February 26, 2009

Businesses Take BC Planning More Seriously

by Stephanie Balaouras
for Security & Risk Professionals

February 26, 2009

Businesses Take BC Planning More Seriously

But Take The BC Readiness Of Strategic Partners For Granted

This is the second document in the "State Of Enterprise Business Continuity" series.

by Stephanie Balaouras
with Simon Yates and Allison Herald

EXECUTIVE SUMMARY

Business continuity (BC) planning consists of three critical phases: business impact analysis (BIA), risk assessment (RA), and plan documentation. In our Forrester/*Disaster Recovery Journal* Business Continuity Preparedness 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. Security and risk management professionals, particularly CISOs and BC directors and managers, must ensure that their own planning efforts are on par with those of their peers and pay close attention to the areas where businesses are struggling: testing more thoroughly and frequently, involving business owners in the process from start to finish, and ensuring the BC readiness of strategic partners.

TABLE OF CONTENTS

NOTES & RESOURCES

This report contains data from an online survey that Forrester Research and the *Disaster Recovery Journal* (DRJ) conducted in October 2008 of 295 business continuity decision-makers and influencers at global businesses.

Related Research Documents

"More Businesses Now Institutionalize Business Continuity Management"
January 13, 2009

"CISOs Must Take The Lead On Business Resiliency"
October 21, 2008

"Case Study: Vodafone UK Uses Business Continuity As A Competitive Advantage"
October 8, 2008

"Inquiry Insights: Business Continuity, Q3 2008"
September 22, 2008

INTERNAL AND EXTERNAL AUDIENCES NOW DEMAND PROOF OF BC READINESS

At one time, you might have been able to pass an internal BC audit with a few hastily prepared plans and supporting documentation. Today, whether you're a private or public entity, BC readiness is no longer just an internal concern. You must provide proof of BC readiness to multiple external parties. According to the Forrester/*Disaster Recovery Journal* Business Continuity Preparedness 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, including (see Figure 1):

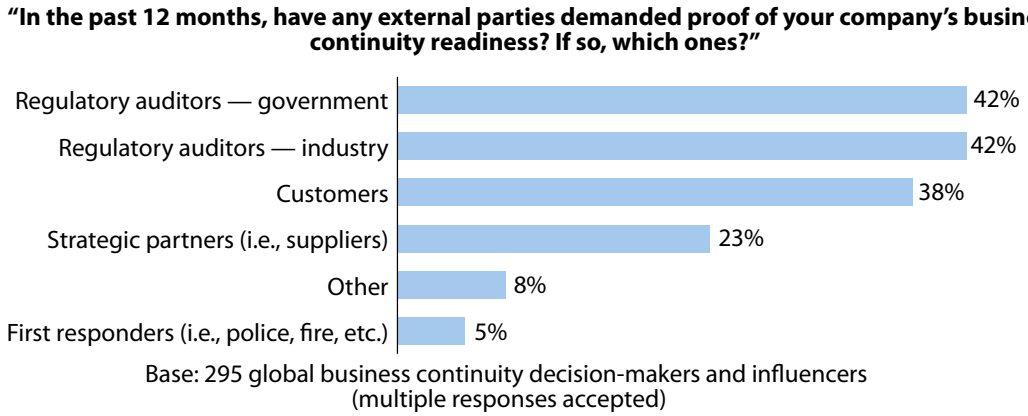
- **Regulatory auditors who enforce readiness mandates.** A number of government regulations expressly mandate BC planning. The Health Information Portability and Accountability Act (HIPAA), for example, mandates BC planning for organizations that either provide healthcare or support other healthcare providers. Financial institutions must comply with guidelines set out in the Federal Financial Institutions Examination Council (FFIEC) Business Continuity Planning Booklet in the US and Basel II in Europe.

