Reputational risk and IT in the banking industry

How security and business continuity can shape the reputation and value of your company

Findings from the 2012 IBM Global Reputational Risk and IT Study

Reputational risk and IT: How security and business continuity can shape the reputation and value of your company is an IBM study that investigates how organizations around the world are managing their reputations in today's digital era, where IT is an integral part of the organization and IT failures can result in reputational damage. The report was written by the Economist Intelligence Unit, which also executed the online survey and conducted the interviews on behalf of IBM.

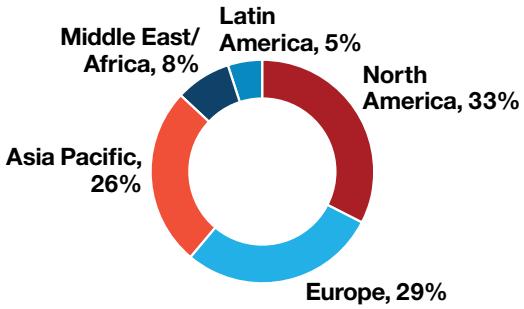
We would like to thank all of the executives who participated in the survey and interviews for their valuable time and insight.

About the survey

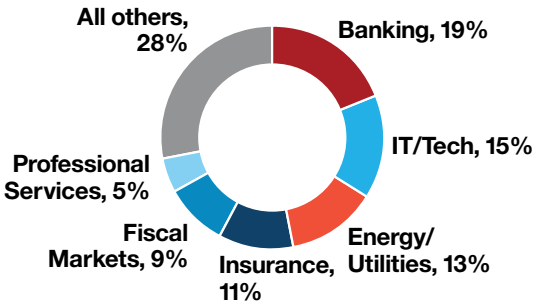
The survey, conducted in June 2012 by the Economist Intelligence Unit, included responses from 427 senior executives from around the world. Of them, 42 percent are C-level executives. About 33 percent of respondents are from North America, 29 percent from Europe, and 26 percent from Asia-Pacific. Companies with less than US$500M in revenue comprise 37 percent of respondents, and 52 percent come from companies with more than US$1B in revenue. The survey covers nearly all industries, including banking (19 percent), IT and technology (15 percent), energy and utilities (13 percent), and insurance (11 percent).

Economist Intelligence Unit | The Economist

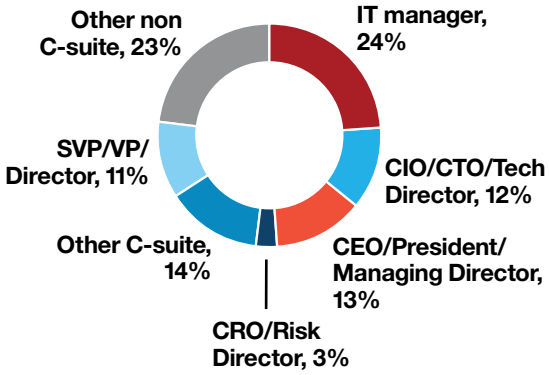
Respondents: 427



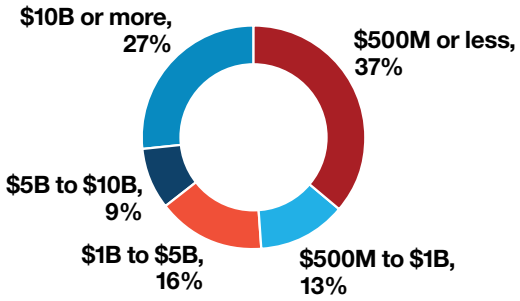
Industries: 23*



Job titles: 15*



Company sizes: 5



*Top responding categories shown

The 2012 IBM Global Reputational Risk and IT Study survey, conducted by the Economist Intelligence Unit, gathered information from 427 senior executives from around the world.

A spotless reputation

Banking industry executives recognize the value of their organization's reputation. A strong reputation generates stakeholder trust. If a bank is trusted, customers will want to do business with it; they will feel confident about using online services; and the good will generated by trust can provide reputational protection should an adverse incident occur.

The unfortunate reality, however, is that any bank's reputation is increasingly difficult to manage in the digital era, and can be easily sullied by any number of factors—among them IT failures. With social media sites such as Facebook and Twitter boasting over 950 million and 500 million users respectively, there is now a highly visible and immediate alternative to a bank's own communications regarding its reputation.

