

10 Minutes

on data and identity theft



October 2008

A collaborative business world's Achilles' heel

Highlights

The Federal Trade Commission estimates that the annual losses to business from data and identity theft amount to almost \$50 billion.

Nearly 90% of our ethical hacking tests are successful in gaining access to highly sensitive information.

High profits and sophisticated techniques are making data and identity theft more lucrative, easier to conduct, and more difficult to police. Weak international laws make it difficult to prosecute thieves.

Identifying sensitive data and safeguarding it end-to-end is the basis of a strong data-protection program.

Protection of sensitive information is an overall business issue, not just an IT issue.

The portability and accessibility of information are crucial components of a collaborative, interconnected business world. However, the problem with sharing information is that it can get shared with the wrong people.

Whenever highly sensitive or regulated information is lost, misused, or compromised, it falls under the banner of data and identity theft. Intellectual property, personally identifiable information (birth dates, Social Security numbers, addresses, etc.), trade secrets, employee and customer data, and payment card data are all examples of sensitive or regulated information.

Data losses can be devastating. Besides potential fines and lawsuits, security breaches can have a long-term impact on a company's brand and reputation. Having strong data safeguards in place can help secure a company's reputation, competitiveness, and financial well-being.

Why data and identity theft is a growing problem:

1. Data and identity theft is being conducted by organized, motivated, and sophisticated groups that are well compensated for their success.
2. Today's business models are based on global collaboration networks that share sensitive information through a variety of methods—potentially leaving companies more exposed.
3. The compromise or loss of intellectual property has led to product counterfeiting, fraud, and loss of revenue. It has had lasting negative effects on brand value and corporate reputation.
4. Current company information-protection measures are often inadequate to detect or prevent targeted hacking or electronic espionage activities.
5. Compliance with industry standards (e.g., Payment Card Industry) or regulatory standards (e.g., Sarbanes-Oxley) can create a false sense of security. Regulatory standards are very specific in scope, and a company's most sensitive data may not be covered by a formal standard.

At a glance

The old way of viewing data theft:

- “This will never happen to us.”
- Disorganized, amateurish hackers working out of their homes, doing it for “fun” rather than money.
- “This is an IT issue.”
- Negligible impact on customers, employees, and company costs.
- “We trust our employees to secure our information.”
- Risk exposures are small and manageable.
- “We passed our audit, so we’re safe.”

The new way of viewing it:

- Companies of all sizes and across all industries confront a real, growing, and strategic risk from data and identity theft.
- Theft is a lucrative business for sophisticated, organized criminal enterprises worldwide.
- Data loss commonly occurs through physical loss, data exchanges, fraud, and human error, rather than just IT breaches.
- Loss of personal data leaves customers and employees at risk of fraud and personal identity theft.
- Employees and collaboration networks are the most common data leak sources.
- Risks are substantial, including compromise of company IT systems, customer lawsuits, erosion of brand reputation, loss of customers, government fines, and new regulation.
- Data protection is a CEO-level concern.

01

Your data? Here, there, and everywhere

The global nature of business has made companies more vulnerable to data and identity theft, since the sharing of information with business partners and third parties has increased opportunities for loss, misuse, or compromise.

The traditional view is that information is confined within a company, and that securing your firewall and perimeter can provide all the necessary protection. That has changed. Data is portable, and can be easily transferred and replicated. Though data centers and servers can provide a higher level of information protection, the preponderance of mobile devices—such as laptops, PDAs, and plug-in drives—are less secure and increase the risk of theft. Once data is distributed, all devices that access the data are potential breach points.

Also, business partners that do not have adequate information-protection standards in place make data more vulnerable, since your data often becomes *their* data.

According to PwC's *2008 Global State of Information Security Study*—a worldwide survey of more than 7,000 IT and information security professionals conducted with *CIO* and *CSO* magazines—71% of respondents stated that their organizations do not maintain an accurate inventory of where high-value data is stored.

Only about half of the respondents said that their company security policies address the protection, disclosure, and destruction of data. And while survey results suggest that the majority of companies worldwide encrypt data in transmission, far fewer appear to encrypt data at rest in databases, laptops, file shares, backup tapes, and removable media.

Boom in theft and fraud

The nature of the crime makes it difficult to prosecute. The anonymity in committing data and identity theft makes it attractive to thieves, as it can be committed miles, even countries, away. All the criminal needs is access to a computer.

Identity theft protections vary greatly between countries, and international patent protections on intellectual property are weak and inconsistent. This has caused a boom in theft and fraud, since criminals can obtain big rewards without significant risk of being caught and prosecuted.

02

Don't assume compliance equals security

An unpleasant fact is that most company information-protection measures are compliance-focused and inadequate against today's sophisticated threats. Simply stated, compliance is merely the minimum level of information protection needed.

Even compliance with regulations such as SOX, GLBA, or HIPAA, or industry standards such as PCI, can leave companies vulnerable and give them a false sense of security.

Our experience in conducting security assessments for clients has shown that, across industries, even those who follow compliance standards or have information-protection policies in place are still at risk of data and identity theft.

Industry: telecommunications. We accessed approximately 250,000 customer order records—including names, addresses, birth dates, Social Security numbers (SSNs), and driver's license numbers—from the Internet.

