



## Table of contents

	<u><b>3</b></u>
Introduction: the changing security game	
	<u><b>4</b></u>
Gambling with your brand image	
	<u><b>5</b></u>
Sizing up enterprise-wide vulnerabilities	
	<u><b>8</b></u>
Stack the deck in your favor: fundamentals of risk management	
	<u><b>10</b></u>
Hedging your security solution bet: what to look for in a provider	
	<u><b>11</b></u>
Conclusion: your deal	



## Introduction: the changing security game

Given the unknowns in business, decision makers often feel like they're gambling as they make educated guesses to set the direction for their company. Their success is based heavily on their ability to weigh risks versus rewards, and to consistently place and win strategic bets. When the variables are known and opponents follow the same rules, it's reasonable to expect that calculated wagers will pay off. But in areas like security, cheaters are rampant and the rules are constantly changing. As a result, it's becoming more and more difficult for chief information officers (CIOs) and chief information security officers (CISOs) to know where to focus resources to protect confidential information and comply with government regulations.

Although there's no such thing as a sure bet to protect critical information, there are approaches that can help to significantly reduce exposure to risks and meet security compliance obligations. What's required is a security approach that's integrated with your business strategy. Without this, you're risking a lot more than downtime or the simple loss of information assets or capital—you may be betting your brand image.



## Gambling with your brand image

---

*Over 98 million consumers have been notified of potential security breaches regarding personal information since February 2005.*

---

*Today's headlines tell the stories of companies that have lost big to security breaches.*


Credit agencies. Government agencies. Financial services companies. Retailers. Higher-education institutions. Healthcare providers. In recent years, in virtually every industry, organizations of all sizes have paid a heavy price for security breaches or the loss of customer or company data.

Consider these statistics. Over 98 million consumers have been notified of potential security breaches regarding personal information since February 2005.<sup>1</sup>

According to respondents to a Computer Security Institute (CSI) and FBI survey, the cost of a laptop or mobile device theft or loss increased nearly 33 percent between 2005 and 2006 to approximately US\$30,000 per incident.<sup>2</sup> This same survey showed, as in prior years, that theft of proprietary information caused the greatest financial loss, with an average loss of US\$2.7 million.<sup>3</sup>

Given the implications of security threats to companies' customers and stakeholders, security incidents are closely scrutinized by the media—compounding their costs. And today's headlines tell the stories of numerous companies that have lost big because of high-profile security breaches.

In some instances, the breaches were process related. For example, a consumer data broker paid US\$15 million to settle data security breach charges. The case focused the news media spotlight directly on the company's failure to protect consumers' privacy rights against identity thieves who used administrative sleights of hand to bypass lax security.



In another situation, an unsecured network gave cyber thieves access to 40 million debit and credit card accounts in a case involving a credit card processing company. The repercussions of the breach were felt not only by the credit card processing company, but also by the credit card providers that used the processing company—and feared damage to their brands.

Even simple employee errors can cause concern. In one case, a major shipping company lost a banking client's non-encrypted computer tape that contained the personal data of nearly 100,000 customers. The oversight exposes the vulnerability of private data.

## Sizing up enterprise-wide vulnerabilities

---

*Most organizations mainly focus security on keeping the bad guys out.*

Chances are that your current security approach is mainly focused on keeping the bad guys out. And if your company is like many organizations, this involves using multiple point products and ad hoc solutions that rely on passwords to guard the perimeters of specific applications. Each department or division may have its own security approach, with no integration. This approach does not provide a way to address security across applications, processes and the extended enterprise. To take on today's security and risk issues, you need to rethink how

you play the rapidly changing security game. The first move is to understand who and what you're up against.

### **From hustlers to honest employees**

Unfortunately, there is no shortage of people inside and outside your organization who are ready to exploit security vulnerabilities, or even expose them. Hustlers in the security game range from professional hackers to careless or disgruntled employees. They don't fit a single profile, and there isn't one method you can use to stop them all.