Our research finds that banks in particular have begun to pay closer attention to the links between IT failures and reputational damage. Three principal forces drive a bank's reputation: customer engagement, provision of a best-in-class product or service and trusted-partner status. Considering how banks are becoming increasingly dependent on technology to fulfill all three—to say nothing of running the business—the consensus is clear: IT risk can imperil a bank's productivity, damage customer relations and ultimately erode trust.

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

—Finance director, U.S. bank

While these concerns apply across industries, the study found that companies in the banking industry have especially broad concerns about IT aspects of reputational risk. As providers of critical day-to-day—and increasingly online—financial services to consumer and business customers, virtually every IT vulnerability puts their reputations at risk. As a result, banking industry executives are far more likely than counterparts in other industries to say that IT issues are part of the organization's overall reputational risk management strategy. More than 92 percent say so, compared with 78 percent overall.

Protecting customer assets

As custodians of their clients' assets, banks are one of a handful of industries where IT failures can enable miscreants to steal money, either directly or through capture of confidential customer data. So it's not surprising that banking executives are much more likely (73 percent, as compared to 61 percent of respondents as a whole) to point to cybercrime than to systems failures as the most important IT risk that threatens their company's reputation (see Figure 1).

They explain that cyber-security is a never-ending battle. "Hackers are constantly advancing the ball against the most up-to-date firewalls," says Ed DeMarco, director of operational risk with the Risk Management Association, a financial services professional body. "While banks are constantly buttressing their information with better protection, criminals are always looking for weaknesses, gaps and workarounds." It's a constant cycle, he says: "You build it, they build something better, you build a response to that and then they build something different."

"While banks are constantly buttressing their information with better protection, criminals are always looking for weaknesses, gaps and workarounds."

— Ed DeMarco, Director of Operational Risk, Risk Management Association

Kuray Aslan, senior manager of technology risk for Australia's Westpac Banking Corporation, suggests that the banking business will become even more vulnerable to IT threats in the future. "Over the next 10 years, more and more things will be done online," he says. "What that means for banks is you need technology-savvy management. They really need to understand the cost of not investing in technology infrastructure, because if you're leaving certain pieces behind, that can come back to haunt you."

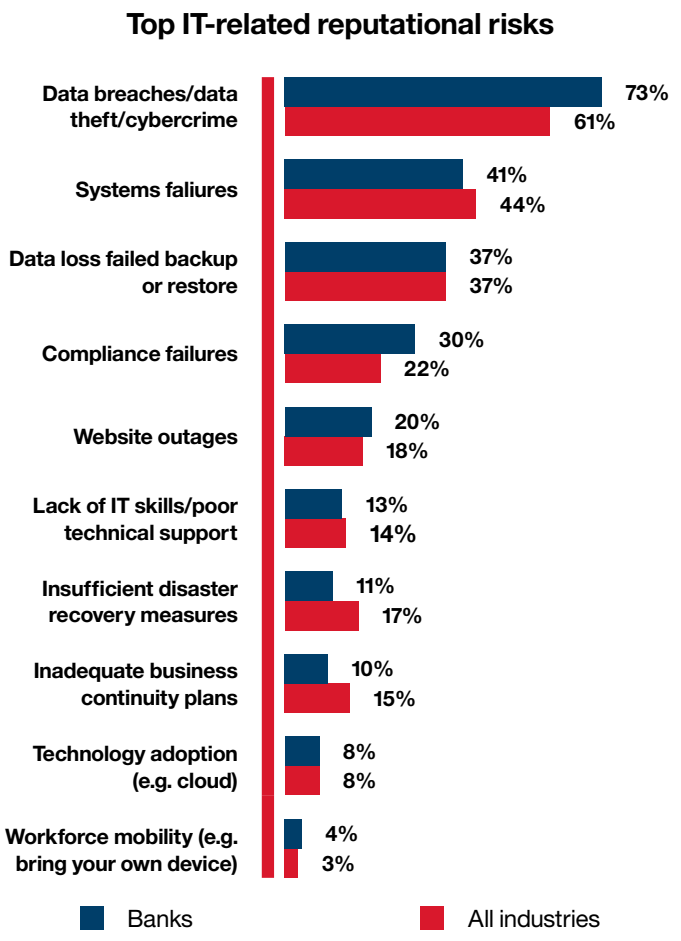


Figure 1. Percent of respondents rating IT risks among the top threats to the company's reputation.

