

Forbes
INSIGHTS

FALLOUT

THE REPUTATIONAL IMPACT OF IT RISK



IN ASSOCIATION WITH:



CONTENTS

Executive Summary	2
Introduction: The Black Friday data breach.....	3
Where the Risks Are: From Human Error to System Failure	5
Sidebar: The Promise and Perils of the Cloud.....	11
Protecting Your Reputation in the Always-On World.....	12
Conclusion	18
Acknowledgments.....	19



EXECUTIVE SUMMARY

U.S. retailers were not the first to suffer a massive data breach. Nor will they be the last, as cyber attacks, security breaches and system outages proliferate. Shadow technology and expanding supply chains bring more risks. How can companies better protect their reputation by ensuring the continuous—and secure—flow of information to support their business?

After all, a major part of the brand experience for most customers comes through the technology that delivers or supports the business. When that technology doesn't work, it's not just a problem for the tech team; an organization's reputation can suffer, and reputation is a board-level concern. Security and resilience affect nearly every part of an organization in the always-on world. Working through the challenges of emerging technologies, such as implementing a cloud strategy, can be a means to reassess not only data storage and transmission but any business function that requires data: compliance, finance and human resources, for example.

Strategies to protect IT security and business resilience can align with a company's broader corporate goals—from protecting intellectual property to maximizing productivity to minimizing customer defections.



INTRODUCTION

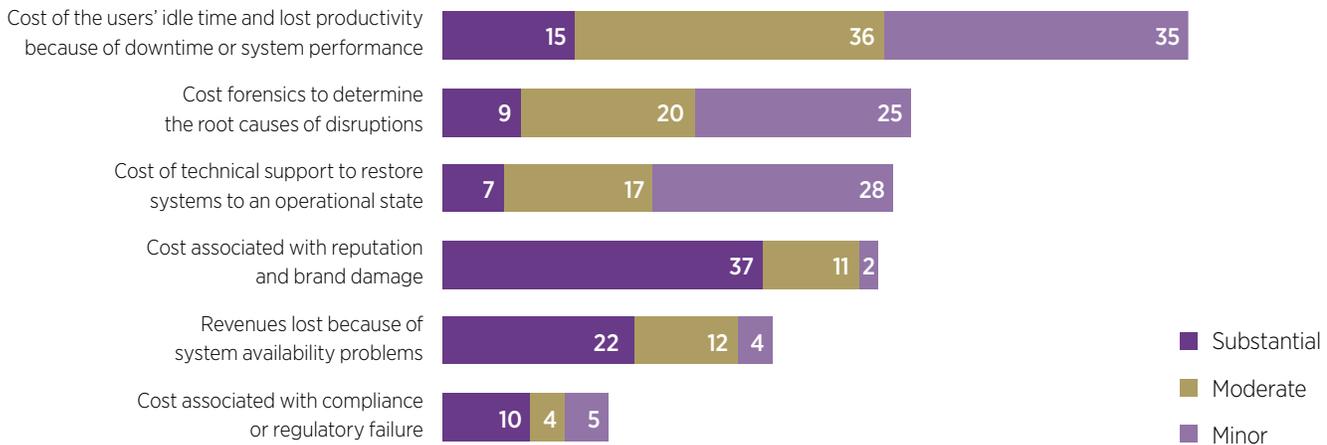
The holiday data breach at U.S. retailers gives new meaning to the term Black Friday. Just as merchants entered into their busiest shopping season, malware installed through a third-party vendor on credit card readers began uploading credit and debit card data to cyber thieves. From just before Thanksgiving until shortly after the U.S. Justice Department became involved in mid-December, hackers made off with data from at least 40 million accounts, including PIN numbers for debit cards. Forensics revealed that the names, addresses and phone numbers of tens of millions of customers had also been compromised. That number could grow as the investigation continues and more retailers become aware of the extent of the breaches.

In the weeks before Christmas, sales fell sharply at affected stores. There was no business disruption at the stores or the back office, but there was for many of the retailers' customers. Some started seeing fraudulent charges on their credit cards. Several card-issuing banks canceled all accounts that may have been compromised by the breach. Others added new credit limits, leaving customers without a credit card during the holidays. Retailers will be on the hook for many of those costs. Expenses related to the data breach are forecast to reach into the billions.

Technology professionals and business continuity experts know how expensive an IT security breakdown or business disruption can be. Lost revenues, downtime and the cost of restoring systems can accrue at the rate of \$50,000 per minute for a minor disruption, according to the business continuity and IT security executives who responded to the IBM Global Study on the Economic Impact of IT Risk conducted by Ponemon Institute. But what about the greater toll a sustained outage or major security breach can take on a company's reputation?

Firms surveyed in a similar IBM study conducted in 2012 reported that the reputational damage lasts months—far longer than recovery times and long enough to affect quarterly results in most cases. For a major incident, such as the data breach suffered by U.S. retailers, the effects could last years. Reputation has always been a thorny thing to value in dollar terms. But there are costs associated with a disruption or breach that can be measured (Fig. 1).