---

*To take on today's security and risk issues, you need to rethink how you play the security game.*



---

*From careless or disgruntled employees to cyber criminals, people present difficult security challenges.*

Today, hackers often work as professionals in criminal gangs, and the time it takes for them to exploit weaknesses is shortening dramatically. Serious losses can also come from the actions of disgruntled employees and business associates, such as the theft of intellectual property or confidential information. Security breaches can also result from careless employee mistakes, such as misplacing a data tape, losing a laptop or allowing unauthorized employees access to a secure area.

**More data assets on the table**

Because of rapid advances in storage technology and capacity—and the corresponding exponential growth of data—security and risk management have become critical concerns. While the resulting information—which provides greater insight into your operations and

customers—can be a jackpot, it also exposes your organization to compliance and privacy issues. And the proliferation of high-capacity portable storage devices, such as personal digital assistants (PDAs), laptops, removable media and cell phones, raises the challenge.

To improve competitiveness, customer service and productivity, your organization must share its data with wider groups of users—often across numerous geographies and on more types of devices than ever before. As you provide more and more employees, customers, suppliers, business partners, contractors and associates access to your data, you increase the odds of a data breach or loss. And according to the U.S. Federal Trade Commission, identity theft has topped the list of consumers' complaints five years running.

---

*While the accumulation of customer and operational data can be a jackpot, it also exposes the organization to compliance and privacy issues.*

---

*Keeping tabs on important physical assets and vulnerable business areas—in addition to securing the network—is critical to mitigating risk.*

Customers expect you to protect their data like it's your own personal information. When policies fail and you show their hand, you risk significant losses. To complicate things even more, telecommuting technologies and outsourcing arrangements that encourage remote workforces make security based on physical control much more difficult. As a result, you must have sophisticated processes for data protection, sharing and backup.

---

*Keeping up with today's rules and regulations requires a host of process considerations on top of security measures.*

#### **Monitoring the floor**

Your risk mitigation strategy and security can't stop at the edge of the network. To mitigate physical threats and reduce losses due to theft—whether those losses are accidental or criminal—you must also keep close tabs on important physical assets and vulnerable business areas across multiple locations and even continents. The challenge is finding a solution that is manageable and that can integrate with existing and future technology without breaking the bank.

#### **New rules for an already complex game**

Depending on where you do business or what industry you're in, keeping up with the rules requires a host of process considerations on top of basic security measures. For example, if you are a publicly traded company in the United States you must comply with Sarbanes-Oxley Act regulations, and healthcare organizations must meet the standards set by the Health Insurance Portability and Accountability Act (HIPAA). Moreover, beginning with California in 2003, more than 30 states have enacted legislation requiring companies to notify customers if their personal data has been compromised.<sup>4</sup> Additionally, effective January 2007, European financial organizations will have to comply with Basel II Capital Accord regulations.



## Stack the deck in your favor: fundamentals of risk management

---

*To determine your areas of risk, you must look across all of your business processes to find potential security exposures.*

Security is now critical to achieving sustainable growth and innovation, and to effectively mitigate risks you must integrate security into your overall business strategy. How can you do this? By developing your security strategy as part of your business model and processes. Before you can make a good bet on a security approach, however, you first need to assess what is acceptable risk in any given area of the business.

### **Determining your risk tolerance limit**

---

*To effectively mitigate risks, you must integrate security into your overall business strategy.*

Operational. Business. Financial. Risk comes in many forms and threats, and vulnerabilities are constantly evolving. To begin an assessment of your areas of risk, you must look across your business processes and determine where you have potential security exposures. By identifying the vulnerabilities and exposures for relevant processes, you can begin to understand the potential impact of associated security breaches.

