IBM Global Business Services
Executive Report

Strategy and Transformation

IBM Institute for Business Value

Managing threats in the digital age

Addressing security, risk and compliance in the C-suite

IBM Institute for Business Value

IBM Global Business Services, through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive report is part of an ongoing commitment by IBM Global Business Services to provide analysis and viewpoints that help companies realize business value. You may contact the authors or send an e-mail to *iibv@us.ibm.com* for more information. Additional studies from the IBM Institute for Business Value can be found at *ibm.com/iibv*

By John Lainhart, Steve Robinson and Marc van Zadelhoff

Recent media attention has highlighted the proliferation of security breaches affecting enterprises across numerous industries. These security failures have not only resulted in significant expense to the affected enterprises, but have significantly damaged consumer trust and brand reputation. No longer relegated to the domain of the IT organization, the topic of security is now unquestionably a C-suite priority. Organizations need to move toward a more systematic and proactive approach to addressing security threats and managing compliance requirements in today's information-driven economy.

As the world becomes more digitized and interconnected, the door to emerging threats and leaks has opened wider. Today, there are billions of RFID tags for items including products, passports, buildings and animals. With more than two billion Internet users and cellular phone subscriptions passing the 5 billion mark at the end of 2010, nearly one in three people worldwide surf the Internet.[1] More than 50 billion objects are expected to be digitally connected by 2020, including cars, appliances and cameras.[2] Intensifying this complex mix, the amount of digital information created and replicated in the world will grow to an almost inconceivable 35 trillion gigabytes by 2020.[3]

Not only has the amount of data increased, but the corresponding value of digital assets has increased as well. Sensitive customer information, intellectual property and even the control of key machinery are all increasingly found in electronic formats. Attacks that affect these assets are much more likely to have a material impact on the entire organization, as opposed to simply the IT department. Take, for example, the Stuxnet virus, which caused process controllers responsible for refining uranium to be altered, and degraded the ability to safely process and control this highly dangerous material.[4] This incident demonstrates that targeted action against an organization's technological infrastructure can clearly impact critical operations.

Even more pressing than the undeniable proliferation of data, devices and connections, other factors are making it critical for enterprises to change how they manage security and compliance. The valuable data embedded within organizations is a target of people who attack systems, whether for criminal reasons such as economic gain, personal reasons such as revenge or frustration, or political reasons such as terrorism. The damage to information and information processing infrastructure is occurring more often and with a high degree of "professionalism" in increasingly organized ways.

So it has become more important, yet more difficult, to secure and protect critical information and related assets. Security has quickly ascended the attention scale and is undeniably an emerging C-level issue, whether it's the CMO evaluating the potential risk to the brand, the CFO understanding the financial implications of adverse events or the COO assessing the impact of IT systems disruptions on ongoing operations. Developing *security intelligence* – the ability to proactively predict, identify and react to potential threats – will take on a new priority in the digital age.

Security challenges are greater than ever

With the increase in data, devices and connections, security challenges are increasing in number and scope. They fall into three major categories: external threats, internal threats and compliance requirements.

External threats

We have recently seen a proliferation of external attacks against major companies and government organizations. In the past, these threats have come from individuals working independently. However, these attacks have become increasingly more coordinated, and launched by groups ranging from criminal enterprises to organized collections of hackers or "hacktivists," to criminal enterprises and even state-sponsored entities. Attackers' motivations are no longer limited to seeking profit, but sometimes can include prestige or espionage. These attacks have targeted ever-more critical organizational assets, including customer databases, intellectual property and even physical assets that are driven by information systems.

These external attacks have significant financial consequences. For example, the release of customer data from Epsilon compromised the email addresses of millions of consumers and directly affected numerous corporate clients. The costs of initial clean-up and longer-term litigation risks is estimated in the hundreds of millions of dollars.[5] Many other companies in the financial services, media and entertainment, retail and telecommunications industries have recently reported similar types of breaches of customers' personal and financial information, each resulting in notable IT, legal and regulatory costs.

