Fortifying your defenses
The role of internal audit in assuring data security and privacy

July 2012

At a glance

Data security breaches are increasing. In 2003 there were 21 publicly reported incidents of large-scale loss, theft, or exposure of personally identifiable information. By 2011, the number of incidents had increased to 1,037, and 2012 looks likely to beat that total. No company, no matter how well it has secured its data, is ever "finished" maintaining information security and privacy.

Companies should construct three lines of defense, with internal audit playing a critical role in providing assurance around data security and privacy controls and practices.

pwc

Introduction

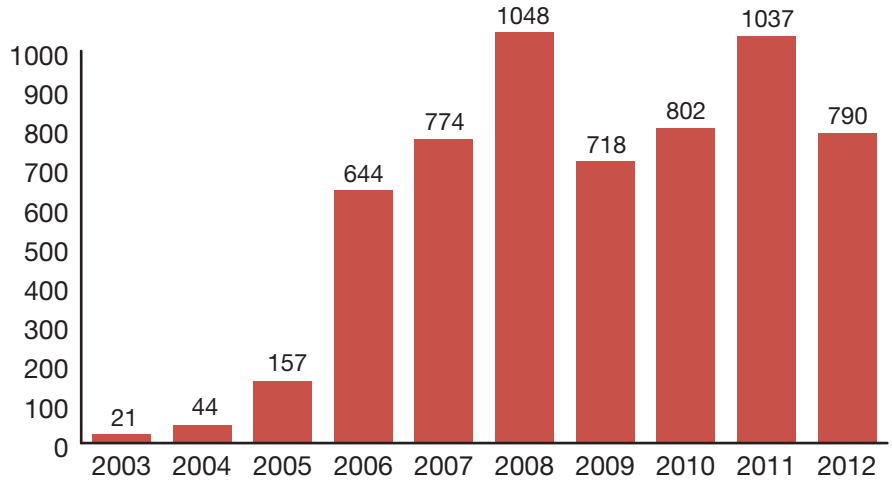
With companies migrating more and more into the digital realm, and people conducting more of their business and personal lives online, data security threats have increased exponentially. User-friendly technologies such as the mobile web and cloud storage are often hacker-friendly as well, opening the door to identity theft, loss of proprietary information, reputational damage, and regulatory involvement. On this playing field, companies must deploy an ever-more robust defense.

Data security breaches increasing

In recent years, theft of computerized customer and employee records has been rising at an alarming rate, with ever-increasing sophistication and audacity. The fact that only the largest of these data breaches are reported widely by the media belies the actual numbers: By one estimate, in 2011 there were 1,037 publicly reported incidents of loss, theft, or exposure of personally identifiable information, up nearly 30% from 2010. In 2003, the number of such incidents was only 21.

Such breaches are costly in terms of dollars, management attention, and company reputation. Fines for a single incident have been as high as $15 million, and court costs, settlements, and other legal bills can reach several times that amount. In 2011, the hacking of Sony's PlayStation Network cost the company more than $171 million in cleanup costs, and analysts predicted the cost of investigations, compensation, lost business, and additional data security investments

Reported incidents over time



Source: Open Security Foundation/DataLossDB.org. Figures for 2012 are the latest available at press time, reflecting incidents reported during the first five months of the year.

could push the total into the billions. Besides the dollar costs, coping with regulators can be an enormous management distraction. To ensure that better security programs are in place, government agencies such as the Federal Trade Commission (FTC) can force companies to operate under consent orders, some of which can extend for 20 years. Companies must then devote resources to monitoring and reporting compliance.

Despite all the attention around data security, the risk of breaches is only likely to get worse, perhaps much worse. Why? First, companies today maintain far greater amounts of personal data on customers and employees than ever before. Second, there is the proliferation of technology. A 2011 study of 583 US companies conducted by the Ponemon Institute (a preeminent research center dedicated to privacy, data protection, and information security policy) found that 28% of digital security breaches occurred remotely, among the mobile workforce. Smartphones and tablet computers are being hacked into in public places, or stolen outright. Many companies also let employees put data on third-party websites such as Google Docs and Dropbox. While these sites let employees share information easily and cost-effectively, they also give hackers more places to poach. Then there are employees who connect to colleagues, friends, and family through Facebook, LinkedIn, Twitter, and other social media, leaving digital trails that make them easy online prey.

