IBM Institute for Business Value

The evolving role of IT managers and Chief Information Officers (CIOs)

Findings from the 2010 IBM Global IT Risk Study

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 based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM Global Business Services to provide analysis and viewpoints that help companies realise 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 Linda B. Ban, Richard Cocchiara, Kristin Lovejoy, Ric Telford and Mark Ernest

Mounting regulatory demands, the growth of around-the-clock online business and the constant shadow of an uncertain economy underscore the importance of managing risk in all its forms – whether related to business, data or events. The 2010 IBM Global IT Risk Study uncovers the challenges associated with IT risk and the steps IT managers and CIOs are taking to better understand, confront and resolve this concern. Of the IT managers surveyed, most expect their risk-related responsibilities to increase. Clearly, IT risk management is far-reaching and can directly influence a company's competitive position, as well as its reputation with customers, partners, regulators and other stakeholders.

From a business perspective, the IT infrastructure plays an increasingly critical role in not only supporting and safe-guarding a company's key assets and assuring proper governance and compliance, but also in driving business growth. Consequently, IT risk management is no longer viewed as a strictly technical function, but a crucial management task that can provide direct business benefits to the entire organisation.

To better understand how companies are working to manage and mitigate risk throughout their business – particularly as it applies to IT – IBM initiated the 2010 IBM Global IT Risk Study, part of the ongoing research IBM conducts in the area of IT risk and the first in a series of research surveys that examine this subject. The survey, which was conducted in May and June of 2010 in cooperation with the Economist Intelligence Unit (EIU), seeks to better understand the areas that IT managers are focusing on today and where they see opportunities and challenges in the short term. Future research will explore these issues in depth and examine the options and decisions that confront all risk management teams.

'During the period where IT has become core to more businesses' operations, the management of IT risk has not gained commensurate prominence.'

Respondent, Travel and Tourism industry, Western Europe

'Although some say that technology has matured and become commoditised in business, we see the technological 'revolution' as just beginning. Our reading of the evidence suggests that the strategic value of technology to business is still increasing.'

Brynjolfsson, Erik and Adam Saunders. 'Wired for Innovation: How Information Technology is Reshaping the Economy.'' Massachusetts Institute of Technology. 2010.

The results of this study are based on a comprehensive online survey of 556 IT managers and others primarily involved in their business's IT function (including 131 CIOs). Representing regions that include North America, Western Europe, Asia-Pacific, the Middle East and Africa, Eastern Europe and Latin America, the study crosses industries – from IT, financial services, healthcare and pharmaceuticals, to biotechnology, manufacturing and government. Companies surveyed reported revenues ranging from GB£330 million to more thanGB£660 billion.

The primary goals of the study were to:

- Survey a cross-section of enterprises to accurately gauge the current state of IT risk management
- Identify factors that can advance (or impede) an organisation's risk management strategies
- Discover to what extent enterprises are implementing new risk strategies, programs and policies
- Understand how IT advancements such as cloud computing align with companies' overall risk strategies
- Examine the evolving role of IT managers, including the CIO.

In general, the findings of the survey were consistent across regions, company size, industry and roles. (All regions represented in the study acknowledged the importance of IT risk management and are working on making improvements in that regard). By and large, study participants expressed confidence about their risk management and compliance efforts (see Figure 1).

Still, although more than 50 percent of respondents reported that their budgets have remained the same or been enhanced,

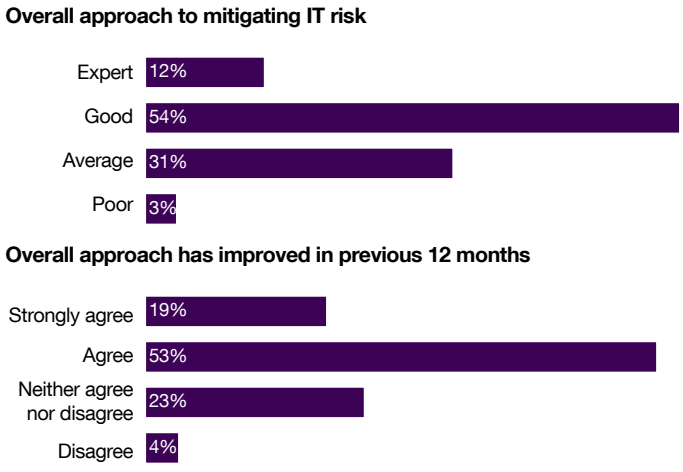

Figure 1: Organisations give their approach to mitigating IT risk high marks.

