

Insights on IT risk

Business briefing

August 2011

Business continuity management

Current trends





Introduction

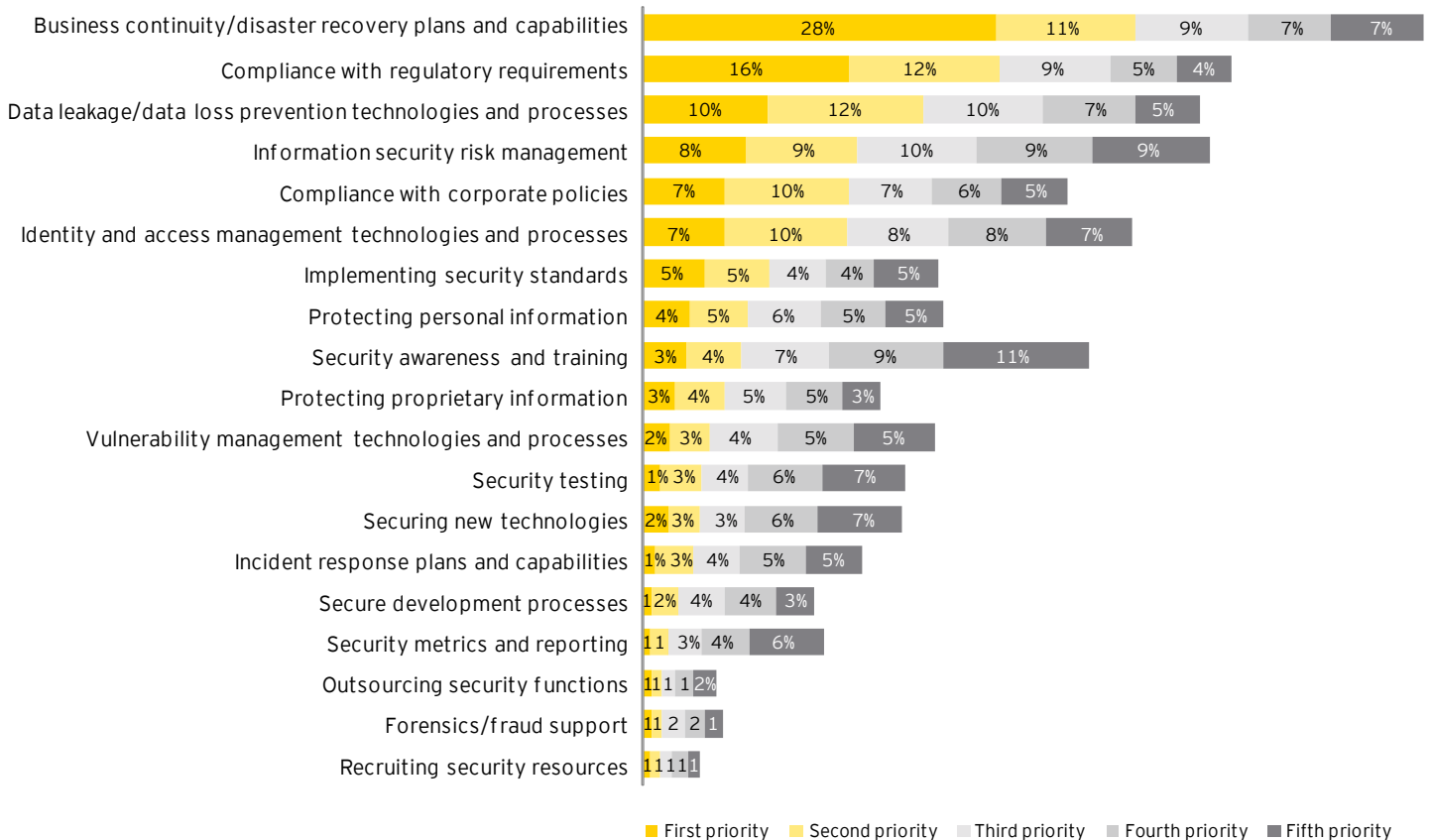
Floods, fires, hurricanes, explosions, earthquakes, pandemics, cyber attacks and even terrorist attacks can cause data to be lost, websites to go down, servers to fail and employees to lose communication with one another. Not being able to give or get necessary resources – data, raw materials, personnel, finished products, and so much more – for any length of time can be devastating. Such inactivity and non-availability can handicap a company for months, reducing income and affecting precious market share. Margins for error in the current economic environment have narrowed, leaving little or no room for mistakes.