Internal threats

In many situations, breaches in information security are not perpetuated by external parties, but by insiders. Insiders today can be employees, contractors, consultants and even partners and service providers. These breaches range from careless behavior and administrative mistakes (such as giving away their passwords to others, losing back-up tapes or laptops or inadvertently releasing sensitive information), to deliberate actions taken by disgruntled employees.

These actions can be as dangerous as external attacks. In one situation, the Wikileaks incident, which involved the unauthorized release of classified records, has reportedly cost the U.S. government millions of dollars and damaged relations with foreign governments around the world.[6]

Compliance requirements

Enterprises are being asked to address a steadily increasing number of national, industry and local mandates related to security that each have their own standards and reporting requirements. The many examples include: U.S. Sarbanes-Oxley (SOX), J-SOX, COSO, COBIT, various ISO/IEC international standards, U.S. HIPAA/HITECH, EU Privacy Directive, India Data Security and Privacy Standards, PCI DSS and BASEL II. Following these mandates often takes a significant amount of time and effort to prioritize issues, develop appropriate policies and controls, and monitor compliance.

C-suite priorities are feeling the impact

Threats and compliance requirements will have a significant impact on the ability of individuals in the C-suite to deliver on their key priorities. As technology plays an increasingly important role, the challenges associated with information security go well beyond the province of the CIO. Our discussions with more than 13,000 C-suite executives since 2008 show that each member of the executive team is impacted by security issues (see Figure 1).

Although different C-suite executives do need to have higher priorities for some security challenges than others, enterprises cannot afford to ignore the need to act in a cohesive way to address today's security risks. Responsibilities for security issues that may have been more clearly delineated in the past now overlap organizational silos, as does the potential damage if things go wrong.

For example, Chief Marketing Officers (CMOs) focusing keenly on brand enhancement could find themselves at risk of losing customer trust and brand reputation if security violations result in the loss of personal information. Unquestionably, this would be a prime risk for any enterprise and a tarnished reputation would require action by the entire C-suite.

Examples of security risks managed primarily by other members of the boardroom include:

- *Chief Executive Officers (CEOs)* need to be concerned about whether their intellectual property and business sensitive data are subject to misappropriation by insiders or outside parties. These types of intrusions can have significant impact in terms of potential loss of market share and reputation, operational risks associated with regulatory shutdowns and potential criminal charges.

	CEO	CFO/COO	CIO	CHRO	CMO
CxO priority	• Maintain competitive differentiation	• Comply with regulations	• Expand use of mobile devices	• Enable global labor flexibility	• Enhance the brand
Security risks	• Misappropriation of intellectual property • Misappropriation of business sensitive data	• Failure to address regulatory requirements	• Data proliferation • Unsecured endpoints and inappropriate access	• Release of sensitive data • Careless insider behavior	• Stolen personal information from customers or employees
Potential impact	• Loss of market share and reputation • Criminal charges	• Audit failure • Fines, restitutions and criminal charges	• Loss of data confidentiality, integrity and/or availability	• Violation of employee privacy	• Loss of customer trust • Loss of brand reputation

Source: Over 13,000 face-to-face executive interviews conducted as part of IBM Institute for Business Value C-level studies.

Figure 1: **Addressing security and compliance needs is a priority across the C-suite.**