36 percent still struggle with securing enough funding to address risk-related challenges. Also in spite of the recognition that IT risk management can provide real business benefits, securing senior leadership support remains a real concern. Respondents' feedback seems to indicate a disconnect between how senior management views the cost of improved IT Risk management and the value that can be derived from it.

Making room for improvement

Recognising the potential business returns of effective IT risk management, many of those surveyed envision extending their risk-related initiatives over the next three to five years. Nonetheless, there were some notable discrepancies. Only about half of the companies surveyed have a formal risk management department (46 percent) or a well-crafted business continuity strategy (54 percent) in place. Also, line of business and other operational risk concerns (financial/business strategy, for example), are not primary focus areas.

'IT organisations traditionally go through extensive testing before introducing new IT enabled business services, with the primary aim to avoid an outage. But modern IT executives need to understand the true cost to the business of such tests. It's not just the IT costs, it's the lost opportunity cost due to a delayed business service. Each day spent testing is one less day generating revenue and profit. What's the risk if the service fails balanced against the benefit of getting the service up and running?'

Mark Ernest, IBM Distinguished Engineer

When asked to describe their organisation's overall approach to mitigating IT risk, 66 percent of respondents rated it as good to expert. While this represents the majority of companies, more than 30 percent regard their business as average to poor in this area. However, 72 percent of respondents report that their company's approach to risk has improved over the last 12 months.

Not surprisingly, 47 percent of respondents indicated that IT risk planning is for the most part a discrete function conducted in business silos. Consequently, getting areas of the organisation to work together is a significant challenge. Also telling: Many of those surveyed revealed that although they are very involved in a number of risk management and compliance activities, they would like to participate more. (While approximately half of survey respondents stated that their company has a risk management department, many believe that the business falls short in terms of educating and communicating to employees the organisation's risk management policies and concerns).

On a positive note: In a tough economic environment, IT risk management and compliance has remained largely immune from budget cuts or cost reductions. When asked about their organisation's 2010 budget for risk management, 14 percent (80 survey respondents) expected a significant increase in funds, and 39 percent saw somewhat of an increase. Thirty-six percent indicated that risk management funding would remain the same.

Survey respondents agree that investing in IT risk management can provide significant business benefits, most particularly in the areas of business continuity (74 percent) and safeguarding the company's reputation (32 percent, see Figure 2). According to respondents, managing IT risk should be viewed as more than a defensive tactic; it can increase a

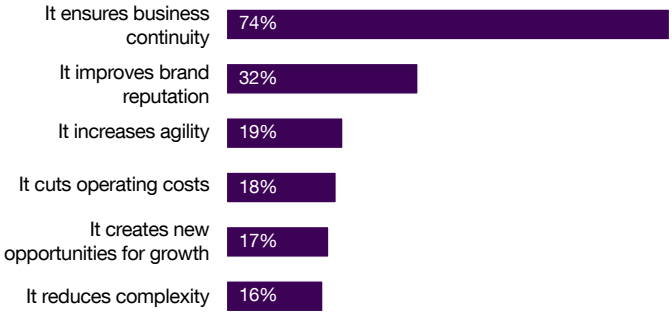

Figure 2: Benefits of improving IT risk management

company's agility (19 percent) and create growth opportunities (12 percent) while reducing costs (18 percent). Yet most IT managers (57 percent) spend their time focusing on infrastructure-related risk.