- **First responders who want you to participate in coordinated exercises.** In the UK, the transportation and utility companies that the government considers critical to the national infrastructure are subject to the UK Contingencies Act. Category 2 responders must take part in coordinated exercises with Category 1 responders like emergency services and local authorities.[1] Mobile communications provider Vodafone UK is considered a Category 2 responder and is subject to the provisions of the UK Contingencies Act.[2]

- **Strategic partners who won't just take your word for it.** If you're the sole supplier of a particular product or service to a business, expect that business to demand proof of your readiness. Repligen Corporation, a small US-based biotech company, is the sole provider of a protein compound for several large pharmaceutical firms, and not surprisingly, Repligen's BC readiness is a major concern to its partners. To ease these concerns and more readily provide proof of its readiness, Repligen became the first North American company to achieve certification to BS 25999, the British standard for business continuity management.[3]

- **Customers who demand uninterrupted service.** In some industries like online retail and brokerage, service interruption is an excuse to jump to a competitor. In some cases, customers rely on timely delivery of products or uninterrupted service to conduct business. In the case of infrastructure, telecommunication, and IT-related services, customers such as financial institutions will demand to see proof of your BC readiness since the delivery of your services is crucial to their business operations.

Figure 1 Who Wants To Know That You Are Ready?



Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

BEFORE YOU CAN PLAN, YOU NEED TO UNDERSTAND YOUR BUSINESS AND YOUR RISKS

Given the cost and complexity of business continuity and disaster recovery (BC/DR) solutions, you can't take any shortcuts in the planning process. You must commit to completing the critical phases of BIA, RA, strategy development, and plan documentation.

More Businesses Will Conduct A BIA, But Not All Will Refresh It Regularly

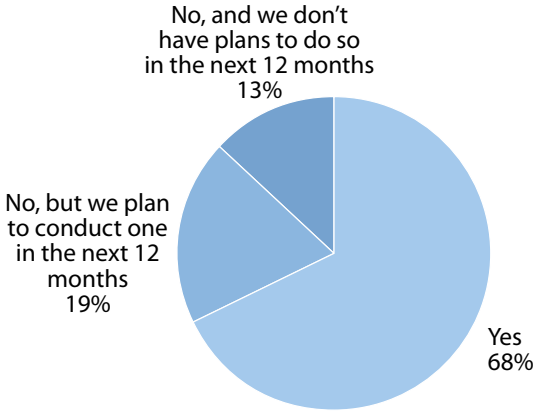
During a BIA, businesses classify their business processes by criticality (i.e., mission-critical, business-critical, business-important), determine the cost of downtime, and map all dependent resources. Resources may include IT assets, non-IT assets (i.e., physical facilities and other physical resources), manual business procedures, paper documents, people, business partners, suppliers, and service providers. In our study we found that:

- **Most businesses will conduct a BIA . . .** Our study found that most businesses do take the time to conduct a BIA before they embark on BC strategy development and plan documentation. Approximately 68% of respondents have conducted a BIA, and 19% plan to do so in the next 12 months (see Figure 2).

- **. . . but not all will take the time to refresh it.** Our survey also uncovered that only 50% of these respondents refresh the BIA annually, while almost 26% refresh it every two years. Businesses need to commit to refreshing the BIAs more regularly. In today's dynamic business environment, businesses routinely merge, acquire other companies, divest parts of the business, launch new products and services while they end-of-life others, and continuously change relationships with partners. An out-of-date BIA means that your BC plans are likely out-of-date as well.

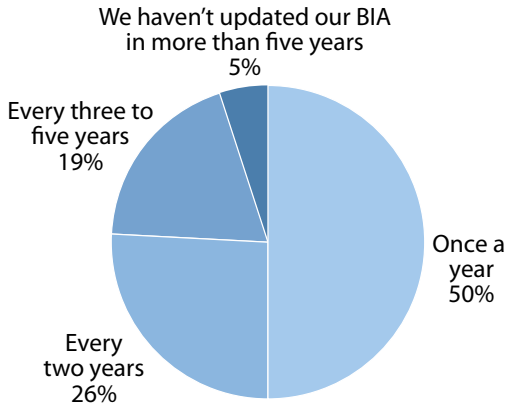
Figure 2 Have You Identified Your Most Critical Business Processes?

2-1 "Have you conducted a formal business impact analysis (BIA) to support business continuity strategy development and planning?"



Base: 295 global business continuity decision-makers and influencers

2-2 "How often do you refresh the business impact analysis?"



