September 2, 2010

Business Continuity And Disaster Recovery Are Top IT Priorities For 2010 And 2011

Six Percent Of IT Operating And Capital Budgets Goes To BC/DR

by Stephanie Balaouras
with Chris McClean, Laura Koetzle, and Lindsey Coit

EXECUTIVE SUMMARY

According to Forrester's recent survey of 2,803 IT decision-makers, improving their business continuity and disaster recovery (BC/DR) capabilities is the No. 1 priority for SMBs and the second highest priority for enterprises for the next 12 months. The scope of BC/DR programs is growing also; mature BC/DR programs address all sources of downtime — including mundane power outages and weather-related disruptions, not just rare, catastrophic disasters. Security and risk professionals should take advantage of this increased visibility as the economic recovery slowly thaws IT budgets to improve the BC/DR's organizational and process maturity for the long term.

AWARENESS AND INCREASED REGULATION DRIVE BC/DR PRIORITIZATION

Historically, it has been difficult to build the business case for BC/DR spending because senior executives viewed it as an expensive insurance policy for risks for which no one had determined the probability or accurately assessed the impact. When security and risk professionals tried to highlight certain threats to the business, the common response from senior executives was, "I know there's a risk of XYZ event, but it hasn't happened yet." Thankfully, this misperception of BC/DR spending is finally changing because:

- **We can better identify, measure, and quantify risk.** Security and risk organizations have become much better at using formal methods for identifying risks, measuring their probability, and quantifying their impact. They're also much better at incorporating business leaders into their formal risk measurement processes. A survey of 345 *Disaster Recovery Journal* subscribers found that 65% of business continuity management (BCM) teams work with the business to determine the impact of risks.[1] And the benefit of this approach is clear: It's much more likely that a CIO or other executive will approve budget for a BC/DR upgrade if you can explain that in the next five years there is a 20% probability that a severe winter storm will knock out power to the data center and cost $500,000 in lost revenue and employee productivity.

- **We have a better understanding of the economic impact of disasters and events.** According to the Centre for Research on the Epidemiology of Disasters (CRED), between 2000 and 2008, the average number of disasters per year was 392, and the average annual economic damage was $102.6 billion worldwide. In 2009, there were 335 disasters and economic damages of $41.3 billion. The US suffered the worst economic impact in 2009 ($10.8 billion), followed by China ($5.2 billion) and France ($3.2 billion).[2] The number of disasters doesn't necessarily increase each year (it seems to be holding steady), but the attention that government agencies, nonprofit

organizations, media organizations, and other outlets pay to disasters does. Awful though they are, high-profile catastrophic events can have one positive outcome: They can inspire senior executives to action.

- **We must deal with a bevy of government and industry regulations related to BC/DR.** Post-9/11, there have been at least 22 worldwide government or industry regulations and standards to address BC/DR in some shape or form.[3] On June 15, 2010, the US Department of Homeland Security (DHS) announced the adoption of the final standards for the Voluntary Private Sector Preparedness Accreditation and Certification Program. Title IX of the Implementing Recommendations of the 9/11 Commission Act of 2007 mandated the creation of the program.[4] The final standards are the National Fire Protection Association 1600, British Standard 25999, and ASIS SPC.1-2009.[5] Although the program is voluntary, Forrester believes that with the adoption of these three recognized industry standards, more US private-sector companies are likely to certify when certification becomes available. There are three types of organizations that are more likely to certify: 1) organizations that must prove preparedness to major customers or partners; 2) organizations that must frequently comply with audits of their BC/DR program; and 3) organizations that believe it provides a competitive advantage in the market.[6]