As organizations grow in size and complexity within the world of the “extended enterprise,” the impact of non-availability of any resources has magnified. High-profile events caused by natural disasters and technology infrastructure failures have increased awareness of the need to develop, maintain and sustain business continuity programs. Although these large-scale events – such as the Japanese earthquake and tsunami – dramatically challenge the existence of some companies, there are smaller, less impactful but more frequent disruptions that cause many executives to question their organization’s ability to react and recover. These big disasters, as well as the smaller disruptions, have prompted leading executives to hope for the best but prepare for the worst by investing in effective business continuity management (BCM).

Recognizing the importance of BCM

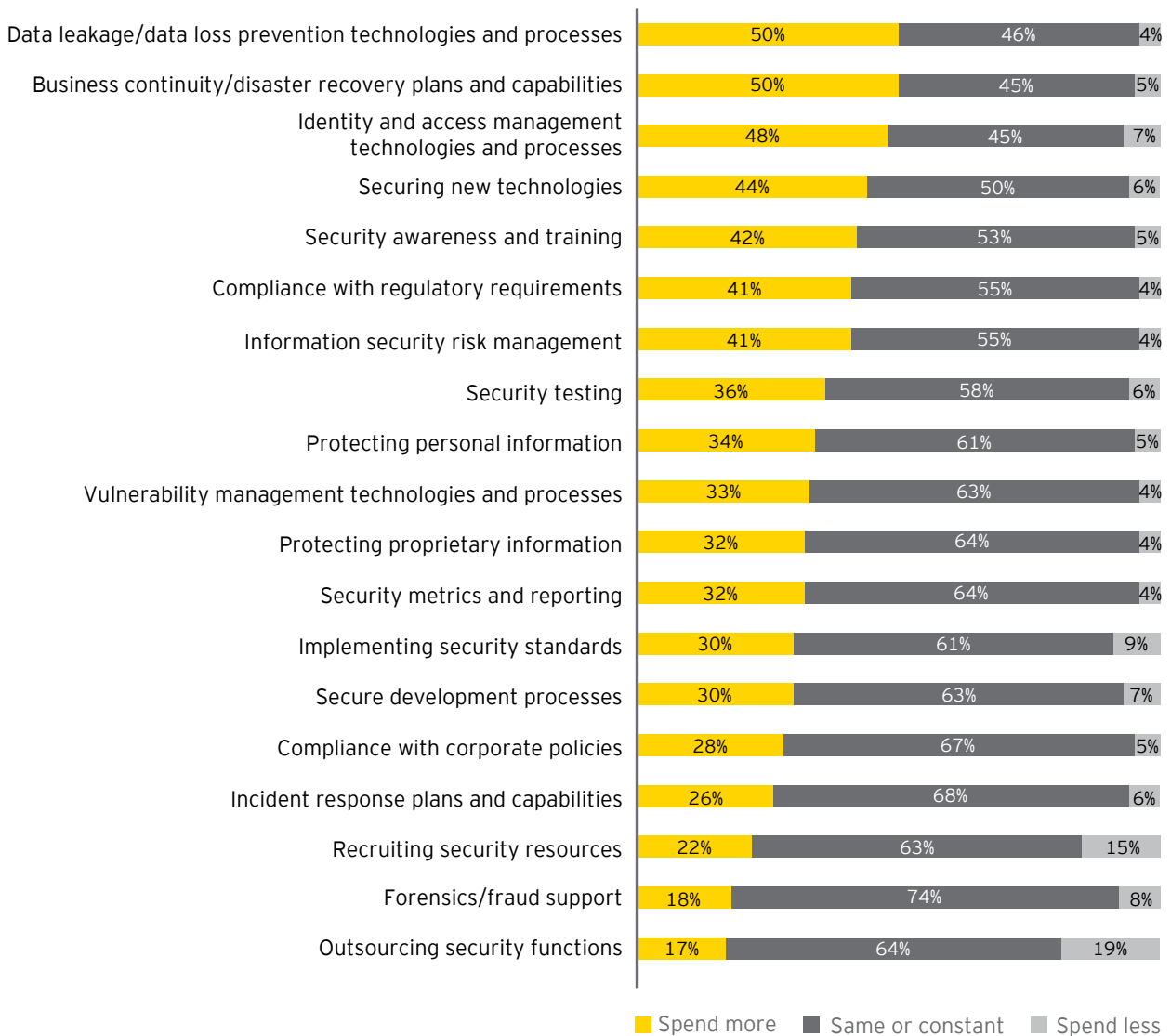
Effective BCM is rising in importance on the corporate agenda. Volatile global economies have shrunk margins for error. Companies that previously would have survived a significant disaster or disruption may now find the same event pushing their corporate existence to the brink. Executives are realizing that effective BCM may be the only buffer between a small disruption and bankruptcy.