At the top of the chart: IT security

Although IT risk applies across processes, activities and systems, IT security (vulnerability to hackers and unauthorised access/use of company systems) is the number-one concern among 78 percent of the IT professionals surveyed. Hardware and system malfunction was next – cited by 63 percent of survey respondents. Power failure and physical security (40 percent) was not far behind, followed by theft, product quality, compliance, natural disasters, e-discovery requests, supply chain failures and terrorism, in that order.

'Business continuity encompasses far more than planning for natural or planned disasters. It is really about building a risk-aware culture – making sure that the necessary tools, processes and methodologies are in place and that every individual in the organisation is aware of their responsibility in regard to the safety and integrity of data. Finally, when implementing tools and processes, it is critical to balance speed to market and acceptable risk."

Jessica Carroll, Managing Director Information Technologies, United States Golf Association

IT managers have clear opinions about the importance of risk management, as well as specific focus areas. Nonetheless, there are significant gaps when it comes to the confidence they have in their organisation's ability to appropriately address and react to risk. For example, only 22 percent of those surveyed believe their organisations are well prepared in terms of IT security. Twenty-three percent of survey respondents feel the same way about their company's preparedness for hardware and system failures. Protection against power failures garnered more support – with 32 percent of survey respondents indicating

Case Study

In the first half of 2010, the IBM X-Force Research and Development team documented 4,396 new vulnerabilities – a 36 percent increase over the same time period last year. According to the report, web application vulnerabilities continue to be the leading threat – accounting for more than half of all public disclosures. Nonetheless, the report noted that organisations were doing more to identify and disclose security vulnerabilities than ever before. This in turn is having positive effects on the industry by driving more open collaboration to identify and eliminate vulnerabilities before cyber criminals can exploit them.[1]

their business was well prepared in that area. However, there is a clear disconnect between respondents' recognition of the importance of addressing overall IT risk and the confidence they have in their company's ability to properly manage and mitigate it.

The communications challenge

There is no doubt that IT risk management can provide genuine business advantages. Yet in spite of the various methods companies can use to distribute risk-related information, communication emerged as a real barrier. Securing the support of senior leadership is still a challenge, according to 25 percent of survey respondents. Communicating risk policies and procedures to employees was also a problem for 30 percent of those surveyed.

Many organisations take a passive, rather than a proactive, approach to managing and mitigating IT risk. In many cases, information is consigned to the business's intranet, where employees must spend time searching for it. Some organisations incorporate risk management policies into training materials for new employees – not taking into account the need to make it available to all. (Only 22 percent of IT

'We struggle with getting management and staff to accept that their behaviour must be modified in order to improve security practices.'

Respondent, Manufacturing industry, Western Europe

'It is increasingly difficult to secure funding to address IT risks, even when the costs of NOT addressing the risks are clearly outlined to executives. There is often a general unwillingness to invest.'

Respondent, Aerospace and Defense industry, North America

managers indicated that risk management policies are part of every employee's formal training). Perhaps most surprising: Less than 15 percent have incorporated an integrated risk management plan into the physical and technical infrastructure of their enterprise.

Given the variety of communication and education channels available to build awareness of risk, companies would be well advised to take a more organised and detailed approach to staying on top of risk issues, communicating those concerns to employees and incorporating IT risk management into every area of their enterprise. In answer to the question, 'How does your company primarily keep abreast of risk?' the majority of survey respondents indicated that security threats were handled by both internal and external resources (38 percent), a cross-functional team of executives (26 percent), or a designated risk management department (19 percent).

'Normally, users, management and partners look at risk from different perspectives. I need to make those ends meet in a sensible way.'