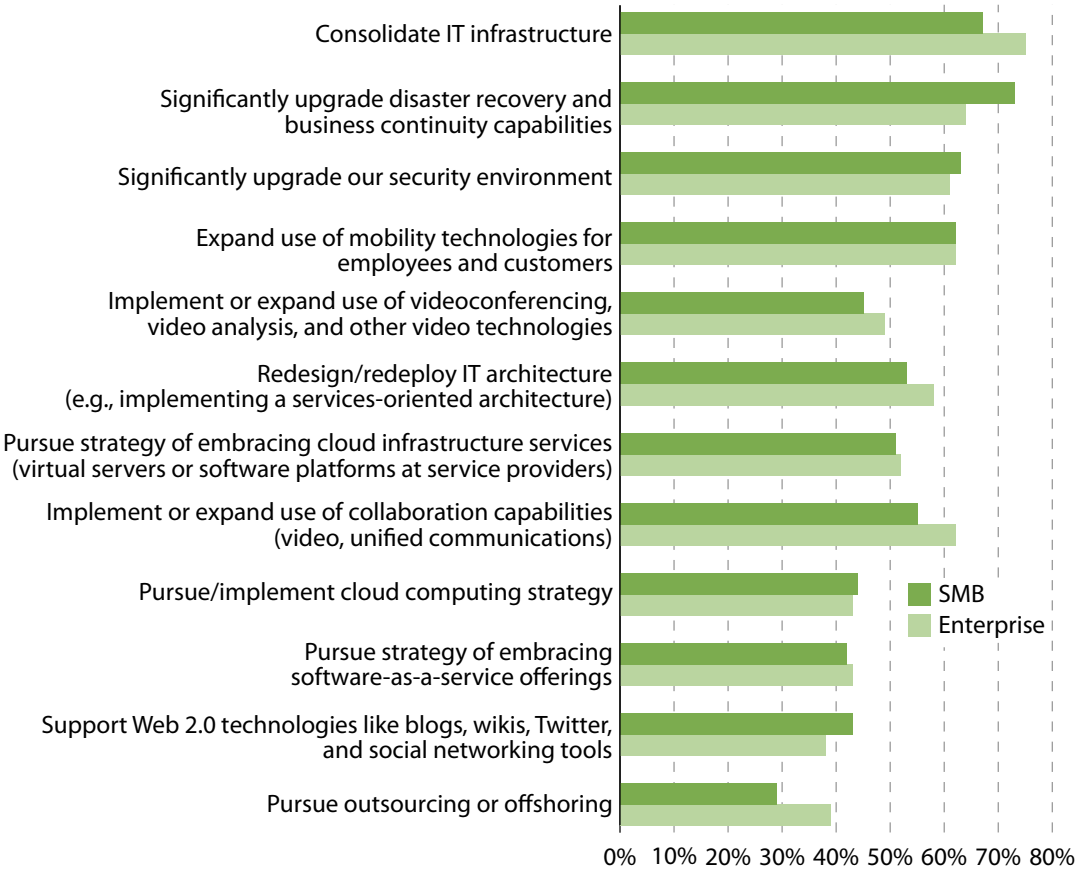
- **We have to answer to our partners and customers about our preparedness.** Since 2008, security and risk organizations have had to respond to an increasing number of BC/DR preparedness audit requests. According to the Forrester/*Disaster Recovery Journal* Crisis, Risk, And Business Continuity Management Survey, Q4 2008, almost 80% of respondents tell us that their firms have had to provide proof of BC readiness to at least one — but sometimes more — external parties in the past 12 months.[7]

- **We have less and less tolerance for downtime and data loss.** Today, business process owners and managers won't accept downtime and data loss that lose revenue, reduce employee productivity, or damage the company's reputation. As a result, BC/DR teams across all industries and company sizes must provide recovery times measured not in hours and days but in minutes and hours. In addition, process owners no longer care about the source of downtime — it doesn't matter if it's a power outage, distributed denial of services (DDoS) attack, disk drive failure, hurricane, or pandemic — they want business processes and the IT systems they rely on up and running at all times.

In response to these drivers, BC/DR is one of the top IT priorities for the next 12 months (see Figure 1).

Figure 1 Top Technology Priorities Over The Next 12 Months

"Which of the following initiatives are likely to be your IT organization's top technology priorities over the next 12 months?"