Ernst & Young's 2010 Global Information Security Survey affirmed that BCM is viewed as the "most" important security risk, according to 1,598 survey respondents.



Additionally, half of the respondents indicated that they were intending to increase their spending on business continuity. This is a further indication that most organizations are not as advanced as they would like to be in this arena.

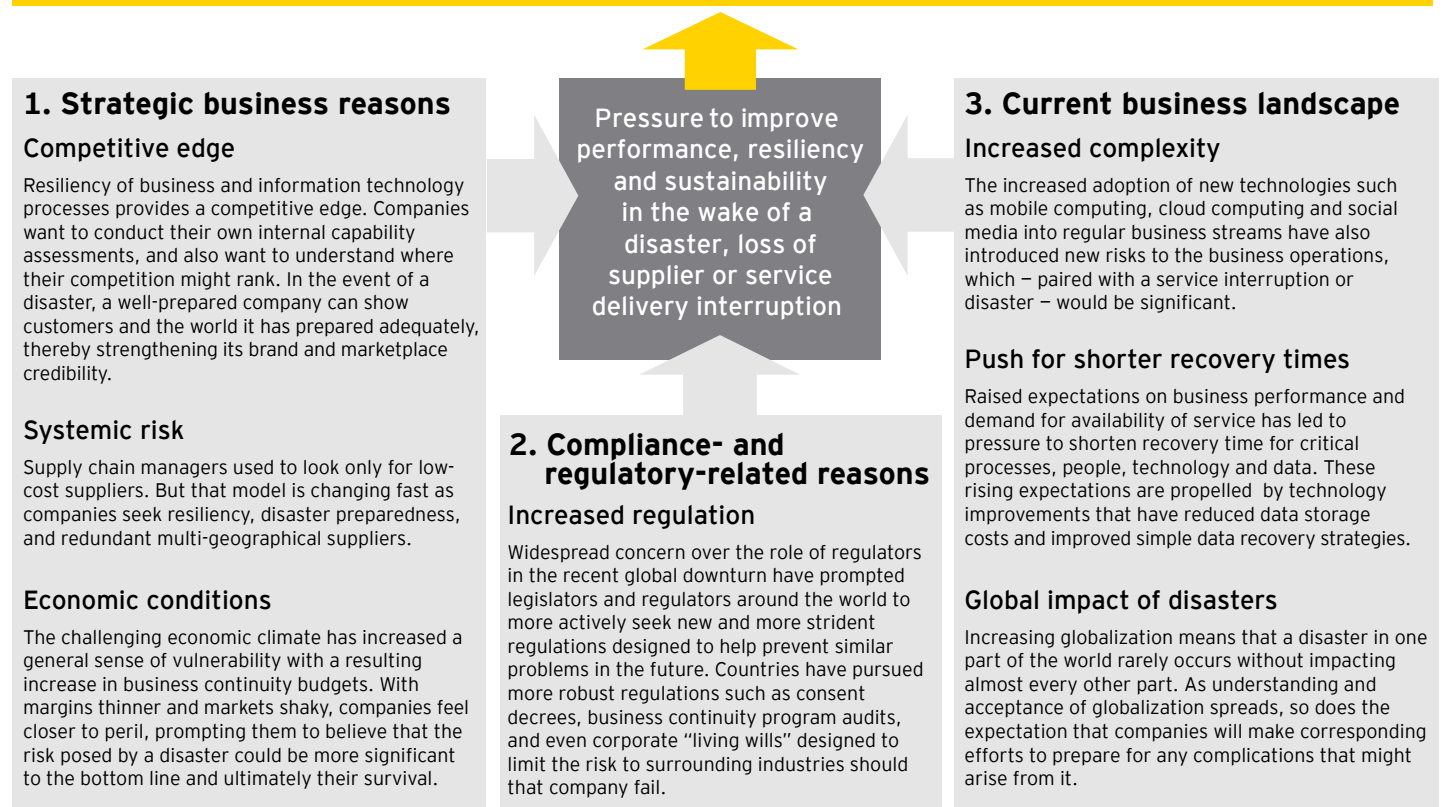
A 2011 Forrester survey, "Global IT Budgets, Priorities, And Emerging Technology Tracking," indicated that for 1,000 respondents, the average IT investment in business continuity and disaster recovery was 6% of the annual budget. While this percentage was considerably lower than within other categories of IT spend, it nonetheless demonstrates that BCM is a significant element of an IT program.