FIGURE 1. SUBSTANTIAL DISRUPTIONS POSE THE GREATEST RISK TO REPUTATION AND BRAND VALUE



For each of the three levels of disruption (minor, moderate and substantial), respondents were asked to use a 100-point scale to apportion total costs across these six cost categories.

Source: [The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013](#)

If customers can't log on to your site, you not only lose a sale today, but you also risk losing future business, particularly for retailers. For financial institutions, a security breach can scare away customers and open the door to fraud. A network outage for any telecom or IT company may leave clients wondering why they should trust their own reputation to a vendor who might make them look incompetent. This is particularly true for the providers and the users of cloud technology.

Winning back trust also has a cost. Just ask the staff at retailers who worked around the clock through the Christmas holiday, trying to answer questions from customers and the press. The retailers involved are trying hard to put their customers first by promising zero-liability protection for any fraudulent activity as a result of the breach. But the head of any organization would be wondering at this point: "What could we have done differently before this happened?"

The retailers involved still have many questions to answer. The malware used in at least one attack was a relatively unsophisticated, off-the-shelf exploit kit that can be easily modified and redistributed with little programming skill or knowledge of malware functionality, says software security firm McAfee in its fourth-quarter security

report. According to McAfee Chief Technology Officer Michael Fey, defending against such an attack doesn't require a new silver bullet; it requires a cost-effective way of deploying technology that already exists. And the problems persist; another retailer reported a fresh attack as late as March 2014.

"You will be held accountable for what you did or didn't do in the months and years leading up to a crisis," explains Prof. Daniel Diermeier, the IBM Professor of Regulation and Competitive Practice at the Department of Managerial Economics and Decision Sciences at the Kellogg School of Management. "You are only as good as the decisions you made when you put your systems in place."

How can companies better protect themselves against cyber attacks, security breaches, data loss, system outages and the most difficult-to-control threat: human error? What new risks does the cloud bring? How do executives view the risks that these failures can pose to their company's reputation?



WHERE THE RISKS ARE

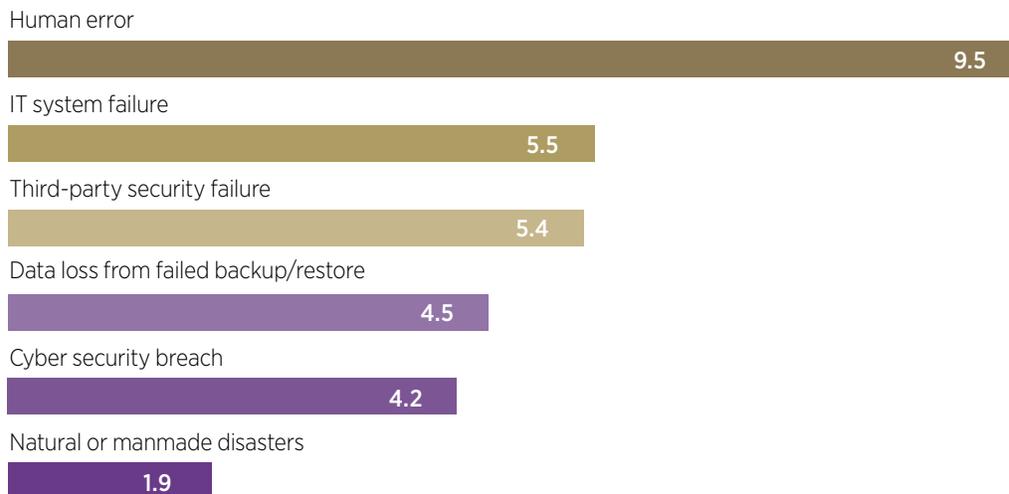
HUMAN ERROR

“The biggest business risk for us and for most companies is a data breach or system failure,” says Patricia Titus, Chief Information Security Officer of Freddie Mac. “But the biggest challenge is the potential for human error.”

In fact, human error is named as the threat with the highest economic impact by the IBM study. Whether it’s a fat finger hitting the wrong key or someone spilling coffee on the server, human error is responsible for nearly a third of IT disruptions—the leading cause. “We can secure the doors, we can button down the system, we can put on behavior and insider threat detection and employ counter-intelligence,” says Titus. “But we also have to remember how vulnerable an entire system can be to one person making a mistake.”

For business continuity managers, the potential impact of human error looks broader and deeper as the world becomes more social and interconnected, says Paige Poore, Director, Global Business Continuity Management for IBM. “From a process perspective, from an IT perspective, it becomes clear that an organization needs a single integrated risk management strategy for business continuity and IT risk that is supported and executed across the enterprise.”