Base: 1,228 SMB budget decision-makers and 1,575 enterprise budget decision-makers

Source: Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010

57818 Source: Forrester Research, Inc.

IT Plans To Spend At Least 5% More On BC/DR In The Next 12 Months

Not only is BC/DR a top priority but it is also earning a larger share of financial investment in both SMB and enterprise organizations:

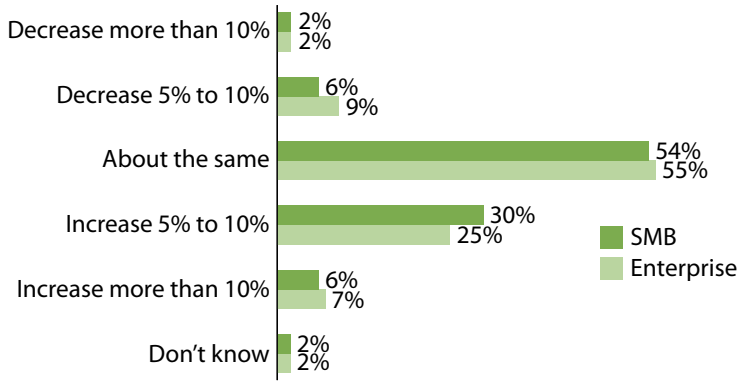
- **Most organizations plan to maintain or increase spending on BC/DR.** According to our survey, 32% of enterprises and 36% of SMBs plan to increase spending on BC/DR by at least 5%. Only 11% of enterprises and 8% of SMBs plan to decrease spending on BC/DR (see Figure 2-1).

- **BC/DR represents between 6% and 7% of the IT budget.** As a percentage of overall operating and capital budgets, BC/DR spending still falls short of other IT functions such as security at an average of 6% among enterprises and 7% for SMBs (see Figure 2-2). However, considering the level of priority and increased investment, BC/DR can confidently consider itself among the critical elements of a comprehensive IT program.

Figure 2 Business Continuity Spending

2-1 Spending increases on business continuity

"How do you expect your spending on business continuity and disaster recovery to change in 2010?"



Base: 1,228 SMB budget decision-makers and 1,575 enterprise budget decision-makers

2-2 IT budget breakdown

"In 2010, how much of your IT operation and capital budget will go to the following IT functional activities?"

	SMB	Enterprise
IT management (CIO or equivalent and direct reports)	9.5%	8.3%
Research and development of emerging technologies	5.3%	4.4%
Business continuity and disaster recovery	7.0%	6.0%
Security	8.2%	7.3%
Application development, customization, and implementation	13.7%	15.0%
Application maintenance	11.8%	13.9%
Information management and storage	10.1%	9.9%
Server and mainframe operations	12.6%	13.1%
Desktop operations	11.0%	11.0%
Network operations	10.9%	11.0%

Base: 1,036 SMB budget decision-makers and 1,183 enterprise budget decision-makers

Source: Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010
Note: Mean numbers provided. Percentages may not add up to 100% due to rounding.

57818 Source: Forrester Research, Inc.

RECOMMENDATIONS

NEVER LET A CRISIS GO TO WASTE

Ideally, we should make investment decisions based on rational, objective risk assessments, but unfortunately, all security and risk pros know that's not always how it works. Headline-grabbing catastrophes, pandemics, and security breaches get the attention of senior executives. Impending regulation or the knowledge that they significantly lag behind their industry peers in spending or best practices also gets their attention. Use industry examples to gauge your BC/DR preparedness level, even running scenarios to see how your organization might have handled similar situations. As you start planning your 2011 budget, you should:

- **Aim for BC/DR to claim between 6% and 7% of your overall IT budget.** Aside from dedicated staff (usually continuity analysts and managers), software (such as BC planning and automated notification software), and any outsourced BC/DR services, it's often very difficult to know exactly how much you spend on BC/DR. You can usually find BC/DR costs built into — and therefore, hidden among — budgets for data center facilities, servers, storage, networking, and telecommunications. You may spend more or less depending on your recovery objectives. For example, if you are in a financial services firm and your executives demand zero downtime and zero data loss, you could spend more. If you are a manufacturing firm and your executives are comfortable with a 48-hour recovery with a few hours of data loss, you could spend a little less.
- **If you are a US organization, select one of the three DHS standards as your BC framework.** Given that the DHS has adopted three standards to support the voluntary certification program, you should select one of these standards as the framework for your own BC management program. While your organization might not have any plans to voluntarily certify today, that could change in the future. In case you do change your mind, it's best to have already adopted one of the three standards. Adoption doesn't mean that you have to go through any certification process. It just means that you use the standard as a model or a framework for your BC management program.