Based on what you learn from your process assessment, you can establish betting limits, or the level of risk that your organization can tolerate, in each process area. The level will vary by process—taking into account the importance of a given process or application to your revenue flow or profitability, the value of the assets involved, regulatory compliance requirements and concerns, and other factors related to your organization's size and industry. Equipped with this knowledge, it is then possible to rank the exposures that you've identified based on their impacts and your risk tolerance. This enables you to prioritize and justify security expenditures based on business priorities. When it comes to reducing vulnerabilities and risks, you can never assume you have the upper hand. That's why it's important to continually try to identify and assess vulnerabilities, as well as policies or regulations that you must comply with across the extended enterprise.

---

*Security solutions today must go beyond individual security products—they must be integrated to provide interoperable, enterprise-level solutions.*

---

*Since business processes are constantly changing, you must revisit processes regularly to address new vulnerabilities.*

### **Improving your security process management hand**

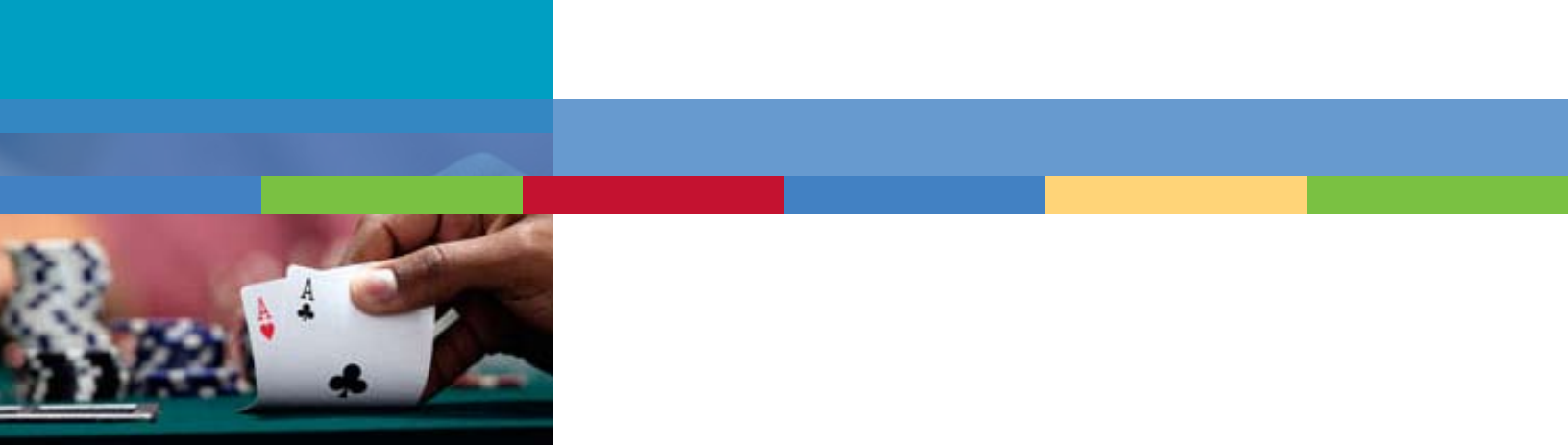
Virtually every company has implemented infrastructure security products; however, individual products in and of themselves are not enough. Products must be integrated to provide enterprise-level solutions that interoperate and deliver capabilities above and beyond a collection of point products. Equally important are solid processes and controls regarding access to and use of information.

A significant component of a good security solution hand entails a couple of aces like managing and provisioning user accounts to carefully control access rights to confidential or mission-critical data. Given the scope of enterprise systems and the risks and challenges associated with manual processes (for example, user error, malfeasance and slow provisioning), the more security

processes you can automate, the better. Automated tools that can detect unusual behaviors by comparing a user's current and historical usage patterns are already in the marketplace. By divvying up authority—based on least possible privilege—and by splitting roles—such as auditing and administration—you create checks and balances to detect potential fraud.

### **Playing it safe**

Threat mitigation is an ongoing process that begins with effectively placing your bets and defining and implementing your security policies and infrastructure. Once you identify your vulnerabilities, you can then calculate the business impact of a breach and prioritize and address potential holes based on risk premiums. You can also carefully evaluate your options to make sure you implement the best solution for long-term business needs. And since business processes and solutions are constantly changing, you must reshuffle the deck and deal again regularly.