The primacy of trust

Banking is a hotly competitive industry where dissatisfied customers can rapidly switch providers in the wake of a reputational incident. Since many customers hold accounts with multiple banks, switching can be as simple as deciding to do a particular transaction elsewhere. In the consumer space, banks must satisfy a diverse range of demands from different demographic groups, ranging from students seeking their first credit card to families concerned about managing their wealth. This has driven a gradual shift towards greater customer engagement.

"In my opinion," Mr. Aslan says, "banks around the world are on a journey from being product-centric to being customer-centric." In the past, some would argue, banks were all about the products they offered. "But now there's a better appreciation that if a customer is valuable, then I want that customer to do all their business with me, so I need to focus on the customer." Banking executives who were surveyed agree. They rank customer engagement as the single most important factor driving their company's reputation (28 percent), slightly ahead of best-in-class products and services (25 percent).

The increased value placed on customer engagement has important implications for the IT function in banks. Banking executives see much stronger and broader connections than counterparts in other industries between effective management of IT risks and threats to reputation. They draw particularly strong connections between IT risks and customer satisfaction (91 percent vs. 75 percent overall) and brand reputation (91 percent vs. 76 percent). And to a lesser degree they see stronger connections between IT and every other aspect of corporate reputation.

of banks draw particularly strong connections between IT risks, customer satisfaction and brand reputation

of banking executives say that IT failures have severe consequences for compliance

Banks are built on trust – their very existence depends on being perceived as reliable in the minds of customers and other stakeholders. It follows that loss of trust can have serious financial consequences. When asked to rate the degree to which IT failures can harm various aspects their businesses, banking executives point first to customer satisfaction and brand reputation. In both cases more than 90 percent agree that the impacts are strong or very strong. But for banks, the link between IT failure and financial performance is also particularly strong. "Banks are more and more reliant on digital distribution channels," Mr. Aslan says, "so an IT incident could make your business unavailable to customers for a period of time." About 71 percent of banking executives say there are strong impacts on profitability, compared with 61 percent of all respondents. And for stock price the proportions are 55 percent and 36 percent respectively.

Getting Social

Most successful companies use social media to push tailored messages out to consumers. And since these channels are amplifiers of an organization's reputation, companies closely monitor what people are saying about them. The banking industry stands out as a leader in the proactive use of social media to manage operational risks. About one-third of banking executives say their company issues guidelines for employee social media use, and a similar number incorporate social media tools into their disaster recovery plans. This compares with only 19 percent of all survey respondents.

Kuray Aslan, senior manager of technology risk for Australia's Westpac Banking Corporation, believes that the shift to using social media as a risk mitigation tool stems partly from a number of recent banking scandals. These incidents (for example, the Libor controversy) have conveyed a perception that banks have become part of "a culture of greed," he says, and this attracts attention in the media, social or otherwise. "If somebody has a complaint against a bank," he says, "they're likely to be on Twitter with a specific hashtag posting negative comments that a lot of people see because they follow banks with their social media accounts."

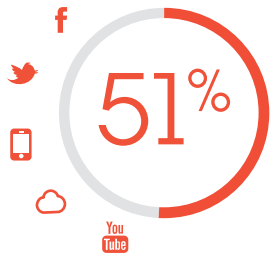
Social media also plays a growing role in responding to IT failures. "Banks tend to have very robust business continuity plans," says Ed DeMarco, director of operational risk for the Risk Management Association. Since they operate across jurisdictional lines and national boundaries with people in different places providing a variety of products and services, "they've got to have a way of communicating in real time if they're going to minimize operational risk and the response time associated with it." Social media can fill that role, he adds, especially since employees can access them on their personal devices when they're not at work.

Companies with social media guidelines for employees

"If somebody has a complaint against a bank, they're likely to be on Twitter … posting negative comments that a lot of people see because they follow banks with their social media accounts."

— Kuray Aslan, Senior Manager, Operational Risk Technology, Westpac Banking Corporation, Australia

This gives these tools power, but this also carries its own risks. "There are lots of complexities whenever you cross the boundary between the individual and the corporation," says a senior risk management executive with a UK-based banking conglomerate, especially when employees are working from home on flexible working arrangements. The solution, he suggests, lies in conveying a consistent set of values to employees. "Our policies require employees to be very clear about whether they're speaking in a corporate voice or a personal one even though they may be at home." This is enforced through training, technology and traditional HR tools, including motivating people through the variable component of compensation.



of responding banks are using social media to communicate with customers.

