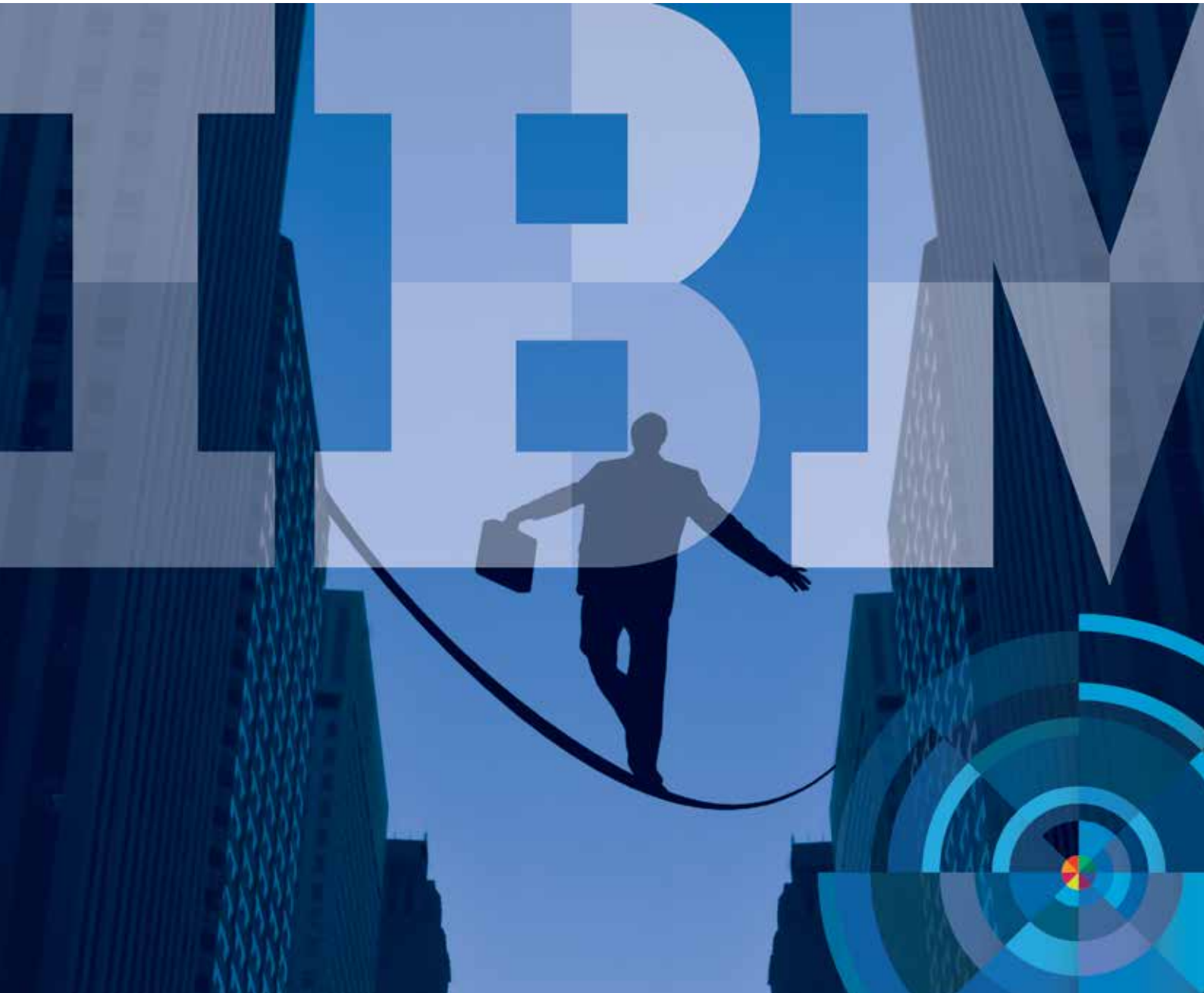
Six keys to effective reputational and IT risk management

How to manage reputational and IT risk to protect and enhance brand value and competitive standing

Implications of the 2013 IBM Global Reputational Risk and IT Study



About the study

The IBM Global Reputational Risk and IT Study is one of the largest studies ever conducted to examine the relationship between IT and reputational risk.