Business continuity: pressure to improve resilience

The increased focus on BCM is being driven by three main factors:

Business continuity management continues to rise up the corporate agenda



These factors create pressure to improve performance, resiliency and sustainability after a disaster or service delivery interruption.

Japan and beyond: local disaster, global impact

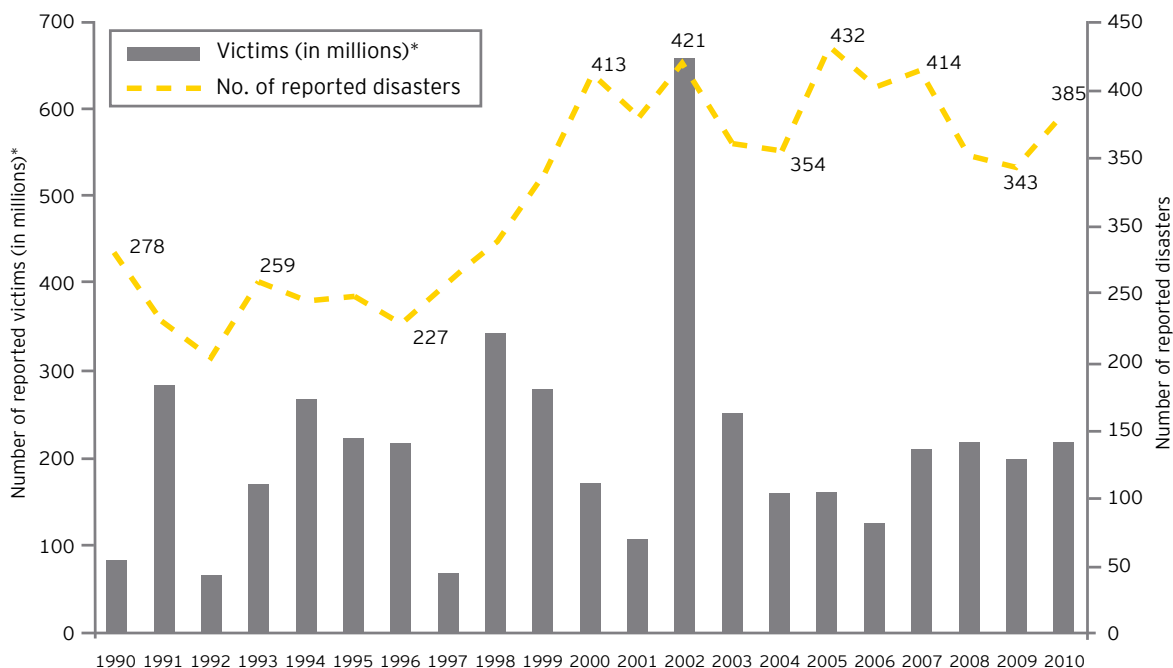
A total of 385 disasters killed more than 297,000 people worldwide in 2010, affected more than 217 million others and caused US\$123.9 billion in direct economic damage, according to the Centre of Research on the Epidemiology of Disasters. These damage estimates do not include secondary damages or impacts caused by loss of revenue through lack of supplies or suppliers. So, while many disasters are local in nature, the operational impacts can be felt worldwide.