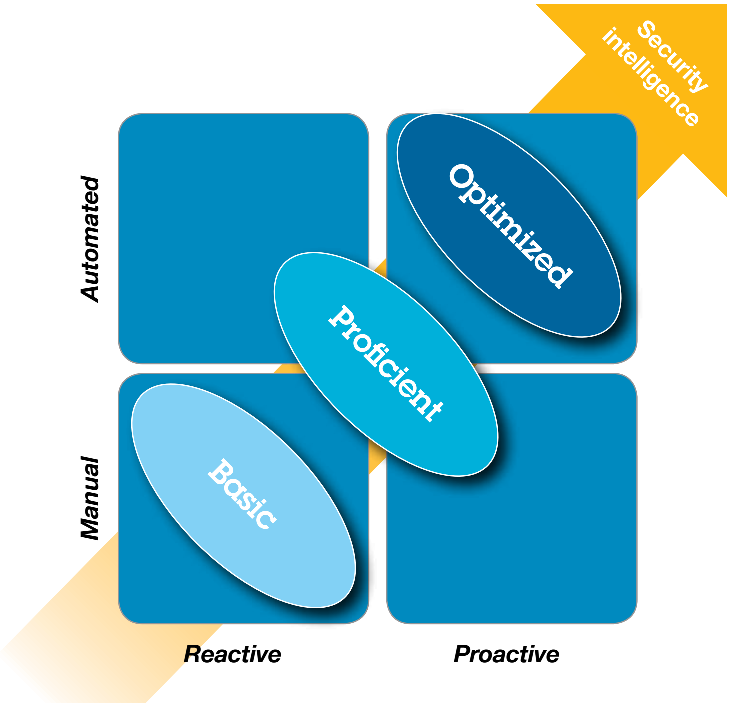
- *Chief Financial Officers (CFOs)* particularly need to address regulatory guidelines. Failure to comply with the security provisions of these guidelines could result in audit failure and resulting penalties for organizations, as well as criminal charges for themselves and their organizations.
- *Chief Information Officers (CIOs)* looking to increase organizational flexibility and mobility have to address challenges regarding data proliferation, the increase in the number of unsecured endpoints and inappropriate access to data. Any of these issues could result in the loss of data confidentiality, integrity or availability.
- *Chief Human Resource Officers (CHROs)*, as they move to increase the flexibility of their labor forces, need to be aware of the potential for the release of sensitive data, as well as potentially careless insider behavior that could result in the violation of employee privacy.

In short, security issues are no longer the sole responsibility of the CIO, nor can they just be delegated to a Chief Information Security Officer. They require attention and action from the entire C-suite.

Building "security intelligence" in waves

To address both the proliferation and magnitude of risks, organizations need to consider a more automated, proactive approach to security. In short, they need to incorporate *security intelligence* as an essential part of the business. This requires a comprehensive approach involving a range of issues, such as physical security, data classification, employee awareness and control.

In many organizations, security intelligence evolves across three levels. These represent a shift from manual approaches to the use of increasingly automated processes for identifying, tracking and addressing threats. The trend is toward more proactive anticipation of security issues rather than reactive approaches (see Figure 2).



Source: IBM analysis.

Figure 2: **A structured, three-level approach to building security intelligence.**

- *Basic* – Organizations focus on employing perimeter protection, which regulates both physical and virtual access. Perimeter protection provides input into manual reporting of incidents and violations. Enterprises at the Basic level are deploying firewalls, antivirus, access control and manual reporting, which are valuable first steps. However, they operate in a reactive and manual operating mode with little insight on their actual security posture.

- *Proficient* – Security is layered into the fabric of IT applications and business operations. This wave includes incorporating security into key applications, databases and business processes. At the Proficient level, security is becoming more comprehensive; but at the same time, complexity is added to an organization's security efforts. As a result, enterprises still fall short regarding their security intelligence, as security becomes more diffuse and less coordinated.
- *Optimized* – Organizations use predictive and automated security analytics to drive toward security intelligence. Security is Optimized as this wave includes the profiling of past intrusions, employee activity and other data sources to anticipate where potential breaches could occur and prevent occurrences before they happen.

Each of these three levels adds an additional layer of preparation against both inadvertent and deliberate security incidents. To identify and close security gaps throughout the enterprise ecosystem, organizations will need to explore and exploit analytics capabilities to meet their most pressing needs. An in-depth evaluation of four "security domains" can guide organizations toward security intelligence by systematically improving governance, risk management and compliance (see Figure 3).

- *People* – Switch from controlling access on an application-by-application basis via passwords to a role-based approach that controls user access through dashboards and privileged user controls.
- *Data* – Move beyond basic access controls and encryption methods to protect data by improving data governance and managing data usage and flow.
- *Applications* – Evolve from reliance on scanning for vulnerabilities in existing applications to detecting fraud and designing security into new applications.
- *Infrastructure* – Replace reactive methods like blocking unauthorized access and viruses with proactive methods that secure systems by enabling advanced network monitoring and forensics.

