with too many restrictions or squandering it with too few.

When companies realize the true value of their data, their natural inclination is often to more vigorously defend it. But the question must be frankly answered: Could this data have more value if we loosened the restrictions on it?

In our experience, many companies have yet to reconcile the issue: They are either overprotecting or not protecting at all.

Every stakeholder has a legitimate expectation that the value of the organization's data is maximized — and every executive has a clear responsibility to make certain it is. Focus your security program on adding value to your business transactions and your products, not on adding value to the security surrounding them.

---

A bifurcated view is required because data is simultaneously the most overexposed liability and underexploited asset in the entire enterprise.



# Untangle the regulatory knot

At a conceptual level, privacy is a simple notion. In application, however, the issue becomes significantly more complex, especially as geographical and political considerations come into play.

Take, for example, the 50 U.S. states. In America's regulatory patchwork quilt, similar incidents involving the loss of customer data can require significantly different responses depending on which state the affected consumer resides in. Even something as fundamental as the definition of PII varies from state to state.

Regional and international standards complicate the picture further. For example, certain Asian countries require that insurance carriers physically house data within the host country. As a result, insurers that operate in multiple Asian countries must maintain an independent data center in each, rather than consolidating into a centralized facility.

Clearly, security and privacy issues present a regulatory quagmire that deepens depending on the size of your corporate footprint. Worse, there is no simple way to extricate yourself from the mess.

Traditionally, companies have taken a purely compliance-driven approach to the problem, making a major resource commitment, involving corporate counsel and outside advisors, reviewing applicable laws and regulations, and mapping them to the businesses by geography. This brute force method, while thorough, can be expensive and time consuming.

Increasingly, organizations are adopting a risk-based approach that looks at commonality of requirements and then develops strategies and programs to take advantage of the similarities, including process simplification and consolidation. The challenge is significant, but the effort can prevent your security and privacy efforts from becoming disjointed and heterogeneous.

Follow through conscientiously with a plan in place to cover not only where you operate, but also where your data may reside. Then, the next time a laptop is stolen in Bangkok or a data tape falls off a truck in Berlin, you won't be scrambling for a timely, appropriate, and lawful response.



# Discover the delights of destruction

A few decades ago, efficiency experts would sing the praises of a favorite tool: the wastebasket. (Sometimes affectionately referred to as the “circular file.”) Today, the delete key and the computer’s recycle bin serve a similar purpose.

To the maxim “stuff happens” we can add a corollary: “data accumulates.” It grows without limits, like an independent life form. Storage capacity always manages to keep up, so your servers aren’t likely to choke on it — but your chief privacy officer, CIO, or corporate counsel might.

As such, now could be an opportune time to discover the advantages of destruction. Many companies rid themselves of potential security and privacy (and related legal) problems just by cleaning house. If you don’t keep it, you don’t need to secure it, and you don’t have to worry about it falling into the wrong hands.

If you initiated the data inventory analysis recommended previously, then you may already have a pretty good handle on what is expendable. Ask your chief data officer or other information security person to develop a data destruction policy. Pull in corporate counsel to confirm the legality of your proposed retention and destruction plans. Create automated purge routines for targeted classes of information. Then verify that your plans are being carried out correctly (and keep verifying).

At the same time, you shouldn’t destroy data unless you clearly understand its value to your organization. Furthermore, the potential legal requirement to retain data for specified time periods should be cause for pause before you purge.

Storage is cheap, but data protection is not. Remember: destroyed data can’t be compromised.

(Remember also that the delete key doesn’t actually delete. Be sure to adopt secure destruction techniques.)



# Solve the people problem

A quick quiz: Which organization had a “people problem”?

- The major American city that was essentially shut down by a disgruntled IT staffer?
- The large European bank that suffered a nearly €5 billion loss at the hands of a single rogue trader?
- The data analytics company whose employees were duped into revealing personal information on over 150,000 people in the company’s database.

The answer, of course, is all of them.

Surprisingly, in an age of heightened security awareness, common sense is often lacking. For example, no self-respecting bank would give the vault keys to a brand new employee. Yet the same institution will hand over the virtual keys to the enterprise to a recently hired network or IT administrator without a second thought.