The initial group of 427 respondents participated in a survey conducted by the Economist Intelligence Unit on behalf of IBM. An additional 175 respondents participated in the study online at a special IBM survey website.

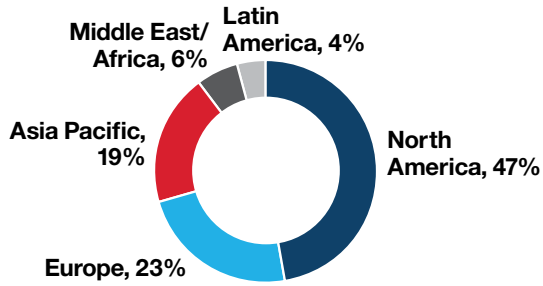
All participants answered questions specifically designed to provide a detailed picture of the connection between reputational risk and IT in business today—including which IT risks have the most impact on reputation, whether these risks are being managed effectively and identification of the gaps that need to be closed.

We would like to thank all of the executives who participated in the survey for their valuable time and insights.

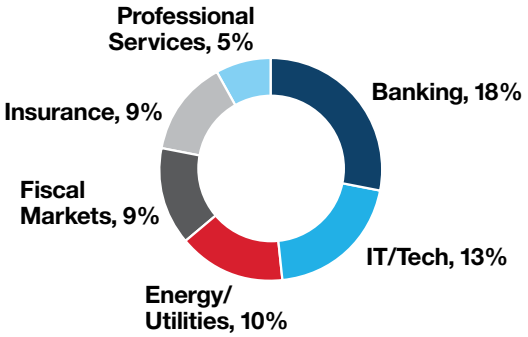
For a detailed analysis of survey results be sure to read the 2012 IBM Global Reputational Risk and IT Study Report

---

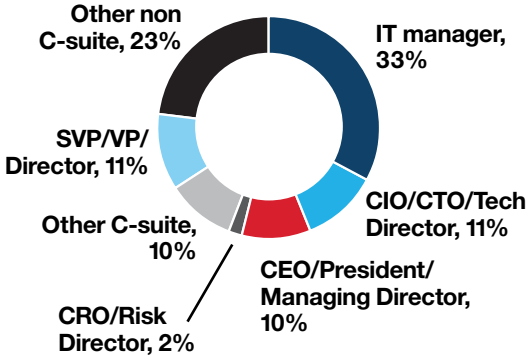
Respondents: 602



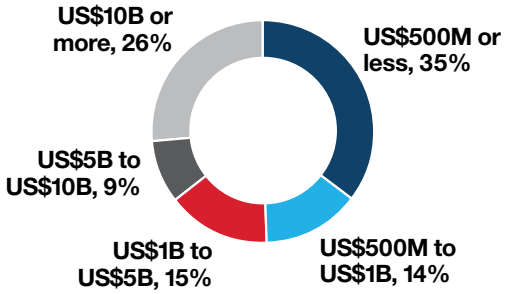
Industries: 23*



Job titles: 15*



Company sizes: 5



*Top responding categories shown

The reputational risk and IT connection

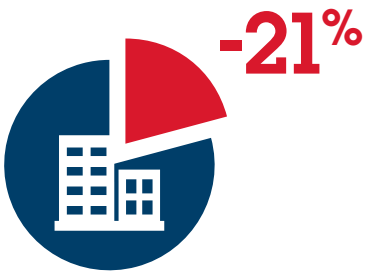
When the corporate world first started paying attention to the concept of reputational risk in 2005,[1] organisations' focus was on business issues such as compliance and financial misdoings. Today, as evidenced by the results from the IBM Global Reputational Risk and IT Study, the focus has shifted to include the reputational impact of IT risks.

Virtually every company is now reliant on technology for its critical business processes and interactions. While it may take 10 minutes or 10 hours to recover from an IT failure, the reputational impact can be felt for months or even years.