Base: 201 global business continuity decision-makers and influencers who have conducted a formal BIA

Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

More Businesses Recognize The Importance Of A Risk Assessment

It's also important that you identify the most probable, high-impact risks, and not spend your time and your money trying to address every possible risk. Some risks might have an enormous impact but are highly improbable, like an accident at a nearby nuclear power plant that has no history of accidents. Other risks have moderate impact but are highly probable and frequent, like severe winter storms in the Northeast US. Forrester's study found that:

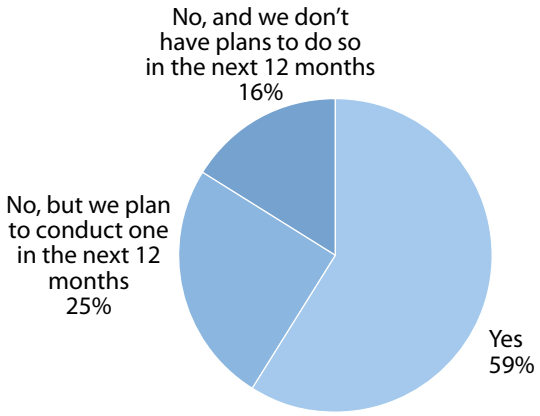
- **Risk assessments have become commonplace . . .** In the past, businesses often focused their BC/DR efforts on natural disasters and overlooked mundane events that actually cause most disruptions, like power outages, IT failures, and human error. But businesses have come to realize that they must take the time to conduct a more comprehensive risk assessment that will identify all probable risks. Approximately 59% of respondents have conducted a risk assessment, and 25% plan to conduct one in the next 12 months (see Figure 3).

- **. . . and will be refreshed every one to two years.** Like the BIA, risks are changing all the time, and businesses of all sizes need to be sure their risk assessments are current. It's not necessary to conduct the risk assessment from scratch each year, but there needs to be a process in place that examines the current assessment to determine if probabilities and frequencies have changed

and whether there are new risks that the business has not considered. Approximately 54% of respondents refresh the risk assessment annually, and 22% refresh it every two years.

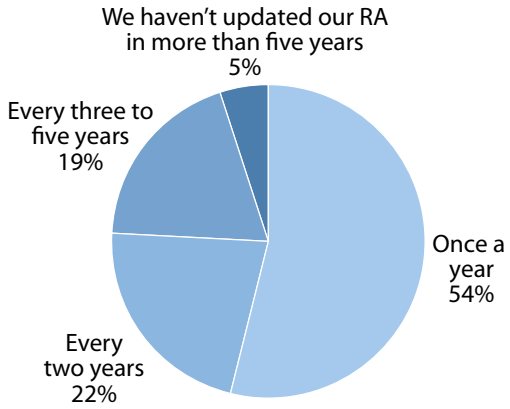
Figure 3 Do You Know What Risks Your Business Will Likely Face?

3-1 "Have you conducted a formal risk assessment (RA) to support business continuity strategy development and planning?"



Base: 295 global business continuity decision-makers and influencers

3-2 "How often do you refresh the risk assessment?"



Base: 175 global business continuity decision-makers and influencers who have conducted a formal RA

Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

YOU MUST DOCUMENT BC STRATEGIES IN PLANS AND KEEP PLANS CURRENT

Once you understand your business processes, dependencies, business resumption requirements, and risks, you can devise specific business continuity strategies that address the threat scenarios identified in the risk assessment. These strategies include components for crisis and emergency communication, workforce continuity, IT, and network continuity. Once strategies are devised they must be implemented as well as documented in actionable plans. These plans must be:

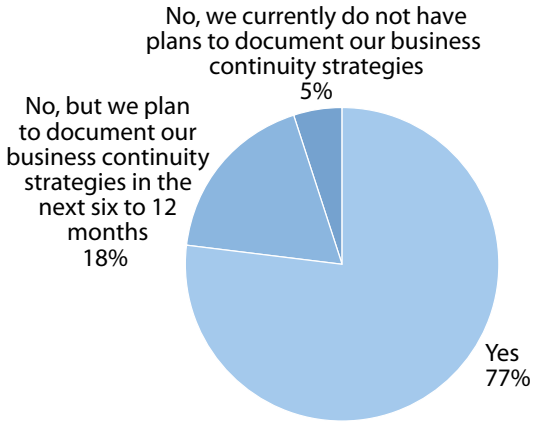
- **Documented.** Seventy-seven percent of both small and medium-size businesses (SMBs) and enterprises in our survey have documented BCPs. Within one year, an additional 16% of SMBs and 19% of enterprises will have documented BCPs (see Figure 4). Having documented BCPs is BC 101: If you don't have them, you don't have anything.