Respondent, Manufacturing industry, Western Europe

Evaluating emerging technologies

Respondents to the survey were asked how their organisation is positioned to acquire and deploy five emerging technologies (see Figure 3):

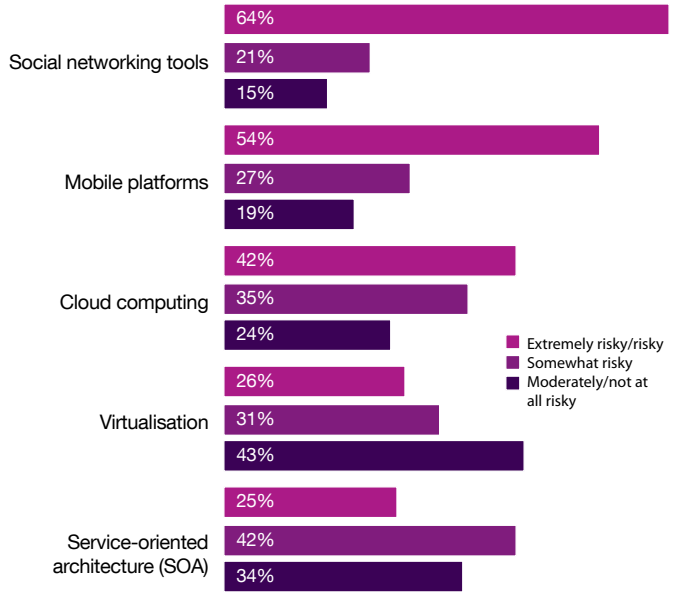

Figure 3: Social networking, mobile platforms and cloud computing present the highest risk concern.

- Social networking tools (intra- and Internet forums, instant messaging, libraries, blogs and wikis, for example)
- Mobile platforms (Windows® Mobile, BlackBerry OS and Google Android OS, to name three)
- Cloud computing
- Virtualisation
- SOA.

Of these five technologies, social networking, mobile platforms and cloud computing presented the highest causes for concern. Social networking tools were the biggest worry in terms of risk for 64 percent of those surveyed, with mobile platforms and cloud computing not far behind (54 and 43 percent, respectively). Most of the risks have to do with the accessibility, use and control of data, especially regarding social networking and the danger of having unauthorised access to confidential, proprietary information. (Many organisations have not yet established processes and methods to integrate social networking tools into their infrastructure and workflow).

'Cloud is only an opportunity to solve a problem when you can leverage the best advantages of the cloud. So that is something that has to be factored in.'

Respondent, Information Technology industry, North America

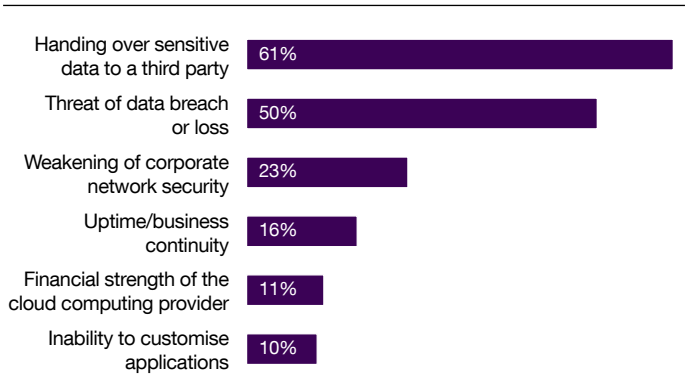

Figure 4: Risks associated with cloud computing.

When asked to cite the two highest risks they associate with cloud computing, the majority of survey respondents pointed to data protection and privacy (see Figure 4). Business continuity was clearly on the minds of more than half of those surveyed, whereas 44 percent believe that private clouds are riskier than traditional IT services and 77 percent expressed concerns about privacy.

Handing data over to a third party was also considered risky by 61 percent of respondents, while only 23 percent worried about network breaches.

Only 26 percent of survey respondents indicated that virtualisation posed significant risk to their organisation. Similarly, SOA was a concern for only 25 percent.