Security domains	Today	Security gaps	Tomorrow: Security intelligence	
People	Manage identities per application		Employ role-based dashboard and privileged user management	Apply advanced correlation and deep analytics
Data	Deploy access control and encryption		Monitor usage and control leakage	
Applications	Scan for vulnerabilities		Build securely from day one	
Infrastructure	Block unwanted network access and viruses		Execute real-time advanced threat detection and forensics	

Reactive → **Proactive**

Source: IBM analysis.

Figure 3: A balanced approach is needed to manage physical, technological and human assets.

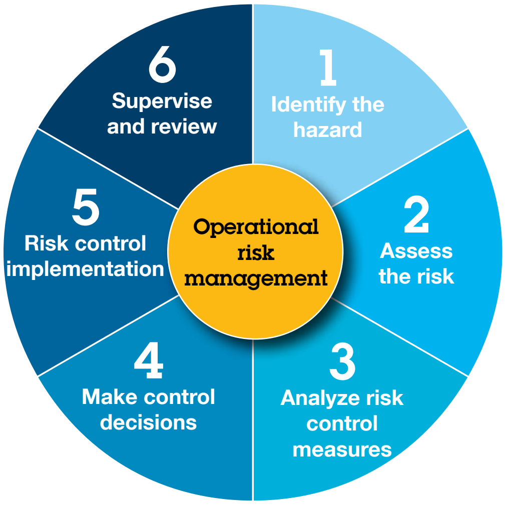
A three-point plan for the boardroom

C-suite executives need to take three important steps toward building security intelligence:

- **Get informed.** Take a structured approach to assessing business and IT risks.
- **Get aligned.** Implement and enforce security excellence across the extended enterprise.
- **Get smart.** Use analytics to proactively highlight risks and identify, monitor and address threats.

1. Get informed

Getting informed involves addressing IT security risk as part of the larger Enterprise Risk Management Framework (see Figure 4).

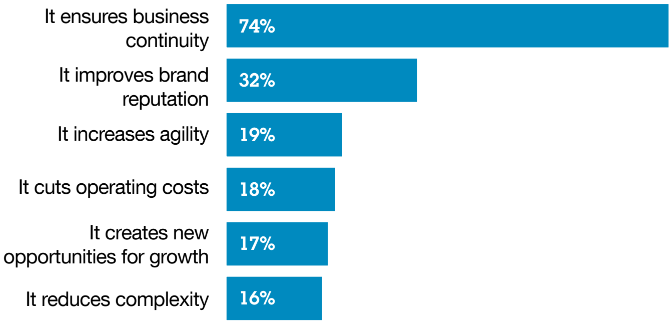

6
Supervise and review
1
Identify the hazard
5
Risk control implementation
Operational risk management
2
Assess the risk
4
Make control decisions
3
Analyze risk control measures

Source: IBM Institute for Business Value. "2010 IBM Global IT Risk Study." September 2010.

Figure 4: Major steps to address operational risk management.

This structured approach to assessing business and IT risks includes identifying key threats and compliance mandates; reviewing existing security risks and challenges; implementing and enforcing risk management processes and common control frameworks; and executing incident management processes when crises occur. Another important action is to empower a Risk Executive at the C-level who maintains regular interlock with the Board of Directors and peers about security-related issues and drives the IT risk conversations into the business.

Respondents to the IBM Global IT Risk Study agreed that investing in IT risk management can provide significant business benefits, particularly in the areas of business continuity (74 percent) and safeguarding the company's reputation (32 percent, see Figure 5). According to respondents, managing IT risk should be viewed as more than a defensive tactic. They also cited increased agility, lower costs, new growth opportunities and lower complexity as benefits realized by better management of IT risks.[7]



Source: IBM Institute for Business Value. "2010 IBM Global IT Risk Study." September 2010.

Figure 5: The benefits of improving IT risk management.