The serious hackers, the ones out to steal precious data, are numerous and innovative enough to threaten any business, regardless of how secure they may think their data is. Consider this statistic: Some 90% of the companies surveyed by Ponemon last June had computers that had been breached at least once in the prior 12 months, and 44% viewed their IT infrastructure as still relatively insecure.

If purloined data includes credit card information, birth dates, and Social Security numbers, data thieves can sell it on the black market to parties who can ring up millions of dollars in unauthorized purchases. However, consumer data is not the only target. Many companies have intellectual property in their digital file cabinets, and when this information is accessed by hackers (some of whom may be sponsored by foreign governments), the consequences can be just as disastrous: product knockoffs selling at 70% less than the patented versions, or exposure of proprietary business processes and formulas.

Sometimes the online intrusions produce only insults, not injuries. Some hackers have broken into the computers of well-known companies simply to embarrass them. But even if these "hacktivists" aren't after your data for its own sake, the mandate is the same: Shore up your information security.

28%

% of digital security breaches that occurred remotely, among the mobile workforce

At least 50 countries have enacted data privacy laws, and more are expected to follow.

Penalties, laws, and reputational damage amplified

Because it's so easy for hackers to profit from stealing personally identifiable information—and because consumers and financial institutions usually get stuck with the bill—it's becoming harder for companies to present themselves as hapless victims of cyber intrusions. Government bodies are increasing the penalties they impose on companies whose security flaws allowed such breaches. At least 50 countries have enacted data privacy laws, and more are expected to follow. While some countries (including the US) lack general data privacy laws covering all industries, they often have regulations that apply to certain sectors. For example, US health care providers and insurers must follow privacy guidelines stipulated by the Health Insurance Portability and Accountability Act (HIPAA). Similarly, the Gramm-Leach-Bliley Act of 1999 requires American financial institutions to safeguard sensitive consumer data.

Enforcement of data privacy laws is also increasingly likely. In the US, the FTC and the Department of Health and Human Services both police and enforce data privacy. FTC consent decrees typically force companies to commission independent assessments and report their compliance with those assessments for an extended period.

Reputational damage is also likely to be more severe because information travels far faster today than ever before. A single consumer outburst about a data breach can snowball into mass awareness when it goes viral via social media. Public companies whose data breaches are reported in the press can face the wrath of shareholders. In the three months following one 2009 hacking incident, the affected firm's stock price fell more than 70%.

Companies continue to fall prey to data thieves

The growing number and severity of data security breaches might suggest that most organizations have been lax about the threat, but that is hardly the case. A 2007 study by International Data Corp. (IDC) found that companies across industries spent an average of 19% of their IT budgets on security. US federal agencies alone budgeted $6.5 billion for data security in fiscal 2012, with the Department of Defense accounting for nearly two thirds of that spending. Yet the investments have not been enough to keep the attackers in check.

In our experience, every company has security controls and privacy policies, often quite comprehensive ones. But all too often, no one checks to see if these protocols are being followed. As well, new threats to information security are often overlooked—threats that might demand new procedures and tools.

Consider for a moment one of the more recent ways that hackers have gained access to information on corporate databases: using social media to get past IT administrators, the guardians of much company data. In a number of very recent large breaches, hackers have perused LinkedIn connections to find IT administrators. Then, they locate an administrator's Facebook profile and send him or her an email designed to look as though it came from one of their Facebook friends. Such emails typically provide a link that directs the recipient to log back into Facebook; however, the link is false and instead uploads a file onto the IT administrator's computer, which then provides the hacker a window through which to quickly download sensitive data.

Several large firms have fallen victim to this practice, paying large fines because of the vast number of consumers whose personal data was revealed. Several of these companies are now under 20-year FTC consent decrees to comply with effective data security and privacy practices. These companies had data security and privacy policies and procedures in place, but they hadn't adequately prepared themselves for this new type of attack.