FIGURE 2. AVERAGE NUMBER OF DISRUPTIONS OVER THE PAST 24 MONTHS CAUSED BY SIX COMMON THREATS



Source: The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013

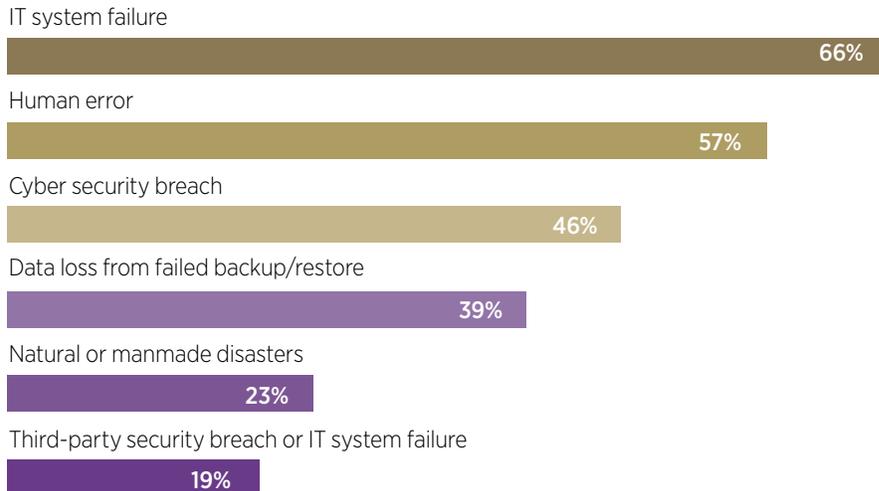
IT SYSTEM FAILURE

When online and mobile brokerage systems went dark for a few hours on January 8, customers flooded the twittersphere with tales of all the money they lost during the outage. At least two firms experienced an outage that day. Was it a distributed denial of service attack? Customers have a lot of questions, but some aren't waiting for an answer.

In fact, IT system failure was the most widely reported threat to affect reputation and brand value in the IBM study. This is a broad category that can include everything from a cyber attack to someone accidentally pulling the plug on a server. (See "Human error.")

This is what happened to a train line in New York in January when technicians cut the power supply to the computers that run the railroad's signal system. The head of the railroad acknowledged that the project should have been analyzed for risks beforehand, and not performed while commuters were trying to get home in wintry weather.

FIGURE 3. PERCENTAGE OF ORGANIZATIONS THAT HAVE EXPERIENCED DAMAGE TO THEIR REPUTATION AND BRAND VALUE DUE TO COMMON THREATS OVER THE PAST 24 MONTHS



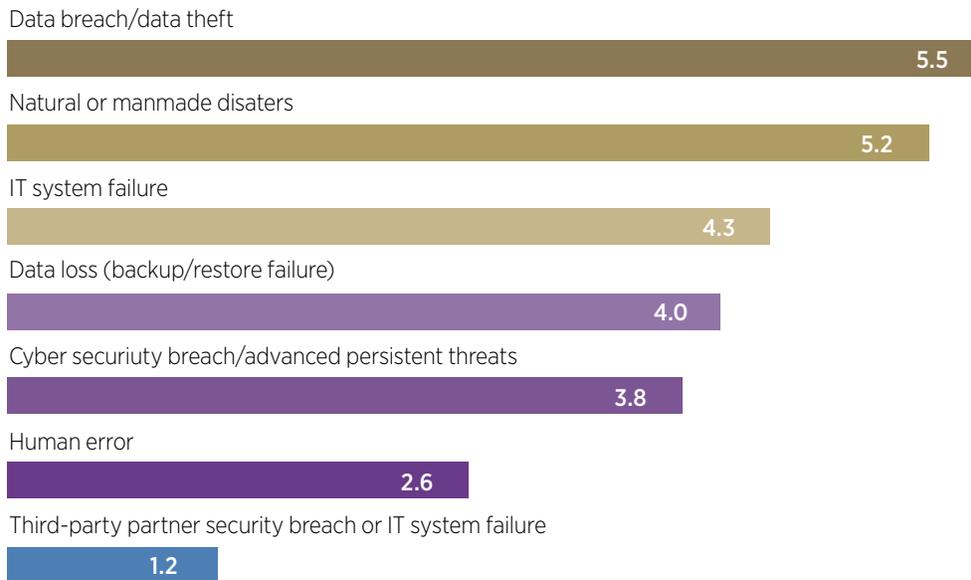
Source: The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013

SECURITY BREACH

In terms of reputational impact, a security breach has the potential to do the most damage. Cyber security is one of the most vexing risks faced by any company. Even for an organization that is doing everything it can to safeguard its data and systems, attackers will always have the advantage. An attacker needs to find only one weak point in a system's defenses, while a system's protectors need to defend all vulnerable points forever. The Internet was built in a way that favored resiliency over security.¹

That tradeoff between strong security and a more open, easy-to-access environment is echoed in the dilemma facing many organizations and the protectors of their systems: How do you provide always-on service while protecting your data, your customers and your reputation from hackers? How do you provide a flexible environment while also being secure?

FIGURE 4. COMMON THREATS RANKED IN TERMS OF REPUTATIONAL IMPACT



Source: The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013

¹Global Risks 2014, Ninth Edition, World Economic Forum, pg. 39

DATA LOSS

Data loss is named as the fourth most common threat to reputation in the IBM study. Yet it is one of the easiest threats to avoid. By automating backup, any enterprise, large or small, can avoid most data loss. With the advent of the cloud, backup can be both automated and outsourced. Nonetheless, data loss is still named as a common threat by many organizations.

When service is disrupted because of a data loss, customers tend to be less forgiving than they would be in the case of something perceived to be outside a company's control, such as a natural disaster. In Africa, a fire last summer gutted the international terminal of a major airport, including part of the data center, and forced its temporary closure. Fires like the one in Africa may or may not be avoidable but data loss can be minimized or prevented.