Case example:

Audit challenges related to IT security control risks spark IT governance revamp

A large U.S. financial institution was facing significant IT governance and business controls challenges both within and outside the company. Its external auditor cited a number of significant deficiencies, including Sarbanes-Oxley (SOX) weaknesses, while internal audits generated multiple unfavorable IT security reports.

The company prepared to implement a comprehensive, strong governance program based on industry best practices, as well as a system to help ensure the new controls were regularly updated and improved. The process began with a comprehensive evaluation of the company's security and entire system of controls, including IT general controls, application controls and IT governance. The organization's information security governance was assessed, including reviewing security processes and writing or updating policies, standards and procedures.

The identified gaps were closed through the establishment of four IT governance committees with clear policies, standards and procedures. In addition, the company implemented an IT governance framework and supporting toolset that successfully remediated issues and weaknesses relating to financial reporting in the areas of security, data integrity, change management and operations.

As a result of these efforts, this financial institution achieved a clean financial statement audit and SOX opinion from its external auditor – something that had eluded it in the prior three years. This allowed the company to register a new common stock offering with the Securities and Exchange Commission (SEC) which increased investor confidence and increased its stock value. Further, it was able to institutionalize the IT governance lifecycle program to enable continuous improvement of its IT governance and security processes and practices.

2. Get aligned

Security does not stop at the organizational boundaries. Successful firms need to implement and enforce security excellence across the extended enterprise. This includes involving key stakeholders, including:

- *Customers* – Develop and communicate personal information policies. Remain transparent and rapidly address privacy breaches.
- *Employees* – Set clear security and privacy expectations. Provide education to identify and address security risks. Manage the access and usage of both systems and data.
- *Partners* – Work with organizations across the supply chain to develop and implement security standards. Report on and manage risks, including security incidents, as a normal part of business operations.
- *Auditors* – Align enterprise and IT risk. Contribute to controls frameworks. Conduct regular reviews of regulatory and enterprise policies.
- *Regulators* – Manage regulatory risks and demonstrate compliance with existing regulations. Review and modify existing controls based on changing requirements.

Case example:

Effective governance aids industry compliance and improves audit responsiveness

Faced with a multitude of audits each year, a U.S. health insurer wanted to manage risk, implement and maintain prudent controls instead of having to react to each audit report. In addition, it hoped to reduce the impact these audits had on the business. At the same time, the company needed to establish compliance with new insurance industry regulatory requirements, such as those relating to the Health Insurance Portability and Accountability Act (HIPAA) and the National Association of Insurance Commissioners (NAIC) Model Audit Rule.

The solution involved an overhaul of the insurer's IT process governance structure. As part of this undertaking, the company instituted industry-standard IT governance controls that span all of its operations and business units, including governance for 15 critical IT processes. For each, a cyclical process was used, which identifies risk and defines the control framework by establishing, implementing and operating the governance procedures; testing them; and, finally, monitoring and reporting outcomes.

Not only do the new controls help the company monitor compliance with industry regulations and standards, they better align business and IT, help manage risk and help increase security. The company now has a more efficient, consistent response to audits – and has reduced the amount of effort needed for audit response by approximately half.

3. Get smart

Use analytics to proactively highlight risks and identify, monitor and address threats. As enterprises need to bolster their security defenses, the use of predictive analytics plays an increasingly important role (see Figure 6). They can do sophisticated correlation to detect advanced persistent threats, have a sense of governance and have automated enterprise risk processes in place – critical building blocks for enabling security intelligence.

This includes the ability to:

- Identify previous breach patterns and outside threats to predict potential areas of attack
- Mine employee systems behavior to identify patterns of potential misuse
- Monitor the external environment for potential security threats.

Security intelligence

	People	Data	Applications	Infrastructure
Optimized	• Governance, risk and compliance • Advanced correlation and deep analytics			
	• Role-based analytics • Privileged user controls	• Data flow analytics • Data governance	• Secure application development • Fraud detection	• Advanced network monitoring/forensics • Secure systems
Proficient	• Identity management • Strong authentication	• Activity monitoring • Data loss prevention	• Application firewall • Source code scanning	• Asset management • Endpoint/network security management
Basic	• Passwords and user IDs	• Encryption • Access control	• Vulnerability scanning	• Perimeter security • Anti-virus

Source: IBM analysis.

