Deloitte
Review

ISSUE 6 | 2010

Complimentary article reprint

Lock it Up or Set it Free?

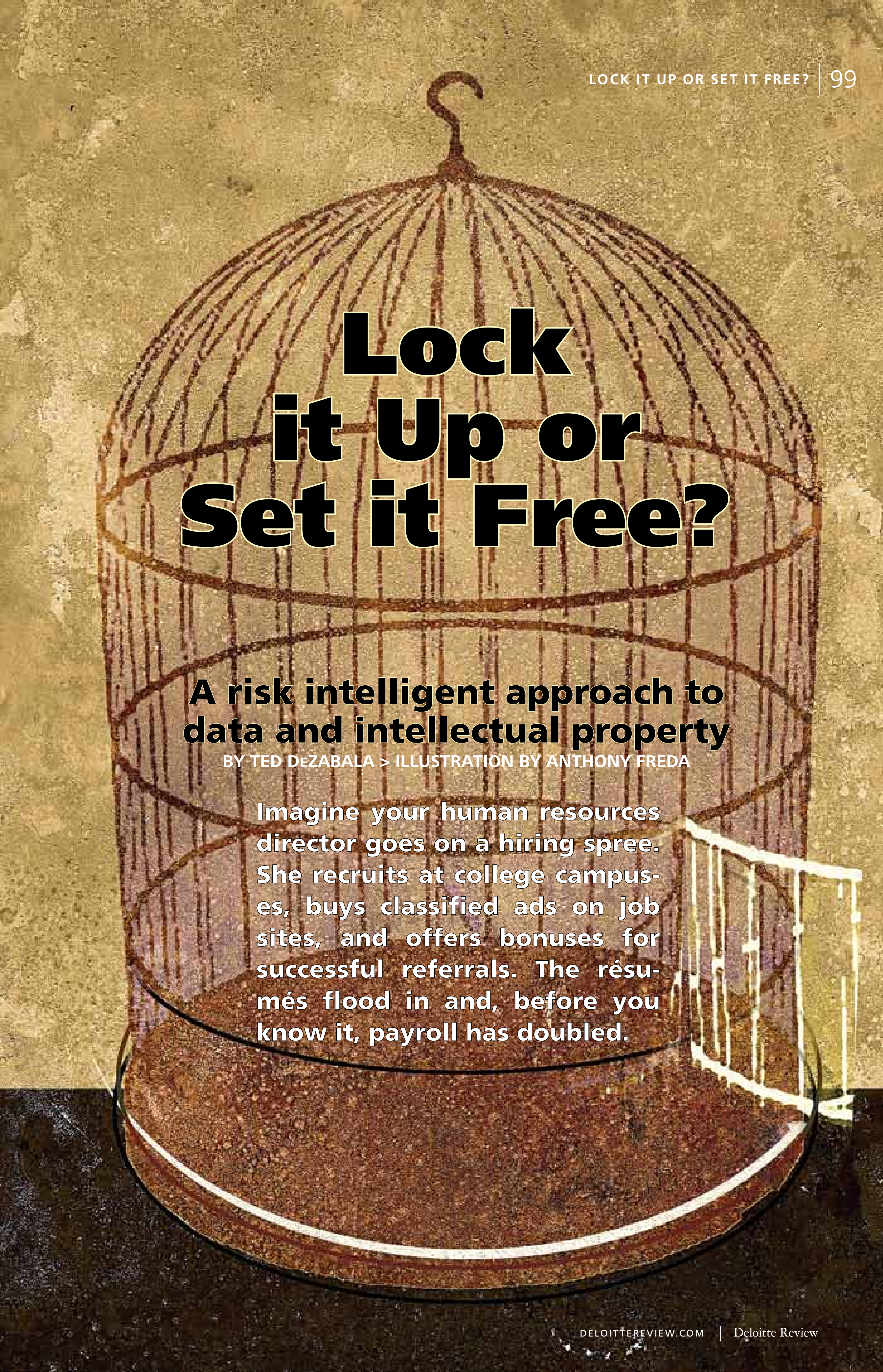
A risk intelligent approach to data and intellectual property

BY TED DEZABALA > ILLUSTRATION BY ANTHONY FREDA

This publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, 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 finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.



Lock it Up or Set it Free?

A risk intelligent approach to data and intellectual property

BY TED DeZABALA > ILLUSTRATION BY ANTHONY FREDA

Imagine your human resources director goes on a hiring spree. She recruits at college campuses, buys classified ads on job sites, and offers bonuses for successful referrals. The résumés flood in and, before you know it, payroll has doubled.