While data thieves have become more inventive, corporate policies, procedures, tools, training, and compliance efforts haven't kept up. In fact, PwC surveys over the last three years have shown that some security capabilities have actually been degrading. For example, in 2011 only 39% of nearly 10,000 executives in 138 countries said they reviewed their privacy policies annually, compared with 52% in 2009. And only 41% had an identity management strategy in 2011, versus 48% in 2009.

No matter how strong its data security policies and controls, a company won't really know the adequacy of its defenses if it doesn't continually verify that those defenses are sound, uncompromised, and applied in a consistent manner. To achieve such assurance, internal audit has to play a far more substantial role in information security than is often the case today. Companies' audit committees must also pay more attention to the problem, and heighten the expectations they place on internal audit regarding information security.

Constructing three lines of defense

To combat the ever-increasing attacks on their data, companies should institute and continually shore up three lines of defense:

1. ***Management.*** Companies that are good at managing information security risks typically assign responsibility for their security regimes at the highest levels of the organization. Management has ownership, responsibility, and accountability for assessing, controlling, and mitigating risks.

2. ***Risk management and compliance functions.*** Risk management functions facilitate and monitor the implementation of effective risk management practices by management, and help risk owners in reporting adequate risk-related information up and down the firm.

3. ***Internal audit.*** The internal audit function provides objective assurance to the board and executive management on how effectively the organization assesses and manages its risks, including the manner in which the first and second lines of defense operate. It is imperative that this line of defense be at least as strong as the first two for critical risk areas: Without a function that provides competent and objective assurance, a company faces real risks of its information privacy practices becoming inadequate or even obsolete. This is a role that internal audit is uniquely positioned to fill. But to do so, it must have the mandate and the resources to match.

The three lines of defense listed above are not unique to data privacy and security, but should be in place and operating at a robust level to deal with any critical risk to the business. For most companies, information security and privacy is one of these critical risks because of its potential to cause financial and reputational damage, and because it is so difficult to mitigate.

On page 7, we describe how one company, LexisNexis, has established these three lines of defense.

The case of LexisNexis

One company that has carefully set up three lines of defense against data breaches is LexisNexis, the $4 billion provider of information to legal, risk management, corporate, government, law enforcement, accounting, and academic markets. Among other reasons, the company collects data on individuals and businesses to help insurance companies monitor risk and employers make better hiring decisions. Protecting data is paramount. The company's three lines of data security defenses play out this way:

1. ***Management.*** The top of the organization sets the tone about the importance of protecting customer data, propagating the message to employees, contractors, vendors, and other parties or individuals who may interact with the data.

2. ***Risk management and compliance.*** LexisNexis's policies go through three levels of development and approval. First, working groups develop data security policies and controls. Next, the policies go through a security review board (chaired by a vice president). Finally, a senior management committee evaluates the policies and issues its approval. Additionally, an independent function is in place to monitor the ongoing effectiveness of policies and controls.

3. ***Objective assurance.*** Controls are periodically tested internally for effectiveness and consistency.

Internal audit's role

In the US, LexisNexis's information Audit & Compliance function is part of a larger group called the Privacy, Security, and Compliance Organization (PSCO), which employs approximately 60 people. PSCO reports to parent company Reed Elsevier's general counsel for intellectual property and information governance.

To establish a strong third line of defense, the PSCO function has put several things in place. The first is a standards framework. The company follows the guidelines, as applicable, established by ISO 27002 for its information security program. However, since ISO 27002 is not all- encompassing, company-specific criteria have been adopted. One example is "customer credentialing," the process of determining that a customer who wants to access the company's products or services has a legitimate business and legal reason for doing so, and that they are who they claim to be. LexisNexis's PSCO continually evaluates the firm's policies and procedures with regards to customer credentialing as well as the other internal controls that make up the information security program.