Of course, most of your employees are honest, diligent, and loyal. You can maximize these attributes by providing effective training around security and privacy. Raise awareness in areas such as data security and dealing with suspicious activities. Involve employees in refining processes and plugging security gaps. And provide training for newly promoted employees who may now have different data access rights.

When it comes to training<sup>10</sup>, it’s important to avoid the trap of generality. Some commonality may exist in the curricula, but most employees will need help with specialized situations. For example, the training that a bank teller needs will differ from that required by an investment banker or securities trader within the same financial institution.

Unfortunately, training represents a major gap in many companies’ security and privacy programs. According to Deloitte’s “Enterprise@Risk” survey<sup>11</sup>, only 35 percent of companies surveyed offer privacy training annually. Forty-three percent offer it only once during an employee’s career. Meanwhile, 40 percent offer security training annually; with 37.5 percent offering it only once in a career.

Yet addressing your people needs may be the most important single step you can take. According to the Deloitte security survey, “an organization’s best defense against internal and external breaches ... is a culture of security within an organization — a mindset on the part of every individual so that actions in support of information security become automatic and intuitive.”<sup>12</sup>



## The Airline Approach

Consider taking an “airline approach” to security and privacy. At most major airlines, safety is the paramount concern, with the message and mindset embedded in the corporate culture. Every employee on the aircraft, from the flight attendants to the pilot, is trained to think safety first, and every one of them understands that one of their primary duties is that of a “safety officer.” When a US Airways plane made an emergency landing on the Hudson River in January 2009, that high level of training became dramatically evident.

<sup>10</sup> See Deloitte’s publication, “The People Dimension of Security & Privacy: Eight Training and Awareness Habits of Highly Effective Organizations,” Deloitte Development LLC, 2009. Available at <http://www.deloitte.com/dtt/article/0,1002,sid%253D26554%2526cid%253D266196,00.html>.

<sup>11</sup> “Enterprise@Risk: 2009 Privacy & Data Protection Survey,” Deloitte Development LLC, publication pending.

<sup>12</sup> “Protecting What Matters: The 6th Annual Global Security Survey,” Deloitte Development LLC, 2009. Available at <http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html>.

# Adopt a workable model

What type of structure should support your security and privacy program? Many large global corporations adopt a federated model. Emulating the structure of government, a federated model has a centralized group in charge of setting common standards and performing coordinating functions, with business units managing “local” execution.

The federated model is a hybrid of centralized and decentralized, the two other predominant forms. The Deloitte security survey found the use of federated models on the rise, with 22 percent of respondents in 2008 (compared to 13 percent in 2007) stating that they followed this model.<sup>13</sup>

The federated model promotes distributed responsibility for security and privacy issues, which can get more people involved and accountable for the safety and protection of information assets. Under the model, governance oversight takes place at the board level; common tools, policies, and procedures are developed and deployed from the executive level; and risk ownership and application of risk management tools resides at the business unit level.<sup>14</sup> Monitoring and enforcement occurs at each level of the model.

Of course, most companies align their security and privacy programs with their overall corporate structure, and are unlikely to revamp their business model solely to accommodate security and privacy concerns. It may not make sense, for example, for a strictly centralized and hierarchical organization to adopt a federated model. As such, security and privacy practices usually work within the confines of the existing organizational structure.

Each model has its strengths and weaknesses; choose the structure that is best aligned with your business needs. The simple existence of a security and privacy structure is more important than the particulars of the design.

---

The federated model promotes distributed responsibility for security and privacy issues, which can get more people involved and accountable for the safety and protection of information assets.



<sup>13</sup> Ibid.

<sup>14</sup> For elaboration, see “Putting risk in the comfort zone: Nine principles for building the Risk Intelligent Enterprise™” at [www.deloitte.com/RiskIntelligence](http://www.deloitte.com/RiskIntelligence).

# A few takeaways

While certain security and privacy issues can be solved with encryption, strong passwords, or process reengineering, such steps are tactics and should not be confused with business strategy.