Figure 6: Using analytics to proactively highlight risks and identify, monitor and address threats.

Case example:

Analytics help upgrade security risk capabilities

While seeking a "smarter" way to address threats, a global pharmaceutical company also wanted to reduce the cost and complexity of its multi-vendor security environment. A lack of correlation between reported threats and vulnerability data in its old security infrastructure made it difficult to identify truly critical incidents. In addition, skilled resources were needed to proactively monitor alerts in real time from multiple security devices and take action before breaches occurred.

Using security software solutions, consulting expertise and managed services, the company was able to both expand protection and reduce cost and complexity. Now, millions of multi-vendor security events are analyzed across the company's computing environment, and sophisticated analytics process real-time security event data. Expert remediation guidance is used to rapidly correct issues and reduce vulnerability windows. In addition, reports allow the organization to track and trend vulnerability and threat data over time to gain a broader view of its security posture.

As part of this security transformation, the company was able to consolidate five vendor environments to one. Even more important, by taking a proactive approach, the company reduced its security management costs by 57 percent, while critical security events dropped from 10,000 per day to 15.

Are you building security intelligence?

Based on the potential for threats, and the opportunities to mitigate these risks using more advanced security intelligence, organizations should consider their answers to the following questions:

Across security domains

- What is your plan to assess your security risks?
- How are you able to detect threats and report compliance across domains?
- Do you have a log retention and audit capability?
- Which processes do you use to handle incident response and disaster recovery?
- How do you involve key internal and external stakeholders in security matters?

People

- To what extent have you rolled out an identity program?
- How do you know what authorized users are doing?
- What is your plan to automate identity and role-based management?

Data

- In what ways have you classified and encrypted sensitive data?
- How do you know if sensitive data leaves your network?
- How do you monitor access to data, including privileged access?

Applications

- How is security built into your application development process from day one?
- How do you regularly test your website for vulnerabilities?
- What is your approach to test legacy applications for potential exposures?

Infrastructure

- How do you promptly patch connected devices?
- In what ways do you monitor in- and out-bound network traffic?
- How are you building security into new initiatives (such as cloud, mobile and the like)?

Conclusion: Real risks demand an integrated C-suite

In today's increasingly complex and interconnected world, risks are real and increasing exponentially. An enterprise that delegates security matters solely to the CIO is compounding its risk factors. More than ever, each member of the enterprise's leadership owns a significant stake – and a powerful role – in securing the data and intellectual capital that flows through the organization (see Figure 7). There is one common denominator: security today is more than a purely technical issue. Rather it requires a frank discussion about risk, investment and taking a preventative approach to security issues.

Clearly, not every potential risk and contingency can be addressed in a cost-effective manner. Organizations must prioritize the business impact of potential risks instead of trying to protect against every conceivable threat. However, this prioritization depends on input from multiple C-suite executives who provide unique perspectives on their particular disciplines.

To learn more about this IBM Institute for Business Value study, please contact us at *iibv@us.ibm.com*. For a full catalog of our research, visit:

ibm.com/iibv

Be among the first to receive the latest insights from the IBM Institute for Business Value. Subscribe to IdeaWatch, a monthly e-newsletter featuring executive reports that offer strategic insights and recommendations based on our research:

ibm.com/gbs/ideawatch/subscribe

CEO	CFO	COO	CIO	CHRO	CMO
Prevent security risks from impacting shareholder value and trust	Know the financial implications of adverse security events	Evaluate impact of IT systems disruptions on ongoing operations	Understand the fallout effects of information security lapses across the business	Determine risks associated with unwarranted release of employee data	Address brand issues associated with security breaches

Source: IBM analysis.

Figure 7: **Security is a C-suite responsibility.**

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment. Through our integrated approach to business and execution, we help turn strategies into action. And with expertise in 17 industries and global capabilities that span 170 countries, we can help clients globally anticipate change and profit from new opportunities.