For example, an analysis by Dun & Bradstreet showed that the catastrophic Japanese earthquake and tsunami has the potential to impact 86,418 businesses, 311,934 employees and \$209 billion in sales volume. Based on the Japanese suppliers that the business and credit information firm monitors for its US customers, the top 10 Japanese supplier industry categories that can potentially be impacted include manufacturing durable, services, computer services, wholesale durable and manufacturing non-durable. The industries most likely to be impacted include electronics (Japan produces 40% of the global electronic component supply), automotive and certain textiles.

As a result, thousands of businesses and industries – many of which are located around the world and were not directly impacted by the catastrophe but rely on suppliers and buyers that were – will be severely affected. Many of them were left desperately scrambling to find new suppliers, ensure IT system integrity and get data back up and online.

Several automakers and their suppliers impacted by the earthquake and tsunami suffered lower earnings as a result of the catastrophe.

A high cost: disasters in 2010



* Victims: sum of killed and total affected

Source: Centre of Research on the Epidemiology of Disasters

Leading trends: making good from bad

Disasters do not have to be large in scale to capture world attention or cause severe business damage. A flood at a key overseas distribution center may hardly make headlines back home, but it might cripple critical supply chains if no quick alternative exists. A now-common denial-of-service attack can bring down a popular, high-volume website, frustrating consumers, potentially jeopardizing data security and quickly eroding an otherwise strong brand. The collapse of a regional stock exchange can panic investors, shrink capital availability for months and put construction and expansion plans on hold for years.

In today's environment, companies want to secure a level of confidence such that they can effectively manage an emergency situation to both protect life and prevent an escalation of the situation. Management seeks confirmation that it has the ability to detect and swiftly address issues as an effort to change the course of a crisis, or at least minimize its overall impact.

Leading companies want to invest in BCM programs by moving their approach from reactive and tactical to proactive and strategic. They want the ability to prepare for events before adverse effects occur. Many of these leading companies have deployed leading practices to maximize the chances of success in the wake of a disaster or disruption including:

1. Implement a BCM governance model and an enterprise BCM framework

BCM programs should be based upon a clearly defined governance model, supported by a single, common framework that defines a methodology, a set of policies and roles. The overall BCM governance focuses on: how the BCM program should be operationalized within the business and IT by setting well-defined policies and principles; who makes what decisions by defining roles and responsibilities for clear accountability; and what mechanisms are in place to ensure that decisions are made, acted upon and complied with in relation to the company's overall direction. The BCM governance should steer and respond to decision requests that emerge from the business continuity assessment process whereby senior management can make informed decisions in order to reduce enterprise risk.

Background

In recent years, both the enterprise risk environment and enterprise BCM measures have evolved considerably. As all risks are converging, enterprise risk management (ERM) consolidates previously siloed risk management efforts within a single, centralized governance structure. BCM, which has evolved from backup and disaster recovery efforts, now incorporates a wide variety of risk areas within the business and IT. Bringing BCM under ERM is becoming increasingly important as the business and regulatory compliance environment forces the development of a consolidated view of risk. The emerging trends suggest that the global BCM executive leader should report to ERM under the chief risk officer (CRO).

Companies lacking centralized direction often develop BCM processes, protocols and plans that are fragmented in nature, do not synchronize with each other, and do not share a common taxonomy or event classification. This type of fragmentation is very disruptive in a global disaster, and divisions that developed their processes in a silo may have difficulties getting what they need from corporate in a disaster. A consistent framework spanning different geographical BCPs allows them to be better synchronized with each other if there is an actual event that forces them to be activated.

2. Integrate business impact analysis (BIA) and risk assessment

BIAs and risk assessments are two long-standing components of any business continuity standard and methodology. They remain two of the most critical inputs toward any BCM program, as major strategy and funding decisions will be made based on their results and how critical they are to the enterprise.

Background

More than just an understanding of threats and risks, a risk assessment also includes determining whether mitigation measures can cost-effectively be implemented to lower the probability of the risk's occurrence or lessen its impact. By looking at the BIA results and risk assessment results in a single view, management can gain a firmer understanding of where the most critical business functions reside and can apply a comparative risk rating to a particular site. By integrating the BIA and risk assessment results in this way, management will be able to make more informed business decisions on how to better allocate funds to reduce risks and determine which risks it is willing to assume.