“When I consider
the possibility of
[the electromagnetic
interference] threat,
I have to wonder:
Does anybody hate us?”

—FRANK LADY
SVP, Business Continuity,
Bank of America

NATURAL OR MANMADE DISASTER

Business continuity specialists lie awake at night contemplating such black swan events as, what would happen if space junk knocked out our GPS? What if Silicon Valley were swallowed by an earthquake? What if electromagnetic interference caused a shutdown? Such interference can be delivered by anyone with a grudge for as little as \$10,000 in a device the size of a small suitcase and can seriously impact an institution's technology infrastructure, says Frank Lady, senior vice president of business continuity at Bank of America. “When I consider the possibility of that threat, I have to wonder: Does anybody hate us?”

Disruptions from unpredictable sources can wreak havoc on any firm, even a global giant such as Toyota. The massive 2011 earthquake and tsunami disrupted the automaker's supply chain for months. Customers, regulators and vendors may be understanding in the wake of a disaster, but if a company cannot restore service in a timely way, sales will be lost and trust will be shaken.

THIRD-PARTY BREACH OR SYSTEM FAILURE

Almost half of the respondents in the IBM study said that most of the disruptions they experienced were caused by a third party's IT or security failure. Yet when IBM asked whether or not these companies require partners to comply with their own internal requirements, an alarming percentage said "no." For IT, 40% do not require third-party compliance with security measures, while the figure for business continuity is 31%.

Compliance for business continuity is easier to quantify. There are international standards and guidelines. Partners either have an acceptable continuity or disaster recovery plan or they don't. IT security, where the threat landscape changes daily, is not as straightforward.

FIGURE 5. PERCENTAGE OF DISRUPTIONS TO BUSINESS AND IT OPERATIONS CAUSED BY THIRD PARTIES OVER THE PAST 24 MONTHS

Zero	1%
<25%	21%
26 to 50%	37%
51 to 75%	20%
76 to 100%	21%

Source: The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013

"This is one of the most significant risks that organizations have but don't recognize," says Dr. Paul Robertson, Director, Business Resilience at PricewaterhouseCoopers. "With the rise of outsourcing there are a whole bunch of people in the supply chain who want to interface with your systems. The spread is so phenomenal, yet the IT department can only control what exists in-house. External controls are through service agreements and contracts. It's a horrific place to be to retrospectively try to put resilience into the mix or put some sort of risk control in place, because you have a series of third parties who have never been part of that conversation."

A pharmaceutical business, for example, recently had its data corrupted by a vendor. "It wasn't corrupted in a

way that you could look at it and clearly say, 'Oh, that's all wrong.' It was corrupted in a way that was incremental. Instead of seven boxes, it read eight boxes; instead of lot number one, it was lot number two," Robertson explains. "And the corruption had taken place for weeks." Fixing the data cost the firm thousands of dollars.

What's more, the breach created an awkward situation with regulators. No matter the source of the corruption, the pharmaceutical company is ultimately responsible, as far as regulators are concerned. "When you're talking about a highly regulated business with dozens or hundreds of suppliers and third parties involved in the process, the scope for even small things turning into a big crisis is phenomenal and very scary," Robertson says.

OVERLAPPING THREATS

Of course, these common threats do not exist in isolation from one another. Human error can lead to data loss, for example. A cyber attack can cause a system outage. Or, as in the Black Friday incident, unprotected dealings with a third party can lead to a data breach that reverberates throughout the financial system for months. In fact, the economic and reputational risk of a third-party security breach or IT failure is emerging as one of the most difficult to quantify or manage.

“Some risks are caused by the growing complexity and globalization of what we do,” says Chris Green, head of business continuity at Qatar Air. “The difficulty in the supply chain discussion is even understanding that chain. Firms have suppliers, who have suppliers, who have suppliers. Who performs the assurance, and to what depth of understanding, and at what cost?”

“The difficulty in
the supply chain
discussion is even
understanding that chain.
Firms have suppliers,
who have suppliers,
who have suppliers.”

—CHRIS GREEN
Head of Business Continuity,
Qatar Air

THE PROMISE AND PERILS OF THE CLOUD

Every company needs electricity, but that doesn't require building a power plant. Many organizations have reached the same conclusion about computing and storage needs. Why build out data centers if that's not your core business?

There is one big difference, however, and that is security. How do you secure something over which you have no physical control? And how do you handle resiliency and latency?

Companies in highly regulated industries—finance, pharmaceuticals, defense or transportation, to name a few—have unique security and compliance concerns. Any government contractor, for example, may be prohibited from sharing data with a foreign enterprise. What happens if a cloud provider uses offshore resources to maintain the infrastructure? How is data protected?

Patricia Titus, CISO of Freddie Mac, has worked in several highly regulated industries. "I'm not afraid of the cloud, but you still have to be careful. You don't take your crown jewels and put them on the public cloud." She says, "You have to write a good contract and know the company from a reputation perspective. You have to know the right questions to ask."