Mr. Aslan adds that employee guidelines for social media should also address account security issues, such as password protection to safeguard personal accounts from hacking or identity theft. He mentions an incident where someone opened a social media account in the name of a senior bank official and used it to make derogatory comments. "This shows that you not only have to pay attention to what's being said about you on social media," he says, "but your people also have to understand how social media channels work—that's why it's getting so much attention in the banking industry."

"Any breach of customer data would lead to reputational damage if it was revealed by the affected consumer or through the media, especially since this could be attributed to a lack of adequate controls in the institution's IT system."

— Varun Agarwal, Principal, Capgemini Financial Services

For bankers, the customer may be preeminent, but regulators are not far behind in importance. Regulators impose an array of requirements and compliance often depends on the security of IT systems. Banking executives are keenly aware of this: 87 percent say that IT failures have severe consequences for compliance. Varun Agarwal, Principal with Capgemini Financial Services, points to the Federal Reserve System's privacy regulations as a prime example.

"Regulation protects non-public information about consumers and prevents a financial institution from disclosing this information to non-affiliated third parties," he says. "Any breach of customer data would lead to reputational damage if it was revealed by the affected consumer or through the media, especially since this could be attributed to a lack of adequate controls in the institution's IT system." Mr. Aslan adds that regulators around the world apply similar rules: "We've seen a couple of incidents in the UK involving things like data loss and security breaches. The financial institutions involved were fined because of IT-related breaches."

A deep toolbox

Banks tend to lead other sectors in the development of sophisticated IT risk control strategies. They are much more likely than firms in other industries to have adopted a comprehensive range of procedures, processes and controls to manage IT risks.

Compared with other industries, banks are much more likely to have implemented proactive measures like penetration testing/ethical hacking, intrusion detection procedures, annual security assessments, managed and monitored security controls and vulnerability scanning. The survey asked respondents about more than 20 categories of IT risk control, and uptake by banks exceeded the all-industry average for every one of them. Banks are also more vigilant than other firms in requiring supply chain partners to match their internal levels of IT risk control. About half of banking executives say they do this "strenuously" compared with less than one third of all respondents.

"Banks are very technology-driven and very technology-dependent, and when you invest a lot in technology and are very savvy with it, you embrace emerging online communications tools."

— Ed DeMarco, Director of Operational Risk, Risk Management Association

Managing reputational risk involves a large communications dimension. Preventing failures is critical, but convincing stakeholders that robust controls are in effect is the other half of the equation. Increasingly, banks are turning to the social media to get the message out. "Banks are very technology-driven and very technology-dependent," says Mr. DeMarco, "and when you invest a lot in technology and are very savvy with it, you embrace emerging online communications tools."

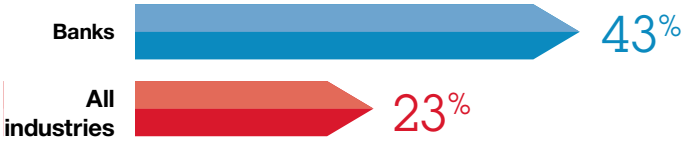
He adds that since social media allow a high level of audience segmentation, "it is possible to influence people by tailoring messages as they move through the different phases of their lives and relationships with a bank." Mr. Aslan suggests that the proliferation of web-based services in the financial services sector has advanced this trend. "Banks figured out that having brand advocates who are active on social media sites can help you a lot," he says, "and it's a very cost-effective way of promoting your business and letting people know about your products."

Shared responsibility across the C-suite

Effective reputational risk management necessarily requires collaboration across the organization. As in other industries, accountability for the company's reputation rests in the C-suite, typically with the CEO. But banks differ in the degree that responsibility is shared by other C-level executives with specialized risk management roles. The survey found that banks are nearly twice as likely (43 percent) to have a chief risk officer (CRO) than the average company (23 percent). Banks are also much more likely to appoint a compliance officer.