- **Actionable.** Without actionable plans, the most sophisticated and expensive strategies are useless. Plans must list roles, responsibilities, resources, pertinent information (like the emergency number for your disaster recovery service provider), and what specific actions need to be taken and in what sequence to resume or continue business operations.

- **Up-to-date.** Once plans are documented, it's not easy to keep them up-to-date. Plans must be updated whenever there are changes to business or IT operations. Forrester recommends that BCPs be updated continuously, but few businesses reach this goal. According to our survey, only 26% of respondents update BCPs continuously.

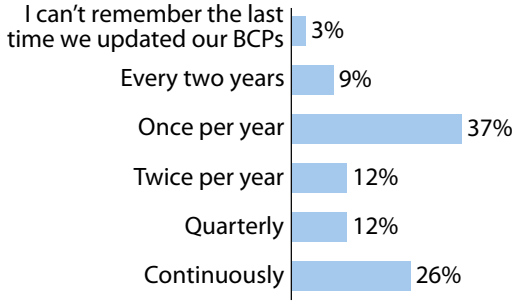
Figure 4 Do You Document Your BC Plans And Keep Them Up-To-Date?

4-1 "Do you have documented business continuity plans (BCPs) in place?"



Base: 295 global business continuity decision-makers and influencers

4-2 "How often are your BCPs updated?"



Base: 227 global business continuity decision-makers and influencers who have documented BCPs in place (percentages do not total 100 due to rounding)

Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

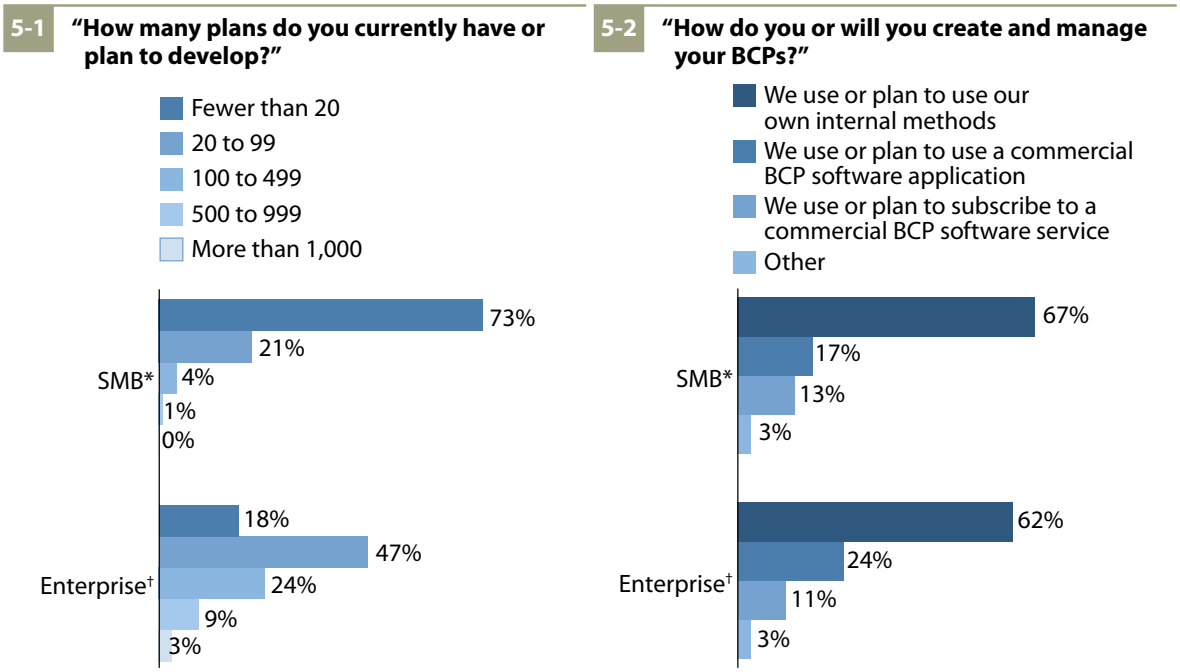
Some Businesses Will Leverage Commercial Software To Manage Plans