Chris Green, head of business continuity at Qatar Air, has a similar view. "If you have performed a proper risk evaluation as well as a technical evaluation, then you can make an informed decision. In one sense, it's no different from outsourcing your contact center; you are just outsourcing some of your technology infrastructure. If you're worried about the security, then you haven't done your risk assessment properly—or you haven't made the right risk choice!"

Our contributors have some good advice for managing a cloud strategy.

- Develop an exit strategy from the start. The first question you need to ask is "What happens to my data?" What if

you want to move to another provider? Some providers translate data to a proprietary application. If you don't have the intellectual property to read it, it's just ones and zeros.

- Talk to your security people before you move any data to the cloud.
- Ask: what if we need to run forensics?
- How often is data backed up?
- How is data encrypted? Is it encrypted at rest as well as in transit?

**"YOU DON'T
TAKE YOUR
CROWN JEWELS
AND PUT THEM
ON THE
PUBLIC CLOUD."**

**-PATRICIA TITUS
Chief Information Security Officer,
Freddie Mac**



PROTECTING YOUR REPUTATION IN THE ALWAYS-ON WORLD

Then there's the difficulty of dealing with these risks in real time in a wired world. Customers expect the same consistency, whether it's watching a movie on an iPad, withdrawing money from an ATM anywhere in the world, or finding the product they want on the shelf when they want it. And when they entrust an organization with their personal data, they expect it to be protected. Any company that fails to live up to these expectations risks the kind of viral publicity that can scare away customers, destroy stock prices and lead to months of trust rebuilding.

"Social engagement is powerful," notes Laurence Guihard-Joly, General Manager, Business Continuity & Resiliency Services, at IBM Global Technology Services. "Before, we only talked about big disasters. Now when something goes wrong, everyone knows about it pretty fast. The disruption from human error, system outage or loss of data, even a minor disruption can have a significant impact on your reputation. A cost, first, but also a real impact on whether people will choose your service."

She cites the use of mobile maps as an example. "Before, if you needed directions, you would go online and print out a map. Now, most of us will type the address into our smartphones and listen to the directions. Millions of people do this every day around the world. We take

it for granted that service will be there." Customers are connecting with traditional businesses in new ways as well. Airlines, for example, offer apps that helped reroute passengers who missed flights during the endless snowstorms of 2014, as did Guihard-Joly when she was trying to fly out of Las Vegas and back to the East Coast. "I felt I had a friend trying to help me," she says, "and I sure needed that service to be fully available."

This new model of engagement through social media and networking is constantly expanding as every product from baby monitors to refrigerators to automobiles gains the ability to connect to a network. Known as the Internet of Things, this connectivity offers tremendous potential to interact with consumers as well as manage production and distribution. It also makes any service disruption more costly and visible. "Having always-on business continuity is becoming core to any activity, even for physical objects," says Guihard-Joly. "If you promise always-on service, you must deliver always-on service. You cannot just say, for instance, 'I was attacked by bad guys.' That is why having security and resiliency embedded in your IT infrastructure as well as your processes is becoming critical—above and beyond the threat from hackers."

FIGURE 6. ESTIMATED REPUTATION-RELATED COSTS RESULTING FROM DISRUPTION TO BUSINESS OR IT OPERATIONS OVER THE NEXT 24 MONTHS

Minor	Moderate	Substantial
\$20,929	\$468,309	\$5,274,523

Source: The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013

EMERGING RISKS = EMERGING OPPORTUNITIES

How can you protect what you can't control? For the security professions, that is the dilemma of shadow IT—the use of smartphones, tablets or any other hardware or software not part of an organization's sanctioned infrastructure—and social media, as well as the elaborate interconnectedness of the global supply chain and the always-on economy.

The warnings about shadow IT sound like they could be descriptions of a black market during wartime. “Organizational dysfunction,” “barriers to enhancement” and “data hoarding” are some of the headings on the Wikipedia entry for shadow IT. One thing is certain: unsanctioned IT is a security challenge, whether or not its users are guilty of any of these crimes.

“There is more power in the hands of end-users,” explains Larry Ponemon, chairman and founder of Ponemon Institute. “From a continuity management perspective, this is most difficult, because you don't have the usual capability to know what people are doing.” Uploading sensitive data onto a memory stick, running company spreadsheets outside of a secure VPN, using a drop box to store plans for a prototype—all of this data is invisible to the IT security team. “If you can't see what's going on, it's much harder to recover when there is an event,” says Ponemon.

Personal computers have 20 years of security built into them, says Freddie Mac's Titus. They grew up with the criminals that attack them. Tablets and smartphones are so new that innovation is getting ahead of security, and security is not being built in to the consumer-grade products. “This explosion of mobility has created a whole new dimension of security. How do I protect the data that's going into a device that can be dropped into a commode? You can lose information. You can lose intellectual property,” says Titus.

Mobile computing may be a challenge for IT security, but it is a tremendous opportunity for many businesses to

expand their reach to employees and consumers. People expect the same experience whether they're at the office, at home, in a coffee shop or at the airport. Progressive CIOs are embracing the idea of providing different applications for employees to get their job done wherever they happen to be.