PSCO stays on top of new risks in three ways, according to Asim Fareeduddin, Senior Director, Audit and Compliance. One is through an annual risk assessment that identifies areas of risk to the company and controls/strategies to mitigate these risks. Another is through assessments that precede the implementation of new information systems. For example, if a business function wants to adopt a new application or product, PSCO, in conjunction with key business stakeholders, ensures that the risks are understood and appropriately mitigated before the product or service goes live.

To keep company data secure, PSCO's most important role is measuring the effectiveness of data security controls. If PSCO finds a weakness after auditing each control, it alerts the relevant business or IT management to remediate it. When the remediation is more involved, Audit & Compliance professionals get to the root of the deficiency and instruct their colleagues in PSCO's Program and Policies group to develop and institute the solution. As Fareeduddin explains, the time from detection of an inadequate control to the implementation of a remediated control is timely and coordinated because his group and the people in Program and Policies both report to the same leadership—i.e., the general counsel. This synergistic organizational structure drives accountability and speeds the organization's ability to remediate deficiencies.

Acting today to protect data: The critical role of internal audit

What the audit committee should expect of internal audit

Given that data security and privacy breaches can cost a company dearly in financial losses and market reputation, the firm's board of directors will want to stay on top of these risks. Keeping the audit committee apprised of emerging risks and effective ways to address them is a key role of internal audit.

In the risk assessment report that it presents to the audit committee, internal audit should highlight the organization's significant data security and privacy risks, including any new risks. Further, it should identify weaknesses in policies and controls. At one global financial services firm, for example, the internal audit function briefs the audit committee about risks it sees within the company, both present and potential. In turn, the company's audit committee often alerts internal audit and management to emerging security issues that directors hear about at other firms with which they are involved. Such two-way exchanges between internal audit and the audit committee are invaluable in keeping the spotlight on emerging information security risks.

Because the nature of information security risks is evolving continuously, internal audit functions need to stay ahead of the threat curve. Internal audit functions should participate in numerous internal and external forums to stay plugged in to emerging security threats, and practices for protecting against them. Networking internally and externally on information security issues is vital to staying vigilant.

Internal audit's role in ensuring that information security threats are properly considered becomes especially important when a company is ready to roll out a new business process, product, or information system. In such initiatives, the project team does not always believe it has time to fully consider data security, particularly if the initiative has fallen behind schedule. If internal audit stays on the sidelines, the company could rush into launching a new process, product, or system without adequate controls.

But recognizing information security threats and creating policies and procedures to defend against them becomes just an abstract exercise if functional managers and field personnel are not following those policies and procedures rigorously and consistently. Internal audit is uniquely positioned to assess whether existing controls are being used, but it must also keep its ear to the ground and move quickly to conduct special audits for new information security threats, which some executives consider as important as regularly scheduled audits.

Overcoming the barriers to internal audit playing an effective role

Effective data privacy and security measures are not easy to effect. In fact, we commonly find four barriers in organizations that try to adopt them.

1. **A mindset that believes adequate controls are already in place.** We frequently hear managers say, "We have firewalls" or "Our access controls are tight" or "We do SOX and we comply with PCI." In fact, Sarbanes-Oxley (SOX) only covers security controls where they coincide with financial reporting, and a company cannot be sure it is compliant with the Payment Card Industry (PCI) standards unless it regularly checks that it is. Companies with inadequate controls should realize that many disastrous security breaches have occurred in companies that had strong firewalls and seemingly tight access controls, and that were in compliance with the latest regulations. Since exposures are changing constantly, policies and controls need to change alongside them.

2. **Cost.** Achieving and maintaining effective information security can cost significant money and effort. When senior managers balk at the expense, it's often because they don't realize the magnitude of the potential downside. To be prudent, they should conduct a cost/benefit analysis that accurately assesses the potential damage of various types of security breach.