But the workload hasn't. You have no new contracts, no fresh products, no fledgling partnerships. Your new employees have nothing to do. Meanwhile, there are paychecks to sign, taxes to pay and benefits to administer.

Such a situation would be absurd, of course (and your HR director quickly unemployed). Yet many organizations find themselves in an analogous situation in terms of their information and intellectual property. They voraciously collect data from customers, suppliers, employees and business partners, harvesting all manner of personally identifiable information (PII): account numbers, passwords, mothers' maiden names, health information, purchasing habits and who knows what else. They spend significant sums storing and protecting this data in accordance with industry and regulatory standards.

Most companies carefully guard their intellectual property—trade secrets, formulas, creative works, trademarks, patents and processes—with expensive layers of protection and through costly and time-consuming demand notices, injunctions and lawsuits. Yet we've found that many efforts to safeguard intellectual property are ineffectual or even counterproductive – depressing the value of the very thing they are trying to protect.

The expenditure may be going to waste. Based on our experience with hundreds of organizations, up to half the data assets that companies maintain and defend are neither needed nor used. This excess data carries a steep price tag for collection, storage, maintenance and protection. Even more importantly, however, it carries almost incalculable potential costs in terms of liability. A cursory glance at the news shows that many companies have paid dearly—in currency and reputation—for the misuse and loss of data that, in many cases, they never needed or used in the first place.

Similarly, most companies carefully guard their intellectual property—trade secrets, formulas, creative works, trademarks, patents and processes—with expensive layers of protection and through costly and time-consuming demand notices, injunctions and lawsuits. Yet we've found that many efforts to safeguard intellectual property are ineffectual or even counterproductive – depressing the value of the very thing they are trying to protect.

Of course many data, information and intellectual property assets that organizations possess *do* have value. The problem is that most companies do not distinguish between crucial and useless data. Even if they attempt to inventory and classify these assets, oftentimes they do so haphazardly.

This situation presents concerns regarding both value and risk. Can the leaders of these companies assure their boards that they extract high value from their information assets? And, on the risk side, can they declare that the company's data security and privacy practices are comprehensive, efficient, reliable and aligned with the company's risk tolerance?

At a more fundamental level, do organizations truly know what information assets they control (or have a shared responsibility to control with their business partners)? And are they sure these assets are worth keeping and defending?

CORPORATE IDENTITY CRISIS

The business of business used to be simple. A half century ago, most companies were clearly defined entities, operating in a single industry, tied to an identifiable geography, and run by employees of long tenure, if not lifetime allegiance.

Today, conglomerates engage in multiple industries; operations are spread worldwide; workers are virtual or contract. Companies outsource and offshore, form alliances and partnerships and acquire and divest in a manner that borders on the promiscuous. They may outsource payroll, benefits administration, manufacturing or fulfillment. Doing so exposes critical data, from the personally identifiable information of employees to intellectual property and trade secrets.

The boundaries between "company" and "non-company" have blurred, with significant implications. In many instances, data and information can no longer be readily protected like the gold in Fort Knox, with security measures around the perimeter and the valuables tucked safely inside.

A new world with no walls and virtual companies presents some difficult questions:

- What new risks were introduced when the vaults were opened?
- How can you protect assets when they are no longer securely under your control?
- What is even worth defending?

INTENSIVE RISK; ELUSIVE VALUE

In the end, it comes down to sight and insight – gaining a view into what you have and how you are handling it; an understanding of what has value and must be protected and what is superfluous and can be discarded; and insight into the opportunities that should be pursued and the risks that must be mitigated.

Here are a few steps to consider.

1) Ease the burden on IT

In many organizations, the information technology department finds itself in a lose-lose situation when it comes to security and privacy. Two factors come into play. First is the widespread belief that security and privacy are primarily technology problems. In a Deloitte* survey of top executives at Fortune 1000 companies, nine out of 10 respondents expressed this opinion.[1]

Second, IT must deal with unrealistic expectations. Since security and privacy are generally viewed as technology issues, many believe IT should take full responsibility for the solution.

This is a counterproductive attitude. Imagine, for example, if similar thinking were applied to human resources. Within most organizations, employment policies and procedures are the domain of HR. But out of practical necessity, day-to-day supervision, performance evaluations, work assignments and related responsibilities must be carried out by other personnel. Without the involvement of the full organization, human resources would quickly lose its capacity to function.