Industry: entertainment. Also using the Internet, we gained access to unreleased content, as well as the salaries, SSNs, and contact information of various employees.

Industry: financial services. With only physical access to the premises, we were able to obtain customer information from a shared department folder. While the data was protected within the mainframe, it had been replicated by the marketing department, where we found it.

Industry: healthcare. Using contractor-level access, 81 million records of insurance claims, customer names, and SSNs were obtained by exploiting weak passwords.

Industry: retail. Posing as members of the company's records management team, we requested and were given original copies of job applications, which included the applicants' SSNs, birth dates, and more.

While compliance provides a safety net, it is still a net with holes. By focusing on risks and risk exposures rather than just compliance, companies can raise their information-protection level to where it needs to be.

03

The impact of not being prepared

The potential impact of data and identity theft is huge. Should an incident occur, companies can expect to face direct financial impacts from investigations, legal fees, credit monitoring services for victims, reissuing of credit cards, government fines, and regulatory sanctions.

Companies may also face significant impacts in terms of brand damage, negative publicity, customer defections, lost revenue, and loss of consumer trust.

When data and identify theft involves consumer information, the Federal Trade Commission can levy fines and mandate that the company conduct independent assessments of its information-protection program for up to twenty years.

In PwC's 2008 global security study, of the respondents who had experienced a security incident during the previous twelve months:

- Four out of ten reported a resulting financial loss.
- Almost one-third classified their incident as intellectual property theft.
- Over one-quarter said the incident resulted in brand/reputation damage.

Many respondents agreed that information security spending will continue to increase. The question is: Where should the company focus its security budget in order to best reduce risk?

This requires knowing, often under constantly changing circumstances, precisely where the greatest data risks exist—both within the company and its collaborative network—and concentrating spending in those areas.

Yet, for many companies, identifying these exposures has not been a priority. Only 44% of survey respondents said their company conducts an enterprise risk assessment periodically. Just 24% said they prioritize data and information assets according to risk level on a continuous basis. And 30% admitted they do not classify data and information assets at all.

Most surprisingly, only 25% reported that their security spending is completely aligned with the company's business objectives.

04

Know where your most sensitive data is—and protect it

With increased data portability, bigger incentives for theft, and greater sophistication of thieves, the C-suite should consider several questions when assessing company information protection:

Where is our most sensitive data and who has access to it?

What regulations and standards apply to our data?

Have we been a target of data and identity theft?

Does our collaborative business model put our data at risk?

Do our employees, customers, and business partners understand their role in protecting sensitive information?

Do our safeguards provide data with end-to-end protection, even on mobile devices?

Have a data protection strategy in place

An effective approach to mitigating data and identity theft risk would include these elements:

- Develop and implement a detailed information-protection plan.

- Identify and classify data according to sensitivity and risk. Know where it resides and flows.
- Understand the threats that are specific to your data and your organization.
- Implement protection capabilities to safeguard your sensitive data end-to-end.
- Test your protection capabilities. Monitor them continually and update them as necessary.
- Plan for a controlled and coordinated response to incidents when they occur.

Strong information protection provides greater freedom to pursue opportunities

Having the right information-protection strategy can create advantage over competitors, and minimize the financial and reputational risk the company faces. Importantly, having confidence in your information protection allows the company greater freedom in pushing the envelope of its business.

Upcoming 10Minutes topics

Why climate change matters today

Concerns over energy security and costs are heating to uncomfortable levels, both at the gas pumps and in the boardrooms. Meanwhile, consumers, employees, and communities are increasingly expecting action from businesses. Climate change has become a matter of managing risks, costs, and reputation. 10Minutes explores how you can link your response to climate change more strongly to your business strategy and your corporate performance.

Competing for knowledge workers more intelligently

A limited pool of knowledge workers means that organizations need to find smarter ways to compete for these professionals. 10Minutes looks at how companies are redefining their approach to people management by not only looking outward to find the best and brightest, but also looking inward to create an environment where they can thrive.

The changing face of financial reporting

The income statement and balance sheet—foundations of public financial reporting and financial analysis—are not optimally serving investors and analysts. This has caught the standard setters' attention and they are considering major changes to basic form and content. 10Minutes provides an update on the state of play.

Improving the integrity of the supply chain

Companies reeling from supply chain breakdowns are discovering that aggressive cost cutting created new risks, as demonstrated by product recalls. It has become necessary to enhance the integrity of supply chains. Yet tough economic times are ensuring continued emphasis on cost reduction. 10Minutes discusses how to balance a competitive cost structure with investment in the future.

How PwC can help

To have a deeper discussion about data and identity theft and its potential impacts, please contact:

Dennis Nally
US Chairman and Senior Partner
PwC
Phone: 646-471-7293
Email: dennis.nally@us.pwc.com

Juan Pujadas
US Advisory Leader and Managing Partner
PwC
Phone: 646-471-7782
Email: juan.pujadas@us.pwc.com

Gary Loveland
Principal, National Security Practice Leader
PwC
Phone: 949-437-5380
Email: gary.loveland@us.pwc.com

Tell us how you like 10Minutes and what topics you would like to hear more about. Just send an email to: 10Minutes@us.pwc.com

This publication is printed on Domtar Cougar stock, containing 10% post consumer waste fiber. It is certified by the Forest Stewardship Council (FSC), and a premier member of the Domtar EarthChoice family.