Even at Freddie Mac, whose customers are financial institutions, “we are going through a generational upgrade to our workforce,” says Titus. “We need to be able to provide enabling technologies that we didn't have to provide previously. You can't turn a blind eye to big data, the cloud and mobility. You have to embrace them, and if you don't embrace them, I can guarantee that in most companies you won't have a job for long if you're the office of 'no,' otherwise known as the sales prevention team.”

Ultimately, many organizations are finding great benefits with a hybrid approach that blends mobile, cloud-based and on-premise IT resources to address key elements of risk management, says Kris Lovejoy, General Manager, IBM Security Services. “Securing these infrastructures can be complicated without a single, integrated management system that avoids creating silos of data, making it almost impossible to uniformly monitor security risks and threats across environments,” she explains. “One key trend we are seeing is senior management and the board asking the CIO's office to map out a strategy for deploying new security services and solutions that are designed to break down those silos and better secure data no matter where it resides.”

TAKING THE CASE TO THE C-SUITE

Building a resilient enterprise may be accomplished at the operational level, but charting a course for the best way to protect and engage customers in the always-on world is a question of strategy that goes beyond the IT department. “There has been a sea change in the way companies are viewing IT risk to reputation over the last few years,” says the Kellogg School’s Prof. Diermeier. Many C-suite executive and board members, he says, are already thinking about the damage that a cyber breach or system outage can have on brand image and stock prices. “Corporate boards are more worried,” he notes. “They are particularly concerned about black swans, social media and what their suppliers are doing.”

Years of practice in business continuity has taught PwC’s Robertson that in a crisis, it will always be those most senior people who will be facing questions. “It always lands back at the C-suite, regardless of operational impact,” he says.

At some larger companies, chief risk officers, chief security officers, chief marketing officers and other CXOs are asserting themselves in what was once the domain of the IT department or business continuity management. They may also become natural allies in the progress toward better security as well as enhancing engagement with customers, suppliers and regulators. “What do you

do with marketing teams who have this unbridled enthusiasm about how they want to use the cloud and employ all forms of social engagement and generate lots of data?” asks IBM’s Poore. “The answer is you support them and help them understand the risk tradeoffs.”

The flipside, she says, is that marketing people understand the value of protecting the brand by building a resilient system that can deliver as promised. “At IBM, we’ve established governance on continuity that goes all the way to the top,” she says. “Across the enterprise, we have strategic risks, new market risks, integration risks, and we have to look at the ripple effects they cause. We’ve looked at not only the traditional siloed view but also the end-to-end view of interdependencies across the global enterprise,” she says. “Taking a holistic view is an increasingly critical aspect of managing business continuity and reputational risk.”

At financial institutions, business continuity professionals might find themselves working more closely with the chief risk officer, says Bank of America’s Lady. “It’s a natural fit for most financial institutions, which are used to dealing with all sorts of risk, from credit risk to counterparty risk. Adding operational or technological risk to the equation makes sense and gives business continuity planners a voice on the board.”

THE POWER OF COLLABORATION

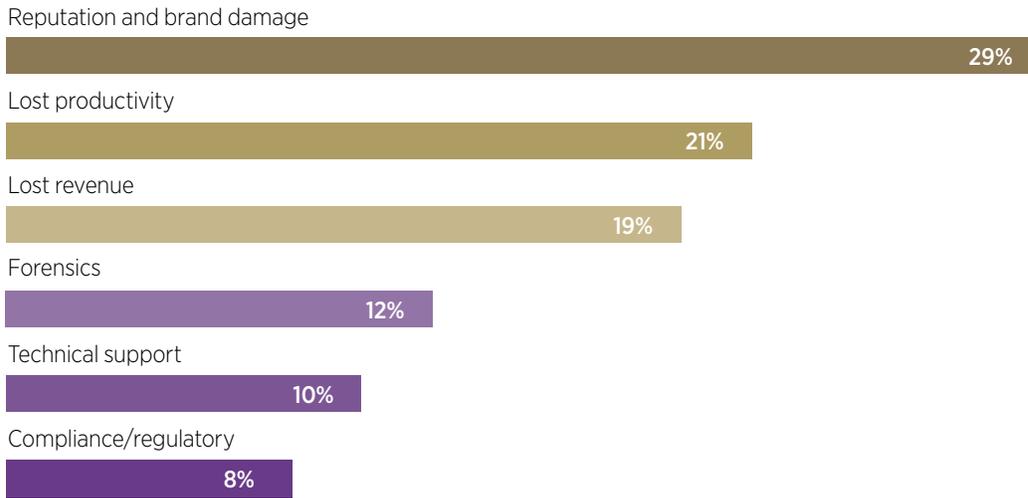
Collaboration extends beyond the board. “Cyber risk, for example, is phenomenally challenging because you’re asking all of the protective disciplines to work together toward a strategic solution rather than operationally tick off line items,” says Robertson. Some firms have already married their continuity management with their IT management, adds Ponemon.

For some companies, assembling a virtual team makes more sense than creating a new C-level post. Robertson explains why: “You can improve resiliency by creating links between different disciplines, especially when you’re in an environment where you need to do more with less. You can make a pretty effective virtual team with existing resources, as long as they have the right strategic goal and remit to act.”