Many, if not most, businesses will develop and manage their BCPs using everyday office tools such as Word documents, spreadsheets, network shares, or team portals. This is probably fine if you're a small business with just a handful of plans to manage. It becomes much more difficult when you're an enterprise and you must manage hundreds of plans across different geographies or departments. In this case, it does become worthwhile to consider the use of a commercial software application or service.[4] In our study we found that:

- **Businesses have dozens of BCPs to manage . . .** The larger and more geographically diverse your business, the more BCPs you will have. BCPs must address a specific risk scenario in a local geography. For example, you will have separate plans that address bird flu, terrorist events, and extreme weather. According to our survey, 73% of SMBs have fewer than 20 BCPs, while 47% of enterprises manage between 20 and 99 BCPs and 36% manage 100 or more (see Figure 5-1).

- **. . . but most still manage BCPs manually.** Only 35% of enterprises and 30% of SMBs use either a commercial software application or service to manage BCPs (see Figure 5-2). Adoption is very low, considering the benefits of BCP software. The software provides businesses with a centralized repository for all their BCPs as well as a library of BCP templates for various risk scenarios that can give them a jumpstart on their planning and also ensure that the plans are complete.

Figure 5 How Do You Manage Your BC Plans?



*Base: 94 SMB BC decision-makers and influencers who have or will have documented BCPs
†Base: 186 enterprise BC decision-makers and influencers who have or will have documented BCPs

Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

Businesses Now Include Partners In Their BC Tests

One area that businesses of all sizes struggle with is testing BCPs. Testing is critical because it ensures that everyone is comfortable with their roles and responsibilities, that nothing has been overlooked, and that strategies and technology actually work. In this survey, Forrester found that businesses are testing, albeit not as frequently as recommended, and they are including partners in at least one test annually. However, Forrester also found that few businesses demand proof of BC readiness from their partners. More specifically, Forrester found that:

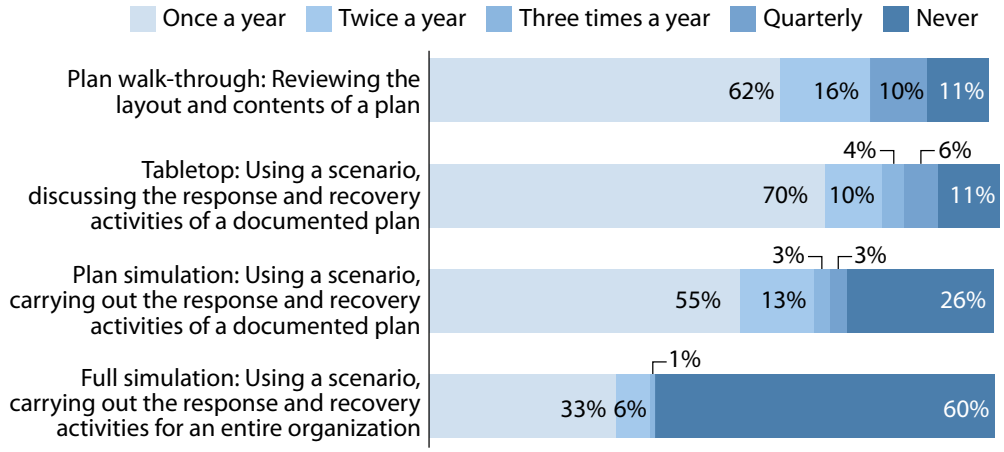
- **Scheduling and complexity affect the frequency of certain tests.** Based on Forrester client inquiries and consulting engagements, BC directors find it very difficult to schedule tests and secure enough participation from key team members in business, IT, facilities, etc. Depending on the nature of the test, it can disrupt business or IT operations. As a result, BC directors will develop a test strategy that includes different types of tests, from simple plan walk-throughs to full simulations. Survey data indicates that the more complex the test, such as a plan simulation or a full simulation, the less frequently it's conducted, and in some cases it's never conducted at all (see Figure 6-1). Forrester recommends that businesses make every effort to run these more complex tests annually. While they may be complex, they're the best way to validate capabilities.