## Hedging your security solution bet: what to look for in a provider

---

*A provider that can help you address the gamut of vulnerabilities and threats can give you the upper hand on risks.*

When it comes to managing security risks across a large enterprise or organization, taking a chance on a long-shot provider or solution makes no business sense. A provider that can help you address the gamut of vulnerabilities and threats can give you the upper hand on risks. Look for a vendor that can help you prioritize potential exposures based on the highest business risks and recommend appropriate solutions. And look for one that has a proven track record, has been evaluated by analysts and has a wide install base across an array of industries. Also look for customizable solutions that can address security challenges such as the following:

- **People.** Automated identity management solutions are essential to provide processes for recognizing and monitoring users, for granting or restricting access to applications and data, and for managing and provisioning user accounts. By gaining visibility into who has access to what applications, instituting single sign-on and eliminating cumbersome manual processes, you can prevent unauthorized access to information and assets while improving user productivity and reducing security costs.

- **Data.** Technology and processes for protecting data, including backup and security-rich data-sharing procedures, are critical. Leading-edge storage solutions should include built-in encryption capabilities and key management to facilitate secure data sharing among business associates and suppliers. Also look for solutions that protect backup data without affecting processes and applications.
- **Perimeter.** Network security can protect the perimeter of your IT enterprise by detecting malicious software, limiting access to your network to authorized users, and checking workstations for compliance with security policies. Additionally, a digital video surveillance solution can help enable comprehensive and cost-effective video monitoring and analysis. An effective solution should enable rapid access to and retrieval of digital video content. Leading-edge technology in “smart surveillance” can provide added levels of security.

---

*“Security has become a business requirement and few of today’s security vendors know how to play in this high-stakes game. IBM certainly does.”*

—Jon Oltsik, senior analyst,  
Enterprise Strategy Group<sup>®</sup>

---

---

*“As security transitions from a tactical IT annoyance to a strategic enterprise business requirement, IBM is poised to win big.”*

—Jon Oltsik, senior analyst,  
Enterprise Strategy Group<sup>®</sup>

---

## Conclusion: your deal

In the security game, small errors can result in big losses. IBM offers security solutions that include a full spectrum of leading-edge security technology and services that span both logical and physical security. Our more than 3,500 professionals with deep security and industry experience can help your company develop a strategic approach to security to solve even the most complex challenges. And our approach is designed to help you control security costs while managing risk to a level that’s acceptable to your business.

Although there is no wild card for addressing security challenges, we can help you systematically close security gaps and integrate your security approach with your business strategy. With strong security policies, procedures and technologies in place, you not only can remove your brand reputation from the stakes—you can also pursue growth initiatives knowing that data and systems are secure.

### **For more information**

To learn more about IBM’s views regarding security solutions and IBM security solutions, contact your IBM representative or visit:

**[ibm.com/solutions/itsolutions/doc/content/solution/1497534131.html](http://ibm.com/solutions/itsolutions/doc/content/solution/1497534131.html)**



© Copyright IBM Corporation 2006

IBM Corporation  
Software Group  
New Orchard Road  
Armonk, New York 10504  
U.S.A.

Produced in the United States of America  
12-06  
All Rights Reserved

IBM and the IBM logo are trademarks of International Business Machines Corporation in the United States, other countries or both.

Other company, product and service names may be trademarks or registered trademarks or service marks of others.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

This publication contains other-company Internet addresses. IBM is not responsible for information found on these Web sites.

- 
- 1 [www.privacyrights.org](http://www.privacyrights.org).
  - 2 2006 CSI/FBI Computer Crime and Security Survey; <http://www.gocsi.com>.
  - 3 Ibid.
  - 4 [www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf).
  - 5 Oltsik, Jon; *IBM Buys Consul and Bolsters Its Enterprise Security Portfolio*; Enterprise Strategy Group; December 7, 2006.
  - 6 Ibid.