Resting on the Cloud

IT managers are feeling the pressure to lower infrastructure-related expenditures, heighten efficiencies and improve service levels across the business. Many are looking at cloud computing to help them achieve these goals. Cloud computing represents a major advancement in computing models – much like its predecessors, client/server and mainframe computing. Processing is handled across a distributed, globally accessible network of IT resources, which are dispensed on demand, as a service. Cloud computing offers a highly automated, dynamic alternative for the acquisition and delivery of IT services – allowing users to tap into public, private and hybrid clouds for computing resources and services without having to deal directly with the underlying technology. Today, companies are leveraging the massive scalability and collaboration capabilities of cloud computing to solve problems in ways never before possible. And they are deploying new services faster – without additional capital investments. Nonetheless, organisations must be prudent and informed when choosing a provider, especially given concerns related to risk.

Implications for IT managers

Of the IT managers surveyed, most expect their responsibilities – from executing policies and procedures and providing input to risk mitigation strategies, to helping set and/or oversee IT risk strategies for the organisation – to increase over the next three years (see Figure 5). More than 65 percent of respondents concurred that risk mitigation is becoming a more integral part of their job, while 83 percent believe that IT managers should be more involved in risk mitigation.

When one considers the growing interdependency of business and IT, these responses are not surprising. Indeed, the IT managers and CIOs surveyed believe their jobs will incorporate support of the overall business strategy, as well as the corporate brand (for example, in marketing and customer service). As more companies stabilise or 'harden' their risk management strategies, processes and procedures, responsibility for the infrastructure may move to a supplier or partner – allowing IT managers to focus more on business security, resiliency and continuity.

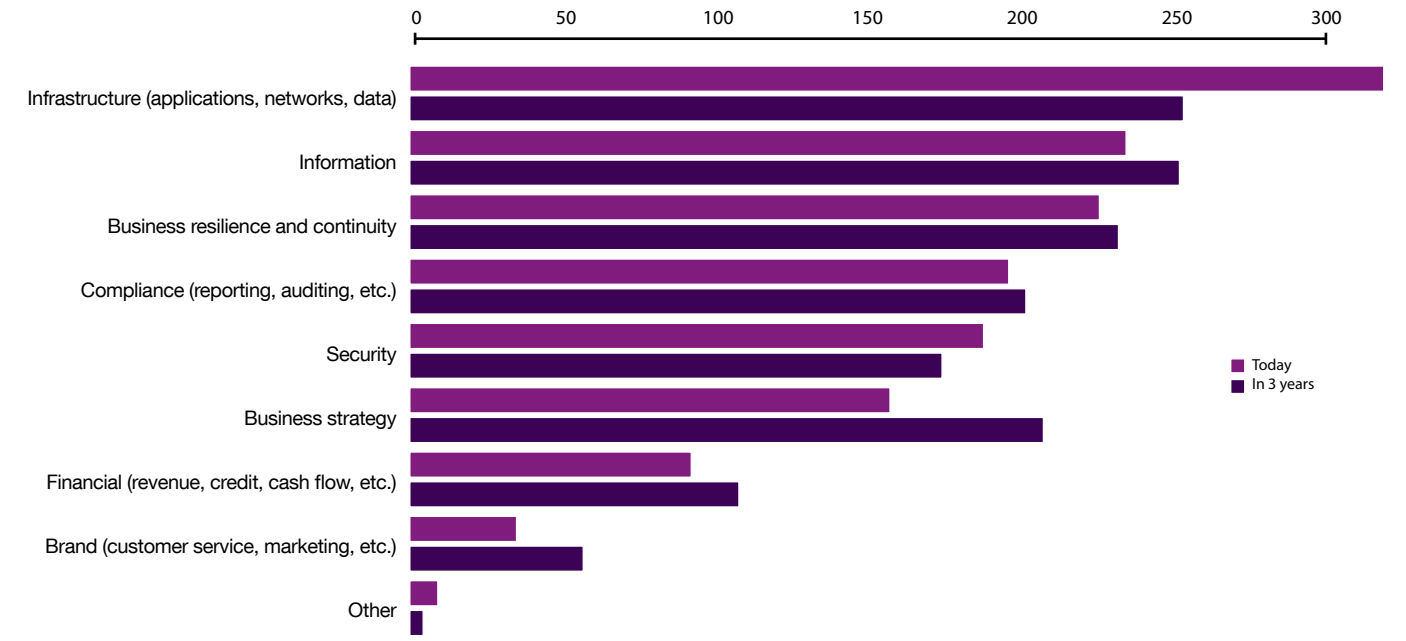

Figure 5: IT managers expect their areas of responsibility to shift over the next three years.