At Freddie Mac, the security practice is organized to ensure there are touchpoints into every business unit, so that there is visibility and assistance if needed, says Titus. “Security is not a simple thing to navigate. You want to make sure it’s transparent but not so transparent that people forget about it. It’s finding that gentle balance.”

One thing is certain: as long as the continuous flow of information is central to the success of a business, the consequences of IT risk expand well beyond the IT department. In fact, more than 75% of the total costs of business continuity and IT security failures represent bottom-line business costs rather than departmental IT expenditures, according to the IBM study.

FIGURE 7. FINANCIAL IMPACT BY COST CATEGORY

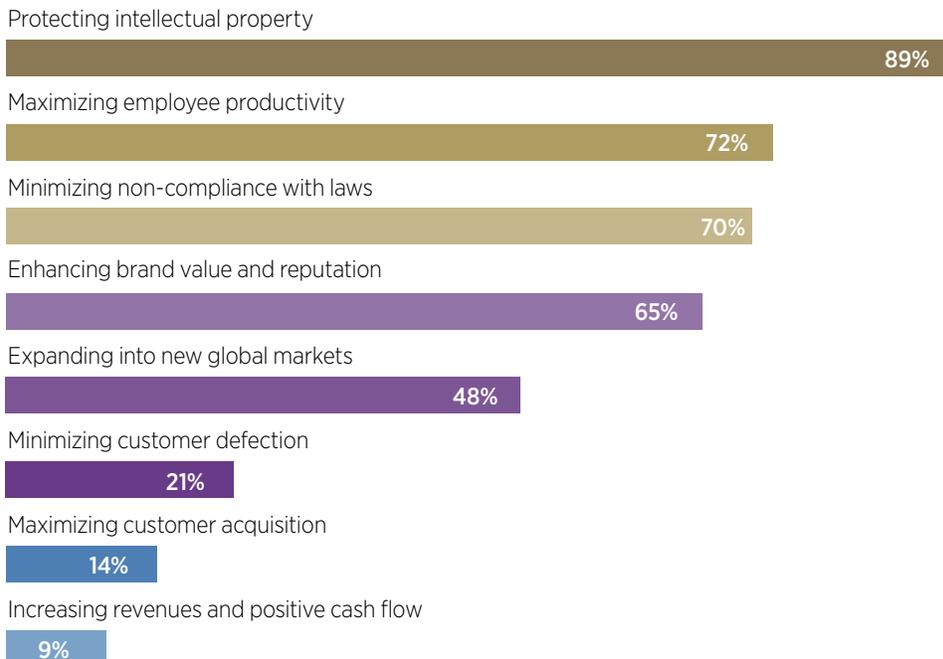


Source: [Understanding the economics of IT risk and reputation: Make the business case for business continuity and IT security with timely cost-based insights and recommendations drawn from the IBM Global Study on the Economic Impact of IT Risk, November 2013](#)

Likewise, many of the objectives of the protective disciplines align with broad corporate goals, such as maximizing productivity, meeting compliance requirements and enhancing brand value. Moving to the cloud, for

example, is an opportunity to reexamine everything, from the finance system to enterprise resource planning to the helpdesk. It is a means of improving business efficiency.

FIGURE 8. BUSINESS OBJECTIVES ADVANCED BY BUSINESS CONTINUITY AND IT SECURITY MANAGEMENT ACTIVITIES



Source: The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013

THE CHALLENGES OF THE CORPORATION

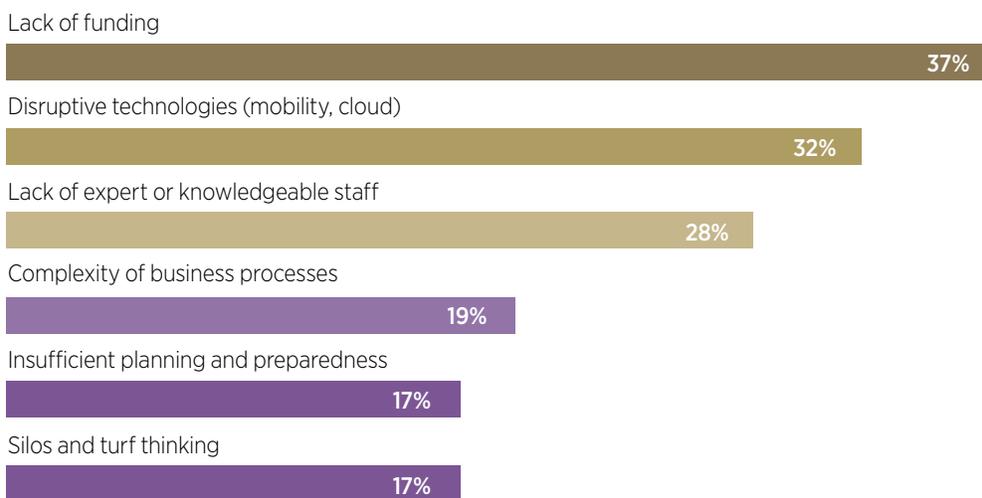
Partnering with the rest of the business may be essential to achieving an effective business continuity or IT security program, but 44% of respondents in the IBM study report that collaboration is poor or nonexistent in their companies.