3. Leverage emerging technologies such as cloud computing and virtualization

Disaster recovery as a service (DRaaS) provides several levels of protection to help companies recover from downtime in a potentially more cost-effective and timely manner. Workload can be replicated from virtual or physical environments to high-availability cloud infrastructure and then hosted in standby mode. Also, the cloud approach can provide companies the ability to replicate across multiple storage platforms to a cloud infrastructure or elsewhere. Systems (e.g., VMware) can be registered on the cloud in standby mode – ready to activate and keep the business up and running should the need arise.

Background

Although disaster recovery outsourcing and managed services are to some extent mature, the cloud adoption trends are clearly amplified by the recent financial crisis, relying upon key elements such as elastic and scalable capabilities, self-service and ease of provisioning; consumption-based pricing; shared and optimized infrastructure; and the ability to be virtualized and dynamic. Many of our global clients are monitoring the cloud market and approaching cloud services with caution while adopting a mix of in-house and managed disaster recovery services with some well-proven DRaaS based on the application's criticality, recovery objectives, suitability and cost of service. This trend is known as a hybrid disaster recovery sourcing approach.

4. Build for a resilient environment vs. a reactive recovery

Most companies are looking to enhance their ability to rapidly adapt and respond to business disruptions and to maintain continuous business operations, be a more trusted partner and enable growth. However, many companies have delayed investing in or updating their disaster recovery infrastructure and plans due to the lack of funding for disaster recovery over the past five years. Companies should focus 70% to 80% of their disaster recovery spending on supporting the realization of the recovery time objective (RTO) and recovery point objective (RPO) targets for the top 20% to 30% mission-critical applications.

Background

For these companies, infrastructure diversification is one key to enhance their business resiliency without the cost and complexity associated with traditional high-availability clusters and fault-tolerant systems. This approach is achievable by creating an operational infrastructure beyond active/standby that is physically

distributed (geographical or regional-based), but capable of being managed as if it were a single consolidated entity. In this case, service resiliency must become a key component of system design (applications and infrastructure) to support disaster recovery based on geographical intelligence and automatic distribution.

5. Understand the true application dependency for recovery assurance

It is essential to completely understand cross-application, data and underlying infrastructure dependency relationships for both disaster recovery planning and as a quality assurance validation that dependent parts have been identified for recovery. This becomes especially critical if an operation is planning to implement (or has already implemented) one or more application services based on service-oriented architecture (SOA), or whose application services are multisourced.

Background

There is a perception that a few selective applications in recovery and testing are needed to ensure that the right applications are recovered at the right time and in the right order. Many enterprises and service provider operations have found this simplistic view to be inadequate. Many applications and services have complex, meshed relationships and dependencies on other applications, infrastructure services (e.g., network, active directory) and data, some of which may be currently defined as being part of a lower recovery tier or assumed to be highly available and recoverable (e.g., network).

6. Increase the complexity of testing

Leading practice organizations are including more complex integrated exercises in their annual test plan. While most do not advocate a "pull the plug" scenario yet, integrated testing between business units and IT is the right way to truly develop confidence in an organization's capability to recover. In these scenarios, the business units may actually deploy to their alternate site and use their IT workaround procedures during the period that the IT systems are being recovered. This type of testing will prove the viability of the alternate site, the viability of the workaround procedures and that the IT systems that the business unit needs can be recovered within its stated RTO. All of these measures will start to establish a validated recovery time capability (RTC) for an organization, while the best tabletop testing can only provide a recovery time estimate (RTE).

Background

Recent Gartner studies from the past three years indicate that increasingly fewer live tests involve testing all production applications and data. Instead, these tests are specific to an individual recovery tier (typically Recovery Tier 1 and/or Recovery Tier 2), or they include a "blend" of a subset of production applications that have related software and data dependencies. Most companies that have developed business continuity programs do perform testing of their business continuity plans. The majority of these types of tests are simple tabletop exercises as it is often deemed unrealistic to do functional testing for all the applications and data from a time and resource perspective. While tabletop exercises are an excellent method to evaluate the completeness of a newly developed business continuity plan, they generally do not provide a high level of confidence that an organization could actually recover from a real disaster. No actual capability is demonstrated through tabletop exercises.