SUPPLEMENTAL MATERIAL

Methodology

Forrester's Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010, was fielded to 2,803 IT executives and technology decision-makers located in Australia/New Zealand, Brazil, Canada, China/Hong Kong, France, Germany, India, Japan, Mexico, Russia, the UK, and the US from SMB and enterprise companies with 100 or more employees. This survey is part of Forrester's suite of Business Data Services studies. Forrester fielded the survey from March 2010 to May 2010. LinkedIn Research Network fielded this survey online on behalf of Forrester. Survey respondent incentives included gift certificates and research summaries. We have provided exact sample sizes in this report on a question-by-question basis.

Forrester's Business Data Services fields eight business-to-business technology studies in 19 countries each calendar year. For quality control, we carefully screen respondents according to job title and function. Business Data Services ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of IT products and services. Additionally, quotas are set for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts.

In addition to sampling error, one should bear in mind that the practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls. Other possible sources of error in polls are probably more serious than theoretical calculations of sampling error. These other potential sources of error include question wording, question ordering, and nonresponse. As with all survey research, it is impossible to quantify the errors that may result from these factors without an experimental control group, so we strongly caution against using the words "margin of error" in reporting any survey data.

These statements conform to the principles of disclosure of the National Council on Public Polls.

We have illustrated only a portion of survey results in this document. For access to the full data results, please contact bds@forrester.com.

ENDNOTES

[1] Business continuity is an essential element of enterprise risk management (ERM), although organizationally, the two disciplines are not often connected directly. In a survey of 345 *Disaster Recovery Journal* subscribers, Forrester found that only 15.5% of business continuity teams reported directly to the risk management function, even though nearly 40% of respondents noted that the two functions work closely together. Upon further analysis, business continuity teams frequently use risk management techniques to prioritize their efforts, and they work closely with the business to understand risk impacts. See the April 30, 2010, "Strengthening The Relationship Between Risk Management And Business Continuity" report.

[2] Source: Femke Vos, Jose Rodriguez, et al., *Annual Disaster Statistical Review 2009*, CRED, 2010 (http://cred.be/sites/default/files/ADSR_2009.pdf).

[3] Some examples include Sarbanes-Oxley Act of 2002, HIPAA Final Security Rule, *FFIEC BCP Handbook*, NASD Rule 3510, NERC Security Guidelines, FERC Security Standards, NAIC Standard on BCP, NIST Contingency Planning Guide, FRB-OCC-SEC Guidelines for Strengthening the Resilience of US Financial System, NYSE Rule 446, *Australia Standards BCM Handbook*, and the UK Civil Contingencies Act.

[4] Source: Federal Emergency Management Agency (FEMA) Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep) Resource Center (http://www.fema.gov/privatesector/preparedness/#1).

[5] National Fire Protection Association (NFPA) publishes NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1600). The British Standards Institution (BSI) publishes BS 25999 Business Continuity (http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999). ASIS International publishes ANSI/ASIS SPC.1-2009 Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use Standard (http://www.asisonline.org/guidelines/or.xml).

[6] Vodafone UK already had a solid approach to business continuity preparedness and ongoing management, but the company wanted to assess itself relative to industry best practices as well as determine a way it could more quickly comply with requests from customers and regulatory authorities for proof of preparedness. Vodafone UK decided to certify to the new British Standards Institution's certification for business continuity management, BS 25999. See the October 8, 2008, "Case Study: Vodafone UK Uses Business Continuity As A Competitive Advantage" report.

[7] In our Forrester/*Disaster Recovery Journal* Crisis, Risk, And Business Continuity Management Survey, Q4 2008, we found that businesses are taking the time to complete each phase and regularly update BIAs, RAs, and plans. This is due in part to the increasing priority that businesses place on BC readiness, but it's also due to the increasing scrutiny businesses are under from both internal auditors and external parties such as regulatory bodies, strategic partners, and even customers. For more information, see the February 26, 2009, "Businesses Take BC Planning More Seriously" report.