Factors strongly affected by IT risk

Reputational damage caused by IT failures such as data breaches, systems failures and data loss now has a price tag. According to analysis performed by the Ponemon Institute, the economic value of a company's reputation declines an average of 21 percent as a result of an IT breach of customer data—or the equivalent of an average of US$332 million.[2]

The true price of reputational harm



The economic value of a company's reputation declines an average of 21 percent as a result of an IT breach of customer data.

Source: Ponemon Institute[2]

The question now is not whether IT risks affect your corporate reputation, but what you can do to effectively prevent and mitigate these risks. Drawing on the best practices of top performers in the IBM Global Reputational Risk and IT Study and the expertise of IBM IT risk management specialists, this paper provides practical advice and recommendations that will allow you and others in your organisation to evaluate reputational and IT risk management with a newly informed and critical eye, and make the changes necessary to protect your company's valuable reputation.

Six keys to effective reputational and IT risk management

An analysis of responses to the IBM study revealed distinct correlations between the initiatives that organisations are undertaking to protect their reputations from the ramifications of IT failures and the overall effectiveness of their reputational and IT risk management efforts.

Based on this analysis, and the pattern it revealed among organisations that are most confident in their ability to prevent and mitigate IT-related reputational risk, there are six key initiatives that IBM recommends as part of every company's efforts:

1. **Put someone in charge.** Ultimate responsibility for reputational risk, including IT-related items, should rest with one person.

2. **Make the compliance and reputation connection.** Measuring reputational and IT risk management strategies against compliance requirements is essential.

3. **Reevaluate the impact of social media.** In addition to recognising its potential for negative reputational impact, social media should be leveraged for its positive attributes.

4. **Keep an eye on your supply chain.** Organisations must require and verify adherence of third-party suppliers to corporate standards.

5. **Avoid complacency.** Organisations should continually evaluate reputational and IT risk management results against strategy to find and eliminate potential gaps.

6. **Fund remediation; invest in prevention.** For optimal reputational risk mitigation, companies need to fund critical IT systems as part of their core business.

How important is reputational risk?

Reputational risk represents the possibility that your company will lose potential or existing business because its trustworthiness has been called into question. Participants in a recent Ponemon Institute study placed economic values on their corporate brand or reputation ranging from less than US$1 million to more than US$10 billion, with the average coming in at US$1.56 billion.[3]

Enough companies assign high value to corporate reputation and its protection that their annual reports contain special sections dealing with this topic. With today's widespread use of social media and other sources of instant news and communication, a company's reputation has never been more vulnerable.

Put someone in charge

When asked to choose the top three job functions most responsible for managing reputational risk, a clear majority (80 percent) of respondents to the IBM Global Reputational Risk and IT Study chose the chief executive officer (CEO). The chief financial officer (CFO), chief information officer (CIO), chief risk officer (CRO) and chief marketing officer (CMO) were also assigned responsibility, but at significantly smaller numbers.

What is keeping the C-suite up at night?

CEO Compliance failure
CIO Data integrity and downtime
CRO Insufficient disaster recovery measures
CFO Financial impact of IT risks
CMO Brand reputation
CISO Data breaches and cyber security
Chief Digital Officer Reputational risk

While the majority of organisations assign responsibility for reputational risk to the CEO, this may not be an effective choice. CEOs already have a number of responsibilities; adding reputational risk to these responsibilities can result in reputational risk not being given the detailed and day-to-day attention it requires. The CRO may be a better choice for many organisations, and is already a part of the C-suite in many financial organisations. But, because the CRO's responsibilities usually encompass traditional risk sources as well as new IT-related risks, the CRO still may not have the bandwidth to give reputational risk the emphasis it deserves.

Forward-thinking companies are starting to appoint chief digital officers (CDOs). The CDO is responsible for anything and everything related to a company's digital presence. Adding a CDO to the C-suite gives reputational and IT risk the emphasis and priority that is essential in today's technology-driven world.

The rise of the chief digital officer

Charged with responsibility for everything related to a company's digital presence, the CDO is on the front line of an organisation's reputational and IT risk management efforts.