3. **Low expectations.** Low expectations of internal audit's capabilities in data privacy hold many companies back from chartering internal audit with this role. Many audit committees and top management teams view the internal audit function as competent in assessing financial controls and sometimes information security controls, but often do not trust their ability to assess information privacy holistically. This concern is not unfounded. Information security practices are complex and ever-changing, and the information privacy field is nascent. The International Association of Privacy Professionals (IAPP) has existed since 2000 but it took until 2008 for its membership to top 5,000. (Today it has more than 10,000 members worldwide.) Few privacy professionals have deep experience, and the supply of techniques and software tools is small. Cyber-security fears are daunting to even the largest companies, and smaller companies are often intimidated by the onerous demands of keeping pace with developments in this complex and fast-changing field. But resigning oneself to being unprepared for threats is not an option. The solution to the lack of privacy and cyber-security knowledge is having the right people: either hiring and training employees to be at the top of their game in this arena and/or outsourcing as needed to experts that have the technical skills in critical aspects of security and privacy.

4. **Fragmented responsibilities.** The job of maintaining effective information security controls is often split among a company's legal, finance, and IT functions, as well as its business heads. When that happens, it's almost certain that some things will fall between the cracks. The solution is to assign a single point of responsibility for information security. This individual role could be an information security officer, the general counsel, the chief risk officer, or an executive on the management committee. Less important than determining who should be responsible for information security is making sure that someone is responsible, and that he or she has access to the right resources to assess the risks, and the authority to address them.

Depending upon the nature of the breach (for example, the scale and type of information lost), the average loss in brand value ranged from $184 million to more than $330 million.

Why internal audit should act

As stated in the opening pages of this paper, data breaches are costly in terms of dollars and management time, and can cause significant damage to a company's brand. A 2011 study conducted by the Ponemon Institute and sponsored by Experian Data Breach Resolution reported that it takes an average of one year to restore a company's reputation after a significant data breach. For the study, Ponemon interviewed 850 senior-level executives, who provided both an estimate of the value of their organization's brand/reputation (ranging in scale from less than $1 million to greater than $10 billion) and an estimate of the average loss in brand value from a data breach. Depending upon the nature of the breach (for example, the scale and type of information lost), the average loss in brand value ranged from $184 million to more than $330 million. The minimum brand loss was 12%.

The frequency of reported data breaches remains resolutely high, and the cost of dealing with breaches—especially large ones—is substantial. Add to that the potential damage to a firm's reputation and it's no wonder that many firms are doing all they can to prevent illegitimate exposure of their data, especially personally identifiable information.

But even when companies have instituted all the proper controls, as countless already have, failures are common. Many breaches happen because users choose weak passwords that are easy for them to remember but also easy for others to guess—this despite company policies that require strong passwords. Even when companies brief their employees about information security practices, the training is often not retained. Tests have shown that even one day after learning how to avoid phishing scams, as many as 50% of employees will fall victim to them.

All of this means that companies need to put in place a strong third line of defense. This is the assurance role that internal audit is uniquely positioned to master. For new and evolving risks such as data security and privacy, such mastery requires that internal audit raise its game with new skills and tools for making sure business functions are implementing the right processes and controls to secure the company's most vital information.

PwC's US Assurance practice

PwC provides clients with a range of internal audit services, from consulting on performance improvement to sourcing the entire function or conducting audits in highly technical and specialized areas, such as data security and privacy.

In addition to supporting client internal audit activities, PwC provides services with a higher level of assurance, especially in areas such as security and privacy, where third parties require a heightened level of comfort.

www.pwc.com

To have a deeper conversation about how this subject may affect your business, please contact:

Dean Simone, Partner
US Risk Assurance Leader
dean.c.simone@us.pwc.com
T: (267) 330 2070

Jason Pett, Partner
US Internal Audit Leader
jason.pett@us.pwc.com
T: (410) 659 3380

Carolyn Holcomb, Partner
Third Party Assurance Privacy Leader
carolyn.c.holcomb@us.pwc.com
T: (678) 419 1696

David Roath, Partner
US IT Risk & Security Assurance Leader
david.roath@us.pwc.com
T: (646) 471 5876

Neelam Sharma, Director
US Risk Assurance Strategy,
Sales, and Marketing Leader
neelam.sharma@us.pwc.com
T: (973) 236 4963