The same principle governs security and privacy issues. With the complexity and strategic importance of data, information and intellectual property rising in recent years, a collaborative, multidisciplinary approach should be applied. The CIO can lead the charge but should work closely with counterparts in legal, compliance, HR and other functions, along with business unit heads.[2]

TREATMENT VS. VACCINES

It's as predictable as fast food (but perhaps not as savory): When news breaks of another security or privacy breach, executives suddenly take notice. They summon key leaders, demand reports and solicit 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,* data breaches cost U.S. organizations an average of $6.65 million per incident in 2008. With nearly one-third of respondents reporting more than 20 incidents per year, and with almost one-half reporting more than five incidents, the costs can quickly spiral.

All of which makes C-suite passivity hard to understand. Most executives are motivated and proactive when it comes to raising revenue, recruiting talent and nurturing growth. Yet when it comes to security and privacy, many of these same executives wait for an external event—be it a full-blown crisis or more routine regulation—before taking action.

Nuclear plant operators don't wait for an accident before investing in safety measures. Seacoast residents don't wait for the hurricane to wash ashore before boarding up the windows. Yet in regard to security and privacy, many organizations opt for the treatment rather than the vaccine.

* Ponemon Institute, U.S. Cost of Data Breach Study, 2009. www.ponemon.org.

* As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

At their essence, security and privacy are about business, not technology. Those who look at security and privacy as a business problem, a customer problem or a stakeholder problem may find solutions easier to come by.

2) Take stock

Executives often have a poor understanding of their information assets. In some cases, even CIOs we have conferred with (who are more likely than others in the C-suite to have a handle on the issue) don't know exactly what they have, who is accessing and modifying it, and whether it is properly archived and secured. This lack of insight can pose problems in many realms, notably competitiveness, efficiency, compliance and security.

Executives often have a poor understanding of their information assets. In some cases, even CIOs we have conferred with (who are more likely than others in the C-suite to have a handle on the issue) don't know exactly what they have, who is accessing and modifying it, and whether it is properly archived and secured. This lack of insight can pose problems in many realms, notably competitiveness, efficiency, compliance and security.

The liability aspects can be particularly vexing. Recently in the United States, the rules that govern legal discovery were modified, and as a result, litigants now have a narrow timeframe to produce sources of potentially relevant information. If your organization was hit with a lawsuit wherein these or similar discovery rules applied, would you be able to respond within the legally mandated timeframe? For companies with a widely dispersed IT infrastructure, completing a timely inventory of email, file sharing, transaction systems, portable drives and more may prove logistically impossible.

Thus, maximizing the value and minimizing the risks associated with information assets starts with a comprehensive data inventory project. Initiated *before* the next adverse event, an inventory project can be completed free of time pressures or other forms of duress.

Through this project, you can gain a comprehensive overview of the company's information assets, enabling you to assign risk and value ratings. It will permit you to reduce risk and improve efficiency by mapping the asset inventory to applicable laws, regulations and market expectations. And, finally, the project can provide the knowledge necessary to strengthen or loosen protections, providing either more security or generating greater return, as analysis dictates.

Some large organizations appoint a chief data officer (CDO) to oversee the task.[3] Companies that don't have the advantage of a CDO may enlist internal audit or IT, or may pull another employee from his or her normal duties. Other companies will hire an outside consultant for the project.

The goals are simple, even if the process is time consuming. The team will examine data structures and management practices, inventory existing information, and assess and assign risk and value. It will determine how you handle internal data, information, and IP along with that of customers and vendors, as well as examining gathering and retention practices. It will answer the questions: Why are we collecting this information? What are we doing with it? Are we gathering unnecessary information that represents potential risk without the opportunity for reward? Are we maximizing the value of what we collect?

Despite these obvious potential benefits, training represents a major gap in many companies' security and privacy programs. According to our "Enterprise @ Risk" survey, only 35 percent of companies surveyed offer privacy training annually; 43 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.

3) Solve the people puzzle

Despite what the headlines might imply, the primary security and privacy threat is not hackers and cybercriminals. Rather, it is the people you deal with every day – employees, contractors and partners.[4]

Nor is the threat limited to insider fraud. In fact, the more significant issue rarely hits the headlines: even honest people make mistakes. They get tired, bored and distracted. They fall for 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."[5]

To address the issue of human failure, many companies impose computer network access-level restrictions under the belief that data that can't be accessed can't be misused. Yet these steps, while important, offer no panacea, as the routine personnel activities of hiring, promotion and firing can undermine the controls. For example, as people change job functions, they often gain new access rights without ever relinquishing their old permissions. As a result, those with a long employment history can accumulate extensive unmonitored privileges.

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, it can be a tall order.

But the situation is far from hopeless. Providing training around security and privacy can raise awareness in areas such as data security and dealing with suspicious activities; it can involve employees in improving security processes and closing security gaps; and it can quickly bring up to speed newly promoted employees who may have different data and information access rights.