The CDO is a fairly new member of the C-suite, and many companies have yet to appoint someone to this position. Those who have appointed a CDO have often chosen an individual from within the organisation who has strong business and technology knowledge. The CIO and CMO are often at the top of the short list of candidates.

It is anticipated that, as awareness and concern over reputational and IT risk continues to rise, the CDO will become part of the C-suite for a significant number of organisations.

Make the compliance and reputation connection

Compliance is often viewed as a separate and discrete risk, with the CFO holding responsibility for the strategies and processes it involves. In reality, compliance and reputation are inextricably linked—as news headlines and share prices attest.

IT risks also have a large part to play in compliance. For example, 87 percent of banking industry respondents in the IBM study say IT failures have severe consequences for compliance, particularly the data protection and archiving that are essential to responding effectively to legal or regulatory inquiries.

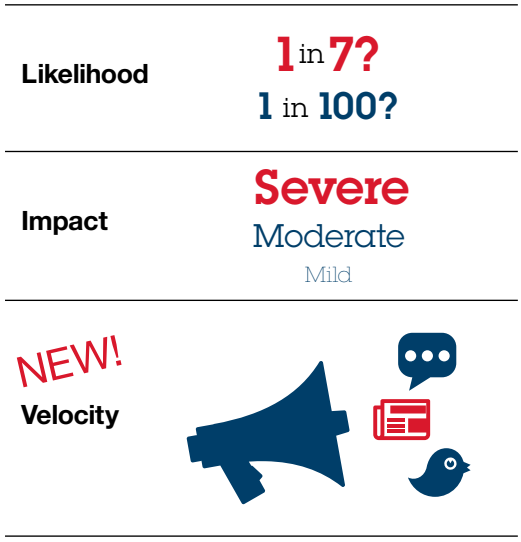
Organisations can no longer afford separate views of compliance and reputational risk. A part of every reputational and IT risk management strategy should be the measuring of this strategy against the organisation's compliance requirements to assure adequate protection and mitigation processes and to expose any gaps.

Reevaluate the impact of social media

Social media have added an entirely new dimension to evaluating and managing reputational risk. In the past, reputational risks were evaluated and mitigated based on their likelihood and their potential impact (two dimensions). Now, thanks to social media, the reputational risk equation needs to take velocity into consideration (third dimension). In today's connected marketplace, customers and other stakeholders know about IT-related reputational incidents almost instantly. A company's response needs to be equally swift.

The impact of social media on an organisation's reputation is not wholly negative, however. Social media provide valuable new channels for customer engagement, which is an integral enhancer of a company's reputation. Social media can also be used as a source of instant information for customers and employees in the event of an IT-related reputation event, helping to mitigate the repercussions of that event and even rebuilding reputation.

Reputation risk needs to be measured across three dimensions



A robust reputational and IT risk strategy needs to recognising the reputational power of social media and require tactics for leveraging social media to protect and enhance the company's reputation.

Keep an eye on your supply chain

A company's supply chain—including vendors, partners and other third-party suppliers—is often its weakest reputational link. Only 28 percent of the respondents to the IBM Global Reputation and IT Risk Study, for example, indicate that they very strenuously require their supply chain to apply the same level of IT risk control as their companies do internally.

"A major deliverable was on a contractor's laptop, and it was stolen. We missed an important client deadline and lost the source files for all the work."

— Chief marketing officer, American education company

The reputational implications of supply chain relationships are two-fold. First, sensitive corporate data that is shared with third parties can be compromised if the third party does not have robust IT security and resiliency protections in place. Second, critical suppliers that do not adequately protect their own systems and data can have a higher level of downtime, leading to disruptions in production cycles or product availability that reflect negatively on both the corporation and the partner.

To be most effective, organisations not only need to require their partners to match their level of reputational and IT risk management, they also need to verify adherence to these standards through regular audits and other reporting methods.

Avoid complacency

Cross-analysis of study responses show that companies are often more confident in their ability to manage IT-related reputational risk than reality proves—opening them up to reputational damage they may not have anticipated or prepared for.

While 62 percent of study respondents rated their company's overall ability to manage IT risk as strong or very strong, a significant percentage also reported a lack of such basic risk management tools as firewall protection, identity and access control, regular penetration testing and access to the latest security intelligence.