- **Partners will participate in at least one test per year.** In addition to the frequency and thoroughness of tests, CISOs and BC directors should include strategic partners in tests. In this study, almost 47% of respondents include their business partners in at least one BC test annually (see Figure 6-2). If you fall into the 41% of respondents who don't include partners, you must be sure that your business operations are truly independent of your partners' people, processes, and technology, or you need to think about including them in at least one test.

- **Too many businesses don't bother to validate partner readiness.** Given that you're making the effort to conduct each phase of the BC planning life cycle, keep your plans up-to-date, and test them on a regular basis, shouldn't you make sure that the partners you rely on are just as ready as you are? What if they're not? According to our survey, 46% of respondents have never bothered to validate the readiness of strategic partners (see Figure 6-3). Far too many businesses are taking the readiness of their partners, suppliers, and service providers for granted. This is a major risk exposure, particularly if you have sole suppliers for some of your inventory or services.

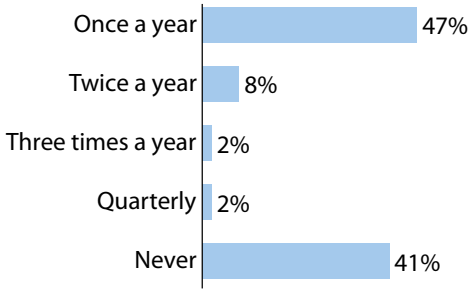
Figure 6 BC Testing

6-1 "How many times per year do you conduct the following types of tests on your BCPs?"



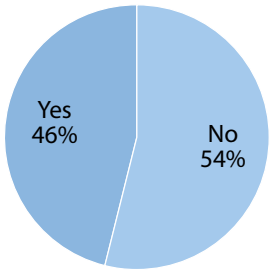
Base: 227 global business continuity decision-makers and influencers who have documented BCPs in place (percentages may not total 100 due to rounding)

6-2 "How often do your business partners participate in your tests?"



Base: 227 global business continuity decision-makers and influencers who have documented BCPs in place (percentages may not total 100 due to rounding)

6-3 "Have you investigated/validated the business continuity readiness of your strategic partners?"



Base: 295 global business continuity decision-makers and influencers

Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

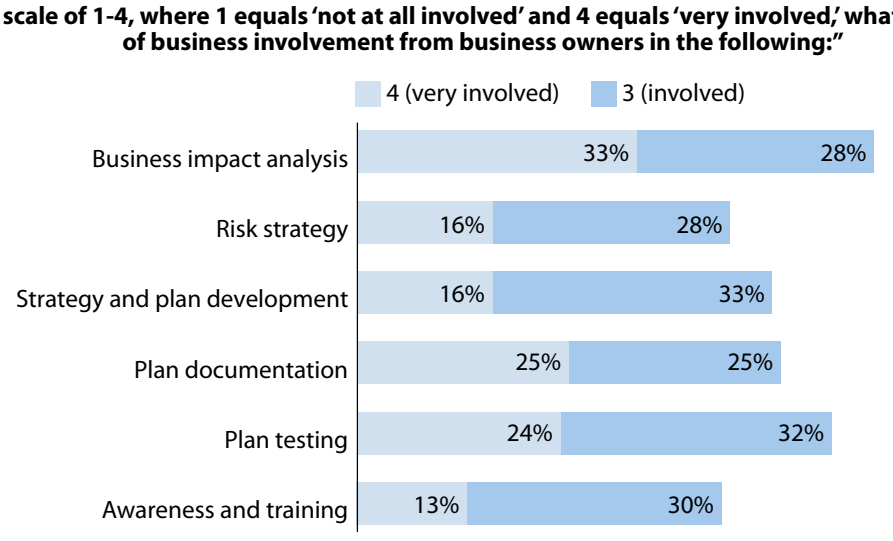
YOU MUST INCLUDE BUSINESS OWNERS FROM START TO FINISH

If your business is serious about BC preparedness, there must be executive-level sponsorship of BC as well as support and participation from senior managers, midlevel managers, and individual contributors. Executives, managers, and individuals must participate in every phase of BC planning so that strategies and documented plans reflect business requirements and deliver business results.[5] Forrester found that:

- **Business owners are most heavily involved in the BIA . . .** Almost 62% of respondents report that their business owners are involved or very involved in the BIA (see Figure 7). This is not surprising; it would be impossible for a BC planner to document business process and dependent resources without working closely with business owners to understand how business is done. Our study also showed that business owners had solid involvement in plan testing. Approximately 55% of respondents reported that business owners were involved or very involved in plan testing.