Despite these obvious potential benefits, training represents a major gap in many companies' security and privacy programs. According to our "Enterprise @ Risk" survey, only 35 percent of companies surveyed offer privacy training annually; 43 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.[6]

In prioritizing activities to get security and privacy practices into shape, it is often best to place people needs near the top of the list. An organization's best defense against internal and external breaches is a culture of security – a mindset on the part of every individual so that actions in support of information security become automatic and intuitive.

4) Translate policy into action

Companies deal with privacy issues in many ways. One common approach has in-house counsel draw up a privacy policy that is then incorporated into the personnel policies of the organization. And there it sits. Training, monitoring and enforcement often never enter the picture.

A similar ineffectual approach often applies to security concerns. The problem often gets dumped into the lap of the IT group, with minimal collaboration or coordination beyond that group.

These are not failures of intention but of connection. Rules are drafted to satisfy a regulatory or legal requirement but often without consideration of the business needs of the organization. Predictably, the policies are often unworkable, unenforceable or even counterproductive.

To be effective, security and privacy must transcend policymaking to become everyone's issue. Risks and opportunities as well as priorities and responsibilities must be widely shared and understood throughout the core and the extended organization.

The board and C-level executives are key in this effort, due to their control of the bully pulpit and their roles as leaders. Unfortunately, recent trends suggest that support and involvement at the top of the organization may be waning. According to a Deloitte security survey, the recent "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 percent in 2008 versus 84 percent in 2007)."[7]

Organizations that want to bring their security and privacy issues under control will take steps to reverse this trend.

5) Untangle the regulatory knot

Theoretically, privacy is fairly straightforward. In the real world, however, the issue becomes significantly more complex, especially as geographical and political considerations come into play.

Consider, for example, the 50 U.S. states. In America's regulatory patchwork, similar incidents involving the loss of customer data can require significantly different responses depending on which state the affected consumer resides in.

Companies that operate on a global scale face even greater complexity. Not only do regulations vary throughout the world, but the target is continually moving as countries elect new leaders, implement new policies, and enact new legislation and regulations.

In response to this regulatory quagmire, many organizations have adopted a purely compliance-driven approach, convening a task force to review 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. Such an effort, which devotes resources to the areas of greatest need, can prevent security and privacy efforts from becoming disjointed and heterogeneous.

6) Encourage destructive tendencies

Data accumulate seemingly without limits. Fortunately, storage capacity has historically expanded at a rapid rate, which means your servers aren't likely to choke on the multiplying data – but your chief privacy officer, CIO or corporate counsel might.

All of this makes now an opportune time to rediscover what most toddlers know intuitively: the joys of destruction. In many cases, you can rid yourself 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.

Yet, unlike a toddler, you should destroy with forethought and care. Get 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 (continually) that your plans are being carried out correctly.

Storage is cheap, but data protection is not, and destroyed data cannot be compromised.

7*) Rethink your data*

Data is simultaneously the most overexposed liability and underexploited asset in the entire enterprise.

For many companies, data liability is potentially vast. Consider: Who owns the data? Who has access to it? What controls are in place? What would be the impact to the organization if it got into the wrong hands?

At the same time, data value is often underexploited and its true worth unrecognized. Are your efforts to safeguard data commensurate with their value?

Sometimes, after companies have ascertained the true value of their data, their tendency is to more forcefully defend it. But this raises another question: Could this data have more value if we loosened the restrictions on it?

LOCK IT UP OR SET IT FREE?

As companies gain visibility into the actual risks and value associated with their information assets, a schism can develop between security-minded professionals who want restriction and profit-minded executives who want liberation. These opposing viewpoints can create dynamic tension that must be resolved. At stake is finding the proper balance between depressing data value with too many restrictions or squandering it with too few.

That balance is far from universal. The unique circumstances, objectives and philosophies of each company can create significantly differing approaches.

Consider, for example, the case of Apple and iTunes. In early 2009, Apple Inc. announced that it planned to remove digital rights management (DRM) restrictions from music sold through its iTunes online music store.[8] Despite the success of iTunes—over six billion tracks sold since its inception—Apple determined that the minuses of the copyright protection mechanism outweighed the plusses.

These drawbacks included negative publicity and customer feedback over the restrictions; software development expenses related to maintaining the effectiveness of the protection in the face of a determined hacker community; and the lack of interoperability between music players and various flavors of DRM protection.[9] In reassessing the tight controls that it had placed on its assets—the music tracks—Apple determined that fewer restrictions would bring more benefits, both to the customer and the company.