Senior-level risk management specialization in part reflects the growing complexity of the banking industry, with an array of profit centers ranging from deposit-taking to investment management, each with its own hierarchy of risks. "As a result," says Mr. Aslan, "it's hard to tell what the reputational impact of one incident means to the overall business." This long-term trend towards financial services companies appointing CROs is the case even where they are not legally required to do so (in the US, large banking companies are obliged to do so under the Dodd-Frank Act).

Companies that have appointed a Chief Risk Officer



Senior-level risk management specialization reflects in part the growing complexity of the banking industry

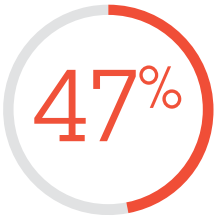
The goal is not to avoid risk, but rather to ensure that the bank earns an appropriate return for accepting it, Mr. DeMarco says. "When a bank makes a strategic decision to engage in a new product or service that has an IT component, they must assess the potential reputational harm if the project is less than successful."

This high level of awareness of the complexity of IT-related reputational risks also reflects the fact that the frequency of adverse incidents in banking is rigorously tracked and well understood. The survey found that banking executives report the frequency of severe IT incidents in several categories at more than double the rate of respondents in other sectors. For example, 27 percent of banking executives report recent severe incidents of data theft/cybercrime compared with only 12 percent overall.

"When a bank [launches] a new product or service that has an IT component, they must assess the potential reputational harm if the project is less than successful."

— Ed DeMarco, Director of Operational Risk, Risk Management Association

of banks will increase their focus on managing reputation going forward



of banking executives say that events in the industry or at their banks are behind the increased focus on reputation

According to Mr. Aslan, these statistics simply reflect a higher level of awareness, due to the fact that failures and other incidents are very well defined in the banking industry, "so if you ask a banking executive how many failures there have been, he's likely to know." He continues, "I think this is partly due to the operational risk discipline that banks follow as well as financial services regulations, worldwide, and the kind of risk guidance that comes from international agreements like the Basel Accords."

Conclusion

The trend towards diversification of accountability for integrated enterprise-wide risk management within the C-suite is evident across the banking industry. The links between IT risks and reputational damage have been clearly recognized. Understandably for an industry that depends on trust for its very existence, data theft and cybercrime will continue as the top priorities. At the same time, however, there is a growing recognition that the industry is becoming more complex, and will rely even more on IT support for critical business systems in the future. Indeed, executives who were surveyed or interviewed for this study suggest that banking enterprises are beginning to shift their risk strategies in a number of ways:

- Banks are already ahead of other industries in terms of investing in managing reputational risk and are only increasing their emphasis. Three-quarters of banking executives say their organization will focus more on managing its reputation than five years ago, a higher proportion than in any other industry.
- They will pay increasing attention to the specific needs of individual customers than in the past, with less focus on broad product offerings. Customers will want to deal with banks using digital channels for a wider range of services.
- They will face a continuing – and even escalating – battle with a diverse array of troublemakers that includes a growing organized criminal element, capable of inventing new holes even as security barriers are tightened.
- Responsibility for reputational risk will remain diversified as the industry becomes more complex and the array of IT risks grows. Senior executives will need to become increasingly IT-savvy to understand the need for investment in IT solutions.

"Banks around the world are on a journey from being product-centric to being customer-centric."

— Kuray Aslan, Senior Manager, Operational Risk Technology, Westpac Banking Corporation, Australia

---

For more information

To learn more about how IBM can help you protect your organization's reputation by strengthening IT risk management, contact your IBM representative or visit the following websites.

For security and IT risk management, visit:
ibm.com/services/security

For business continuity and IT risk management, visit:
ibm.com/services/continuity

For technical support and IT risk management, visit:
ibm.com/services/techsupport

View the IBM reputational risk and IT infographic at:
ibm.co/repriskinfographic

Add your voice to the discussion

Your opinion matters! Participate in the extension of our 2012 reputational risk and IT survey. Just scan the quick response code here or go to **ibmrisksurvey.com**

Your input will be added to what we anticipate will be the largest survey ever conducted on this important subject. You will receive the new analysis and report on the survey findings in early 2013. Thank you very much for your participation.

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
October 2012

[1] *Key trends driving global business resilience and risk: Findings from the 2011 IBM Global Business Resilience and Risk Study.* September, 2011.

[2] *Reputation: Risk of risks.* Economist Intelligence Unit. December, 2005.

Please Recycle

RLW03010-USEN-00