- **. . . and the least involved in training and awareness.** Only 43% of respondents reported that business owners were involved or very involved in training and awareness. While training can be addressed through frequent testing, not everyone in the business can participate in BC tests; there must be awareness initiatives so that all employees have a basic understanding of what to do or what to expect during a major business disruption, particularly if BC plans require employees to work from or report to an alternate site.

Figure 7 How Involved Are Business Owners In The BC Planning Life Cycle?



Base: 295 global business continuity decision-makers and influencers
(percentages may not total 100 due to rounding)

Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

Businesses Don't Report Readiness Efforts To Executives

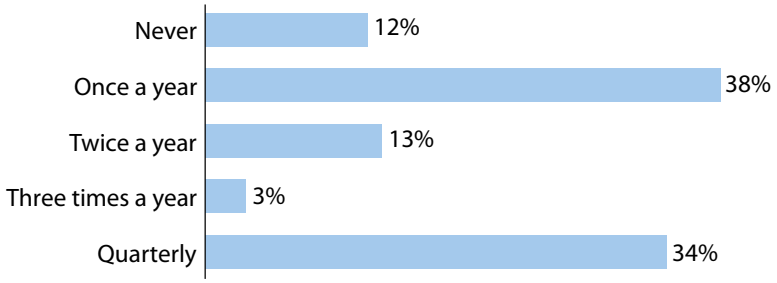
To keep executives informed as well as demonstrate value to maintain or secure additional funding, BC managers must regularly report on BC readiness efforts. According to our survey, however, only 33% of respondents report on readiness to executives on a quarterly basis (see Figure 8). If you only report on readiness once or twice a year, it's not likely that senior executives have an accurate picture of the business' readiness. To increase executive awareness and raise the profile and importance of BC management, Forrester recommends that businesses:

- **Develop a BC readiness "dashboard."** It should report by entity (i.e., subsidiary, business unit, region, department), critical business operations covered by plans, plan maintenance, test frequency, test results, training initiatives, and any actual invocations. This way, the business can quickly see if there are any regions that are vulnerable and out of compliance with corporate mandates for preparedness.

- **Schedule frequent status check-ins with BC managers across the company.** At many of the large companies that Forrester has worked with, the BC director or senior executive responsible for BCM will host monthly calls with BC managers across the business to update readiness status, share best practices, and discuss local challenges. In addition, he or she meets with either a C-level executive or the board of directors quarterly to report on efforts.

Figure 8 Do You Report BC Preparedness Efforts To Executives?

"How many times per year do you report the status of business continuity readiness to executives?"



Base: 295 global business continuity decision-makers and influencers
Source: Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008

47924 Source: Forrester Research, Inc.

RECOMMENDATIONS

FOCUS ON INCREMENTAL IMPROVEMENTS

Maybe you're the business that hasn't updated its BIA in five years or still doesn't have documented BCPs, but most businesses have taken at least the basic steps to devise, implement, and document good BC strategies. Most businesses don't have big gaping holes in their strategies. Instead, where they struggle is in keeping plans up-to-date with business changes and risks, testing plans thoroughly, and including business and partners in the complete BCM life cycle. In the tough economic climate of 2009, CISOs and BC directors should focus on a few incremental improvements that will increase confidence in the ability to successfully invoke plans and highlight areas for improvement:

- **Consider a lower cost commercial software application or service for BCP management.** There are offerings in the marketplace that won't break the bank, especially if you're only interested in the core planning module. If you still manage hundreds of BCPs in Word documents and Excel spreadsheets, it's time to upgrade. Standardizing BCP elements and storing them in a central repository will help you keep them up-to-date, increase collaboration, and improve reporting.
- **Add more plan walk-throughs and tabletop exercises to your test strategy.** One way to identify deficiencies in plans is to identify plans that are out-of-date and increase training and awareness by conducting more walk-throughs and tabletop exercises. Several Forrester clients conduct these exercises on a quarterly basis. Walk-throughs and tabletop exercises won't replace running a plan simulation or a full simulation annually, but because they're less complex, you can schedule them more frequently.
- **Don't take partner readiness for granted.** If you haven't already done so, you must immediately ask for proof of BC readiness from any strategic partner that would materially impact your business or IT operations if their business was down. Don't be satisfied with simple plan documentation; ask for a report on test frequency, test results, and the results of any actual invocations. Also ask to either observe or participate in tests where appropriate.
- **Audit and report on BC readiness efforts corporatewide.** For enterprises with multiple geographic locations or entities, local BC managers must carry out their own planning efforts. However, the CISO and corporate BC director can set some standards. They can mandate the use of a common BCP template, mandate minimum plan components, mandate minimum number of tests, participate in test debriefs, and require reporting of actual invocations. To ensure adherence to corporate policy, corporate BC managers will need to periodically (annually in most cases) audit local efforts and local plans and provide guidance for improvement. If your business has no central dashboard, then this is one area of focus, because without it you won't have an accurate picture of the business' resiliency.

SUPPLEMENTAL MATERIAL

Methodology

In October 2008, Forrester Research and the *Disaster Recovery Journal* (DRJ) conducted an online survey of 295 DRJ members. In this survey:

- All respondents indicated that they were decision-makers or influencers in regard to planning and purchasing technology and services related to business continuity.
- Respondents were from a range of company sizes: 33% had one to 999 employees; 27% had 1,000 to 4,999 employees; 17% had 5,000 to 19,999 employees; and 21% had 20,000 or more employees.
- Respondents were from companies with a range of revenues: 44% of respondents were from companies with revenues of less than $500 million; 9% were from companies with revenues of $500 million to $999 million; 22% were from companies with revenues of $1 billion to $4.99 billion; 8% were from companies with revenues of $5 billion to $10 billion; and 17% were from companies with revenues of more than $10 billion.
- Respondents were from a variety of industries.
- Respondents were primarily from North America: 92% of respondents were from North America; 5% were from Europe, Middle East, or Africa; 2% were from Asia; and 1% were from South America.

This survey used a self-selected group of respondents (DRJ members) and is therefore not random. These respondents are more sophisticated than the average. They read and participate in business continuity (BC) and disaster recovery (DR) publications, online discussions, etc. They have above-average knowledge of best practices and technology in BC/DR. While nonrandom, the survey is still a valuable tool in understanding where advanced users are today and where the industry is headed.

ENDNOTES

[1] Part 1 of the UK Civil Contingencies Act establishes a clear set of roles and responsibilities for those involved in emergency preparation and response at the local level. The Act divides local responders into two categories. Category 1 organizations (e.g., emergency services, local authorities, National Health Service bodies) are at the core of the response to most emergencies. Category 2 organizations (e.g., the Health and Safety Executive, transport and utility companies) are less likely to be involved in the heart of planning work but will be heavily involved in incidents that affect their sector. Source: UK Resilience (http://www.ukresilience.gov.uk/preparedness/ccact.aspx).

[2] 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. See the October 8, 2008, "Case Study: Vodafone UK Uses Business Continuity As A Competitive Advantage" report.

[3] Source: "Presentation of North America's First Certificate for BS 25999, the New Standard for Business Continuity," Reuters press release, July 8, 2008 (http://www.reuters.com/article/pressRelease/idUS160957+08-Jul-2008+PRN20080708).

[4] Firms typically do not have a centralized BC program office that enforces standards, consistency, and quality across a distributed organization or across hundreds of localized BC plans, and these plans are rarely, if ever, tested. To address these challenges, more firms are turning to Web-based software to transform their static BC plans from Word documents and Excel spreadsheets into a more mature BC program. See the May 30, 2007, "Market Overview: Business Continuity Planning Software" report.

[5] In our Forrester/*Disaster Recovery Journal* Business Continuity Preparedness Survey, Q4 2008, 89% of the business continuity (BC) decision-makers and influencers we surveyed said that BC had executive-level support. In addition, about two-thirds of respondents said that BC was a priority or critical priority for senior executives. See the January 13, 2009, "More Businesses Now Institutionalize Business Continuity Management" report.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia
Brazil
Canada
Denmark
France
Germany
Hong Kong
India
Israel
Japan
Korea
The Netherlands
Switzerland
United Kingdom
United States

For a complete list of worldwide locations, visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more than 25 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®