Companies are missing fundamental IT risk mitigation measures

of companies are not performing penetration testing

of companies do not have access to the latest security intelligence

All of these basic IT risk management tools should be in place in all companies, as they represent the minimum table stakes for effective reputational and IT risk management. Penetration testing and access to the latest security intelligence have a particularly low implementation rate. Without penetration testing on a regular basis, an organisation has no way of knowing how secure the interactions between employees and between the company and its customers truly are. Without access to the latest security intelligence, an organisation may leave its most critical business data exposed to hackers or malware without ever knowing that a threat exists.

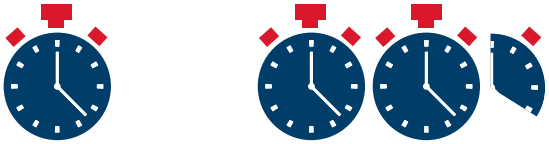
It is absolutely critical that an organisation's reputational and IT risk management strategy maps to concrete and measurable implementation tactics. Organisations should also perform regular gap analyses to assure that both strategy and tactics evolve to address ever-changing risks.

Fund remediation; invest in prevention

The majority of respondents in the IBM Global Reputation and IT Risk Study are reporting both adequate current IT funding allocated to managing reputation risk and adequate anticipated increases in funding. This may, however, be another example of complacency.

When organisations report a strong ability to manage IT risks, but do not have basic risk management tools in place, it can be inferred that what is being reported as adequate funding may, indeed, be inadequate. When the CIO is not an integral part of the reputational risk management process, the organisation may not have a clear idea of where the funding inadequacies lie.

The cost of system downtime



US$181,770
per hour
The cost of data centre downtime

US$418,017
per event
The cost of a business interruption event

In determining what is truly adequate IT funding, organisations also need to take the costs of inadequate funding into consideration—prevention versus cure. The Aberdeen Group reports that the cost of an hour of data centre downtime for an industry-average organisation is US$181,770, and the total cost of a business interruption event totals US$418,017.[5] Multiply that by an average of 2.3 events per year, and the cost rises still further to almost US$1 million.

"Underestimating the cost of reputational risk greatly exceeds the cost of protection. Proaction is preferable to reaction."

—Finance director, U.S. bank

Organisations need to treat critical IT systems as part of their core business, not cost centres whose funding can grow or shrink depending on the need to invest elsewhere in the business. IT is a proven contributor to a company's positive reputation—and IT failures can cause significant reputational damage. Fully funded IT risk management efforts, plus investment in the continuing viability of those efforts, can prevent the loss of millions of dollars in revenue when just one IT failure is avoided. Further, redundancy and diversity can eliminate single points of failure and enhance the overall results of reputational risk control.

The benefits of outsourcing

Recent surveys conducted by Forrester Consulting for IBM examined the reasons why an increasing number of organisations are using outsourcing or managed services partners to manage their IT security and resiliency efforts, and the outcome of this decision.

While cost remains the primary motivating factor in the decision to outsource, organisations that outsource reputational and IT risk management are realising valuable additional benefits, including faster return on investment, round-the-clock coverage, consistent access to specialised skills and—perhaps most important—more frequent and successful testing. In fact, IT organisations that outsource reputation and IT risk management often find that they are more confident in their ability to prevent the issues that affect corporate reputation.