About the authors

John Lainhart is the IBM Global Business Services' Global Security & Privacy Service Area Leader and U.S. Public Sector Cybersecurity & Privacy Service Area Leader. He represents IBM on the American Institute of Certified Public Accountant's (AICPA) Assurance Services Executive Committee's Data Integrity Task Force and the Strategic Advisory Council for the Center for Internet Security. He has held numerous positions in the Information Systems Audit and Control Association/IT Governance Institute, including International President and currently is a member of the Framework Committee and serves as Co-chair of the CobiT® 5 Task Force and Principal Volunteer Advisor for IT Governance, CobiT®, ValIT® and RiskIT® related initiatives. He can be reached at *john.w.lainhart@us.ibm.com*.

Steve Robinson is General Manager, IBM Security Solutions, with worldwide responsibility for IBM security initiatives across the security products and services divisions. As strategy leader, he provides guidance to the development teams in software, hardware and services, as well as the marketing and security sales teams. Prior to this role, Steve was Vice President, Worldwide Sales, IBM Rational Software since 2005 with responsibility for the sales strategy and execution for the Rational brand, leading a worldwide force of over 1,000 sales professionals, channel teams and an extended community of strategic relationships including business partners, system integrators and ISVs. Steve joined IBM in 1984 and has held numerous executive and management positions in sales, technical services, and product management. He can be reached at *steve_robinson@us.ibm.com*.

Marc van Zadelhoff is the Director of Worldwide Strategy for IBM Security Solutions, responsible for overall offering management, budget and positioning for IBM's software and services portfolio globally. In this role, he runs IBM's customer Board of Advisors and meets with customers globally to develop IBM's direction. Previously at IBM, Marc has run security M&A for Tivoli, the marketing team for the acquired Internet Security Systems (ISS) division and most recently, Strategy, Portfolio & Business Development for IBM Security Services in the Global Technology Services division. Marc began his career as a strategy consultant. He can be reached at *marc.vanzadelhoff@us.ibm.com*.

Contributors

Linda Ban, Global CIO Study Director, AIS Studies, IBM Institute for Business Value, IBM Global Business Services

Hans A.T. Dekkers, Associate Partner, IBM Global Business Services

Peter Korsten, Partner and Vice President, Global Leader, IBM Institute for Business Value, IBM Global Business Services

Eric Lesser, Research Director and North American Leader, IBM Institute for Business Value, IBM Global Business Services

Kristin Lovejoy, Vice President, IT Risk, IBM BT/CIO organization

Wolfram Stein, Partner and Vice President, Global Strategy & Transformation Service Line Leader Executive, Consulting Services, IBM Global Business Services

Nichola Tiesenga, Partner, Public Sector, Cybersecurity and Privacy, IBM Global Business Services

Marisa Viveros, Vice President, IBM Security Services, IBM Global Technology Services

References

1 International Telecommunications Union. "Global Number of Internet Users, total and per 100 Inhabitants, 2000-2010." United Nations. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/Internet_users_00-10_2.xls

2 Ericsson. "More than 50 billion connected devices – taking connected devices to mass market and profitability." February 14, 2011. http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c

3 IDC "Digital Universe Study," sponsored by EMC. May 2010.

4 McMillan, Robert. "Siemens: Stuxnet worm hit industrial systems." *ComputerWorld*. September 14, 2010. http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

5 Greene, Tim. "Worst-case projected cost of Epsilon breach: $4B." *NetworkWorld*. May 1, 2011. http://www.network-world.com/news/2011/050111-epsilon-breach-costs.html

6 Fildes, Jonathan. "What is Wikileaks?" BBC. December 7, 2010. http://www.bbc.co.uk/news/technology-10757263

7 Ban, Linda B., Richard Cocchiara, Kristin Lovejoy, Ric Telford and Mark Ernest. "The evolving role of IT managers and CIOs." IBM Institute for Business Value. September 2010. http://www-935.ibm.com/services/us/gbs/thoughtleadership/ibv-global-it-risk-study.html

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
August 2011