It is also interesting to note that when the data from the 131 CIOs who responded to the survey was cross-referenced, the answers did not vary significantly from the IT managers surveyed.

While the significance of IT risk management and compliance is readily acknowledged by organisations across industries and many are working to improve these aspects of their business, few are totally prepared for all of the risk and compliance related situations that could occur.

The findings of the 2010 IBM Global IT Risk Study revealed areas of focus that can help IT managers assess their risk maturity, pinpoint gaps, set priorities and develop strategies in several areas:

- Within a business, risk awareness is everyone's responsibility. Yet unless risk-related policies and procedures are engrained in the corporate culture, many initiatives for managing and mitigating IT risk can fall short, or fail altogether. Results of the study confirm that companies need to work harder at educating, communicating and supporting risk management and compliance initiatives across the enterprise.
- Data is a common concern in all aspects of IT risk management – from security, business resilience and continuity, to availability, disaster recovery, hackers, compliance, infrastructure and data management. With this in mind, companies should take a unified, holistic approach to IT risk – taking into account all of its elements in order to aim for the overall goals of realising more returns and higher efficiencies.

- When adopting emerging technologies, architectures and strategies, developing new applications or integrating existing systems, risk mitigation should be a primary point of discussion. Taking into account both positive risk (that which a company initiates because there is an opportunity that comes with the risk) and negative risk (potential incidents that can bring harm to the business) can add more business value and possibly increase revenues – but only if proper funding for IT risk management is included.

  Not all emerging technologies are created equal, but some – like virtualization and cloud computing – can offer many advantages in terms of support and options for risk mitigation. Although cloud computing requires attention to data security, if properly deployed it can help reduce the costs and alleviate the risks associated with business resilience. However, it is vital to have processes in place to address risks related to any new technology.

'We sometimes tend to consider a project plan rather simplistically in that we think we know where the risks exist, so we approach allocation of resources on that basis.'

Respondent, IT and Technology industry, Middle East and Africa

Getting there from here

Effectively managing IT risk is a multi-faceted endeavor. When approaching this task, IT managers should consider the following:

Examine and assess the organisation's IT risk capability

- Institute cross-enterprise planning for all risk categories (data, security, resilience and disaster recovery and new technologies)
- Consider the range of risk challenges and confirm that there is a plan in place to address each (prioritising and mitigating 'downside' risk like system failures and security breaches, for example) and verifying how to leverage 'upside' risk (shorter time to market and new customer contact points, for instance).

Look for champions among senior leadership

- Become a trusted adviser and valued resource to the CIO; articulate the benefits that they and other leaders bring in addressing IT risk
- 'Sell' the benefits of risk mitigation, such as stronger business growth, more agility and improved brand perception.

Determine how to heighten risk awareness at all levels and within the organisational culture itself

- Incorporate risk awareness into everyday business and IT processes. Make sure there are a variety of methods for educating the entire company
- Create a strategy for regularly communicating the breadth of risk management, as well as compliance topics and issues – emphasizing that it is more than just a 'one-time' activity.

Look for innovative ways to implement risk mitigation procedures

- Build risk-related procedures into the IT infrastructure, as opposed to adding them to applications in a piecemeal manner
- Examine business processes for potential risk issues and establish a specific IT risk governance plan that can be executed across the entire organisation.

Make sure safeguards are in place to help prevent unauthorised access to company data and systems

- Review business continuity plans. Business continuity involves more than planning for a natural disaster; it encompasses a wide range of business interruption scenarios – from server failures to pandemics
- Make everyone aware of their responsibility to keep data safe and protected – and how to execute that responsibility
- Identify tools, processes and methodologies to keep data safe and secure. Keep in mind that many already exist (identity access and control; master data management; information lifecycle management; data ownership processes).