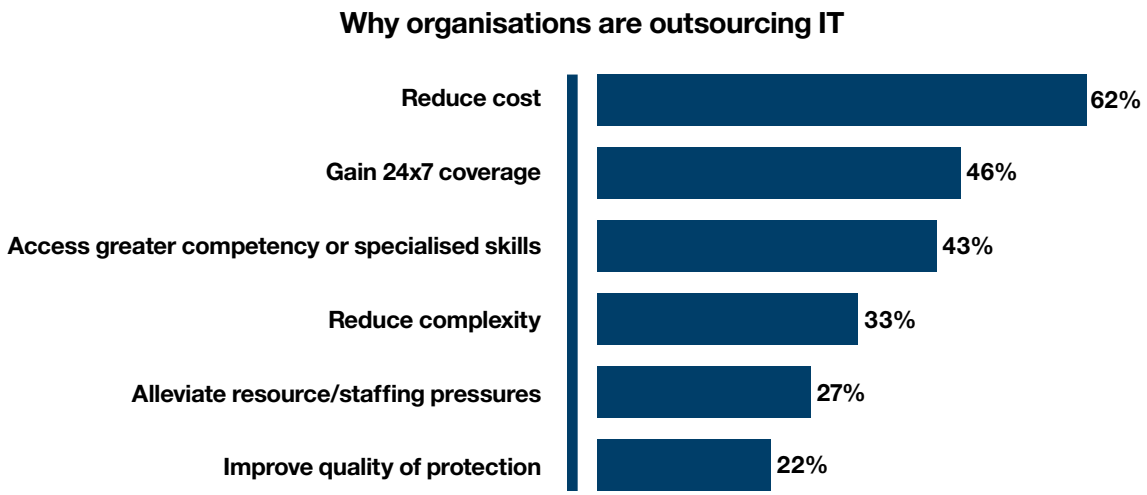
Another important, but often overlooked, benefit of outsourcing: priority, focus and funding do not get shifted to other projects with immediate urgency but less overall importance to the company. Smaller organisations, in particular, should consider outsourcing reputational and IT risk management. Along with saving the organisation money, outsourcing can provide the smaller organisation with expertise and bandwidth that it would be impossible to replicate in-house.

The value of an objective eye

An outside consultancy can provide the objective, end-to-end view of reputational and IT risk that organisations may be currently lacking.

An experienced consultant can address:

- **Responsibility gaps**
- **Strategic and tactical gaps**
- **Viability of current strategies**
- **Integration of IT risk management into overall reputational risk management strategies**



Source: Forrester Consulting[6]

How IBM can help

When planned and implemented effectively, your organisation's reputational and IT risk strategy can become a vital competitive advantage. When you protect against and mitigate reputational risks successfully, you can enhance brand value in the eyes of customers, partners and analysts. Further, your organisation can better attract new customers, retain existing customers and generate greater revenue.

IBM can help you protect your reputation with a robust portfolio of IT security, business continuity and resiliency, and technical support solutions. You can start with an IT security risk assessment, or penetration testing performed by IBM experts. For business continuity and resiliency, you can begin with a Continuous Operations Risk Evaluation (CORE) Workshop and move on to cloud-based resiliency services. Our technical support solutions range from basic software support to custom technical support.

What makes IBM solutions work is our global reach with a local touch. This includes:

- Over 160 business resiliency centres in 70 countries; more than 50 years of experience
- More than 9,000 disaster recovery clients, with IBM providing 100 percent recovery for clients who have declared a disaster
- A global network of 33 security operations, research and solution development centres; 133 monitored countries
- 15,000 researchers, developers and subject matter experts working security initiatives worldwide.

Rate your reputational and IT risk efforts

Is your organisation exposed, aware or capable? Answer a few questions, and IBM's quick and easy online tool gives you an overview rating of your reputational and IT risk management efforts, along with scores in key reputational and IT risk management categories and suggestions for improvement. ibmriskindex.com

For more information

To learn more about how IBM can help your company's reputation by strengthening IT risk management, contact your IBM representative or IBM Business Partner, or visit the following websites:

To learn more about the IBM Global Reputational Risk and IT Study
ibm.com/services/riskstudy

To use the Reputational Risk and IT Index to evaluate your efforts:
ibmriskindex.com

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

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

IBM Ireland registered in Ireland under company number 16226

[1] Google Trends search for "reputational risk," February 2012.
[2,3] "Reputation Impact of a Data Breach: U.S. Study of Executives & Managers,"Sponsored by Experian® Data Breach Resolution Ponemon Institute, November 2011.
[4,5] "Datacentre Downtime: How Much Does It Really Cost?" Aberdeen Group, February 2012.
[6] "The Convergence of Reputational Risk and IT Outsourcing," Forrester Consulting, September 2012.

Please Recycle

RLW03018-GBEN-01