Some security and privacy takeaways:

- It's hard to restrict access to something if you don't control it in the first place.
- In both fashion and in security, "one-size-fits-all" rarely does.
- Your greatest challenge may be in securing an investment before catastrophe strikes. (Naturally, funds flow freely after a problem arises.) So explain the issue in business — not technical — terms to those who control the purse-strings.
- Any hours you spend documenting the ROI on your security and privacy programs will be time well spent.
- Shifting priorities — on an organizational level, but also within your security and privacy program itself — can undermine your objectives. Make sure you have a Risk Intelligent CIO<sup>15</sup> who has a seat at the executive table.
- Change your thinking about roles and responsibilities. It's no longer about departments and divisions; it's about what people can and cannot do with information assets.
- Don't blithely accept third-party data hand-offs. Limit your liability by only accepting the data you actually want and need.
- Data should be treated as an asset — with its value, risks, and expected ROI identified and resources applied to it accordingly.
- Live in the present and anticipate the future. Threats continually evolve. Yesterday's threats will not necessarily be tomorrow's.
- Consider employee demographics. Gen Y brings a digital persona into the workplace, along with their smart phones and MP3 players that can store hundreds of gigabytes. Their web-based email and text messaging capabilities may circumvent security safeguards. Their blogs and Facebook postings may contain sensitive or embarrassing information.
- Adopt a well-rounded perspective. Security and privacy is a complex business problem. While certain security and privacy issues can be solved with encryption, strong passwords, or process reengineering, such steps are tactics and should not be confused with business strategy.
- Avoid a minimalistic approach. Consider what safeguards need to be in place, rather than the minimum you can get away with. Treat security and privacy as you would health and safety in a hazardous industry — take heightened precautions.
- Don't think of security and privacy as a project with a beginning and end point. It must be a sustained, disciplined, methodical process. It encompasses not just policies and procedures, but budgeting, training, technical implementation, monitoring, compliance, and governance.

<sup>15</sup> See "The Risk Intelligent CIO: Becoming a Front-Line IT Leader in a Risky World" at [www.deloitte.com/RiskIntelligence](http://www.deloitte.com/RiskIntelligence).

# Contacts

## U.S. Contacts

### Ted DeZabala

Managing Principal  
Security & Privacy Services  
Deloitte & Touche LLP  
+1 212 436 2957  
[tdezabala@deloitte.com](mailto:tdezabala@deloitte.com)

### Rena Mears

Partner  
Security & Privacy Services  
Deloitte & Touche LLP  
+1 415 783 5662  
[renamears@deloitte.com](mailto:renamears@deloitte.com)

### Henry Ristuccia

Managing Partner  
Governance, Regulatory & Risk Strategies  
Deloitte & Touche LLP  
+1 212 436 4244  
[hristuccia@deloitte.com](mailto:hristuccia@deloitte.com)

### Bruce Murphy

Principal  
Deloitte & Touche LLP  
+1 973 602 6020  
[brmurphy@deloitte.com](mailto:brmurphy@deloitte.com)

### Bill Kobel

Principal  
Security & Privacy Services  
Deloitte & Touche LLP  
+1 214 840 7120  
[bkobel@deloitte.com](mailto:bkobel@deloitte.com)

## International Contacts

### Adel Melek

Partner, Global Leader  
Security & Privacy Services  
Deloitte Canada  
+1 416 601 6524  
[amelek@deloitte.ca](mailto:amelek@deloitte.ca)

### Simon Owen

Lead Partner  
ERS - Information & Technology Risk  
Deloitte United Kingdom  
+44 20 7303 7219  
[sxowen@deloitte.com](mailto:sxowen@deloitte.com)

Through the development of security and privacy strategies, Deloitte helps its clients:

- unleash the value of information
- protect information assets that are critical to the delivery of products and services
- establish and maintain trusted business relationships
- leverage information management resources efficiently and effectively.

For a discussion of your business issues or for more information on our services, contact any of the professionals listed above.

#9078

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright ©2009 Deloitte Development LLC. All rights reserved.  
Member of Deloitte Touche Tohmatsu