Part of the problem is a lack of communication, explains Titus. “There is a translation issue between Internet security and the board. Most IT executives don’t know how to translate security risk to business risk without communicating fear and doubt,” she says. “This is a big problem for us. You think you’re speaking English but you’re talking in techno babble.”

A lack of expertise can also complicate security programs. In IT, especially, “the turnover rate in management is very high,” says Ponemon. Related challenges include silo and turf thinking.

The greatest challenge named in the IBM study, however, was a lack of funding.

FIGURE 9. BARRIERS TO ACHIEVING A HIGHLY EFFECTIVE BUSINESS CONTINUITY OR IT SECURITY PROGRAM



Source: The economics of IT risk and reputation: What business continuity and IT security really mean to your organization, September 2013

WHAT IS THE VALUE OF DISASTER AVERTED?

When everything is working as planned, IT security and business continuity managers are invisible in most organizations. Being invisible should be a sign of success, but it also makes it harder for the C-suite to value what the protective disciplines do.

“It’s normally easier for IT security to present a case to the board,” says Lady. “They can easily quantify how many times the website was attacked or how much spam they captured. It can be more challenging for the business continuity team to keep the discussion alive and relevant because the occurrence of business continuity outages or disasters is much less frequent.” All that changes if the website goes down or an earthquake takes out a crucial part of your supply chain, of course. But how many times does disaster occur?

What is the best way to present the business continuity case? One trusted measure is the return on investment. Identify the risk, estimate the cost of a disruption, and calculate the cost of being prepared versus the cost of an outage. This may work for discreet risks that lend themselves to neat calculations. But it may not always be the best method.

“Measuring ROI for business continuity is not helpful, in my opinion,” says Qatar Air’s Green. “You can’t measure what you have avoided.” He does measure effectiveness of planning, however, and how well continuity plans align with business needs and IT capabilities, “but none of these translate into a ‘dollars-saved’ equation today,” he says. One cost saving that can be measured is a reduced insurance premium. “One of my firms got a premium reduction of \$100,000 because we could demonstrate a risk program that was likely to reduce the chance of events, and the losses resulting from those events,” says Green, who has worked with several global companies in his 20-year career.

But he believes there is a bigger value that needs to be recognized. “We have to accept that these are good things to do for the health of the organization, and then measure how well we do them,” he says. “Much of the output from the program can be used for better business: if I have identified key internal dependencies, can we then streamline those dependencies? If I have identified critical processes and functions, can I then invest in the people skills and technology support to enhance those critical processes further?”

Culturally, there is a pattern of thinking of security and business continuity as an expense, says Poore. “We have to stop thinking about it as a low-level, nuts-and-bolts technical discussion where the debate becomes, ‘Why do we need 10 new servers?’” Moving the conversation to the strategic level can change everything, she says. “You want to move to the cloud? Business continuity is one aspect. Automation is one aspect. We have to raise the consciousness of the organization.”



CONCLUSION

Technology is the way that many clients, suppliers and regulators interact with an organization. Any company that fails to live up to a promise of always-on service puts its reputation at risk.

From underground hacker networks to complex supply chains, the threats to IT security and business continuity are proliferating—and so are the ways to deal with them. The best solutions extend beyond the boundaries of the IT department or business continuity team. A strong program for business resilience and IT security should work beyond traditional silos and extend across every part of an organization.

ACKNOWLEDGMENTS

IBM and Forbes Insights would like to thank the following executives and experts for sharing their time and expertise:

Daniel Diermeier, IBM Professor of Regulation and Competitive Practice at the Department of Managerial Economics and Decision Sciences, Kellogg School of Management

Chris Green, Head of Business Continuity, Qatar Air

Laurence Guihard-Joly, General Manager, Business Continuity & Resiliency Services, IBM Global Technology Services

Frank Lady, Senior Vice President of Business Continuity, Bank of America

Linda Laun, Senior Technical Staff Member, IBM Business Continuity Management

Kris Lovejoy, General Manager, IBM Security Services

Larry Ponemon, Chairman and Founder, Ponemon Institute

Paige Poore, Director, Global Business Continuity Management, IBM

Dr. Paul Robertson, Director, Business Resilience, PricewaterhouseCoopers

Patricia Titus, Chief Information Security Officer, Freddie Mac



ABOUT FORBES INSIGHTS

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, publisher of *Forbes* magazine and Forbes.com, whose combined media properties reach nearly 50 million business decision makers worldwide on a monthly basis. Taking advantage of a proprietary database of senior-level executives in the Forbes community, Forbes Insights conducts research on a host of topics of interest to C-level executives, senior marketing professionals, small business owners and those who aspire to positions of leadership, as well as providing deep insights into issues and trends surrounding wealth creation and wealth management.

Bruce Rogers

CHIEF INSIGHTS OFFICER

Brenna Sniderman

SENIOR DIRECTOR

Kasia Moreno

EDITORIAL DIRECTOR

Brian McLeod

MANAGER, NORTH AMERICA

Matthew Muszala

MANAGER

Lawrence Bowden

MANAGER, EMEA

Deborah Orr

REPORT AUTHOR

Dianne Athey

DESIGNER