It's no longer a question of *if* new technologies will be introduced into an organisation, but *when*. As mentioned earlier, not all emerging technologies are created equal, but some can provide significant benefits in terms of managing IT risk. Newer technologies, such as virtualisation and cloud computing, offer impressive options for mitigating risk and reducing costs.

Are you ready?

- How does your company assess its risk maturity and manage risk, both in terms of the business, as well as its IT infrastructure and assets?
- What strategies does your organisation have in place for following industry and IT best practices for mitigating risk – starting with security and including resiliency and business continuity?
- In what ways do your company's risk-related initiatives help improve visibility and control and help assure compliance with contracts, industry standards, regulations and internal controls?
- How does your IT infrastructure support the ongoing performance objectives of the business in terms of flexibility, security, availability, governance, scalability, resiliency and governance?
- What type of plan does your organisation have for assuring that human capital, processes and systems are able to recover and respond to a disruptive event?

Vigorous, cyclical IT risk governance – from technology and business perspectives – continuously evaluates a business's vulnerability to IT risks, prioritises those risks and acts on them. Consequently, it is important to incorporate risk management protocols into new technologies as soon as they are implemented.

Finally, consider the needs of the business when implementing tools and processes. Balance speed to market and acceptable risk. By taking a proactive approach to IT risk management, companies can position themselves to stay a step ahead of vulnerabilities, and remain more secure and resilient in the face of planned or unplanned incidents.

For more information

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

ibm.com/iibv

To access additional IT risk management resources, please visit:

ibm.com/smarterplanet/security

Authors

Linda Ban is the CxO Study Program Director and Application Innovation Services (AIS) Lead for the IBM Institute for Business Value. In this role, she leads the global team responsible for the development, deployment and support of IBM's thought leadership around the CIO programme as well as IBM's AIS organisation. Linda's diverse background includes extensive experience in emerging and collaborative technologies, business and operations strategy, systems development and operations management. In addition to her work with clients, she has published extensively on a broad range of business topics, challenges and solutions. Linda can be contacted at *lban@us.ibm.com*.

Richard Cocchiara is an IBM Distinguished Engineer and the Chief Technology Officer for Business Continuity and Resiliency Services in IBM Global Services. He has over 28 years of I/S experience and has performed consulting engagements at many fortune 500 companies, particularly in the finance and securities industry. Rich is currently responsible for research and development of Business Continuity and Resiliency solutions and services within IBM Global Technology Services. He can be reached at *rmcocch@us.ibm.com*.

Kristin Lovejoy is the Vice President responsible for IBM's Security Strategy. She was recognised as one of the Top 25 CTOs by InfoWorld in 2005 and as one of the Top 25 Most Influential Security Executives by Security Magazine in 2006. She holds a U.S. and EU patents for Object Oriented Risk Management Model and Methodology. Kristin can be contacted at *klovejoy@us.ibm.com*.

Ric Telford is Vice President of IBM Cloud Services and is responsible for defining new opportunities and services as part of IBM's broad portfolio of cloud computing offerings. During his tenure at IBM, Telford has played a number of key roles in various software and service initiatives for the company, including document management, networking, systems management and IT infrastructure services. Previously, Ric served as VP of Autonomic Computing, leading the development toward more self-managing systems. Ric can be reached at *rtelford@us.ibm.com*.

Mark Ernest is an IBM Distinguished Engineer and a member of the IBM Academy of Technology. He assists clients in the design and implementation of IT management systems to maximise the value of their IT investment and improve the efficiency and effectiveness of their use of information technology. Mark can be contacted at *lernest@us.ibm.com*.

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 design 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 anticipate change and profit from new opportunities.

Reference

1 The IBM X-Force 2010 Mid-Year Trend and Risk Report. IBM Corporation, 2010.

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
PO6 3AU
United Kingdom

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland Limited is registered in Ireland under company number 16226.
The IBM home page can be found at ibm.com

Please Recycle

GBE03365-GBEN-00