Customer convenience also figures into the approach of many credit card companies. Although it may not be readily apparent from the numerous media reports of credit card fraud, the capability actually exists today to almost completely eliminate fraudulent transactions. Various combinations of tokens, passwords, identification, authentication, imbedded chips and biometrics could virtually stop the problem in its tracks. Yet ironclad security measures come at a cost – in this case, affecting the convenience of consumers. Credit card companies realized that in addition to security, customers want speed and convenience in their transactions; they don't want their right to use their card challenged or impeded. Thus, these financial institutions were compelled to strike a balance between the competing needs of security and convenience.

Another illustrative example comes from the fledgling days of the personal computer. In the 1970s, before there was a personal computer on every office desk, word processing systems were ubiquitous in the American workplace. Manufacturers like Wang, CPT and NBI each marketed proprietary, dedicated, specialized machines whose sole function was to handle text input and output. Yet when the IBM personal computer and the Microsoft DOS operating system started to make inroads into corporate America, these manufacturers decided to place their bets on the continuing viability of their closed, proprietary systems, rather than move to the more open platform offered by the PC and DOS system.[10] Other companies that adapted or created word processing programs for the PC, including Word Perfect and, later on, Microsoft Word, were able to capitalize on the shift and capture market share from the legacy word processing companies. Although some of these companies belatedly tried to develop products for the PC platform, the attempt came too late. Wang, CPT and NBI no longer exist today.

Thus, where Apple and credit card companies successfully adapted, the legacy word processing companies went extinct. What was the difference? Primarily, the success and failure of each was predicated on an objective assessment of the true value of their intellectual property. Rather than yield to the instinctive reaction to place additional protections around what they deemed most valuable, the successful companies actually found that they could attain greater profitability and market share by loosening restrictions on their IP.

While this approach certainly won't apply in all cases, companies across the board would be well served by conducting a clearheaded assessment of data value and risk. For example, manufacturers may find protecting their formulas both expensive and ineffectual, since reverse-engineering by competitors has become commonplace. In such an instance, companies might weigh the value of creating protection around the manufacturing process instead of the product.

The key lies in understanding not only what should be locked up and what can be unchained, but also what is actually protectable from a practical standpoint. (Even those items deemed worthy of protection will need to be periodically reassessed, as data and IP typically have a shelf-life.) This evaluation will help companies decide where they can best spend their time and money.

EMERGING FROM THE DARK

Long ago, when a company's valuable information—from Social Security numbers to trade secrets—was stored in locked file cabinets in secure rooms in protected buildings, security and privacy barely deserved a mention in the corporate playbook. Today, when a careless employee or a determined hacker can expose corporate assets to the world in an instant, the issue ranks among the most important facing companies.

Executive and governing branches that have historically been more concerned with top-line growth and bottom-line results will be pleased to learn that a reexamination of security and privacy practices can positively impact both. An energetic spring cleaning can sweep out superfluous data that adds little other than cost, inefficiency and risk. A reassessment of data value can point the way to heretofore unrealized profits. And resisting the urge to continually strengthen protections on all forms of intellectual property can produce surprisingly positive outcomes.

Ted DeZabala *is a principal with Deloitte & Touche LLP and leads its Security & Privacy practice*

Endnotes

1. "Protecting What Matters: The 6th Annual Global Security Survey," Deloitte Development LLC, 2009. http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html
2. For more information on the CIO's role, see "The Risk Intelligent CIO: Becoming a Front-Line IT Leader in a Risky World" at www.deloitte.com/RiskIntelligence.
3. The position of chief data officer is still 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.
4. For more information, see "Building a Secure Workforce: Guard Against Insider Threat," Deloitte Development LLC, 2008. http://www.deloitte.com/dtt/article/0,1002,sid%253D7021%2526cid%253D225950,00.html
5. "Protecting What Matters: The 6th Annual Global Security Survey," Deloitte Development LLC, 2009. http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html
6. "Enterprise @ Risk: 2009 Privacy & Data Protection Survey," Deloitte Development LLC, publication pending.
7. "Protecting What Matters: The 6th Annual Global Security Survey," Deloitte Development LLC, 2009. http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html
8. "Apple Kills iTunes DRM at Its Macworld Finale," internetnews.com, 6 Jan. 2009. http://www.internetnews.com/ec-news/article.php/3794556/Apple+Kills+iTunes+DRM+at+Its+Macworld+Finale.htm
9. "Apple's latest trick to enforce digital rights," Gulf News, 29 Oct. 2008. http://archive.gulfnews.com/articles/07/06/09/10131156.html
10. Amar Bhide, *The Origin and Evolution of New Business*, Oxford University Press, 1999.