7. Adapt crisis management and communications strategies

The premise regarding communication during a crisis is still the same: it is important for companies to be proactive and transparent with their communications. And likewise, customers' and stakeholders' expectations remain the same: they want to know that the companies are taking ownership and accountability and that there is a resolution plan to get the services stabilized and restored. What has changed is the approach to disseminating this information, which can reduce the negative impacts to brand image and customer satisfaction during a disaster. As companies begin to understand the evolution of mass communication, they adapt their crisis communication strategies to leverage the various media outlets to their advantage. This way, they are able to manage their messaging in a timely manner and prevent incorrect information from spreading.

Background

The media landscape is evolving. With a growing internet user base combined with advances in connected devices, compounded by the viral nature of social media, information is more easily accessible to broader audiences now than ever before. From a crisis management perspective, these technological advances present new and complex challenges for managing the flow of information during a crisis. Corporate public relations strategies once considered "rule of thumb" for responding to crises may now potentially do more harm than good.

8. Exercise an integrated ERM program

Leading companies have implemented integrated ERM programs that bring all types of organizational risk under a single "risk universe," regardless of whether a particular risk is classified as a security risk, a health and safety risk, an insurance risk, an environmental management risk or a business continuity risk.

Background:

ERM programs have brought key risk issues to the forefront of executive awareness. Executive risk committees come together to review and make business decisions on all kinds of organizational risk, allowing risks to be better prioritized from an enterprise perspective and managed according to their level of impact. In most cases, business continuity is always a top-10 risk within those companies that have implemented such programs and has attained better visibility in the organization.

9. Solicit support from the Board of Directors and the Audit Committee

It is much more common for companies to develop and implement company-wide business continuity management programs when there is pressure from the Board or Audit Committee.

Background

Members of both the Board and the Audit Committee want to make sure that their organization has thought through the risks and impacts of the operations and has made sound business decisions on the type of strategies they have in place to protect the critical processes and assets.

10. Seek certification and achieve regulatory compliance

The variety of certifications and regulatory compliance approvals related to business continuity does two things: allows companies to better market their business continuity prowess and maturity to customers and prospects; and allows them to better differentiate themselves in a competitive market.

Background

In addition to the business continuity certification process using the BS25999 standard, there is also a Service Organization Controls standard from the American Institute of Certified Public Accountants (AICPA) that will replace the SAS 70 report – now called the ISAE 3402 – for third-party servicers. These reports are intended to meet the needs of a broad range of users that need to understand internal controls at a service organization. With respect to management's need to understand security, availability, processing integrity, confidentiality and privacy at a service organization, the new "SOC 2 report" would contain detailed security and business continuity assessment findings for the use of clients of third-party servicers. These findings may not have appeared within an issued ISAE 3402 report.

Conclusion

The current business continuity industry landscape dictates that senior executives address business continuity planning with renewed vigor. Whether this is fueled by the prevention of high-profile events; the desire to remain competitive within the business landscape; or the natural course of the program as it matures, the C-suite requires that the legacy BCM principles be adapted to align with the increasing complexity of today's environment.

The growth in interest around BCM has yielded insight for those looking to justify investment in it. This is a way of both safeguarding a company's future and providing critical success factors in helping companies secure the output they desire.

Why invest in effective BCM	Critical BCM success factors
Increased pressure to perform and the global economic uncertainty are pushing pragmatic business requirements that increasingly require more complex business continuity strategies and processes	Gain executive sponsorship to drive the policies and framework, and secure certification and compliance
Globalization is requiring that business continuity programs be holistic in implementation and encompass all aspects of the global organization within a single consistent enterprise-wide framework	Establish a consistent process to conduct BIAs, risk assessments and other resiliency assessments – both strategic and operational – to help build the business case for investments around business continuity and disaster recovery options
Increasingly, maximum support from top executives and members of the C-suite requires the business continuity program's strategy to be aligned with the company's objectives	Conduct more comprehensive testing activities that integrate the dependencies to validate the recovery strategies and increase awareness within the recovery teams
The needs of a variety of stakeholders – customers, regulators, suppliers and employees – need to be considered when developing a business continuity plan	Leverage new technologies (e.g., cloud computing, virtualization, tools, as well as social media tools) in designing business continuity/disaster recovery strategies and response procedures

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 Advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject-matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2011 EYGM Limited.
All Rights Reserved.

EYG no. AU0924



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor. The opinions of third parties set out in this publication are not necessarily the opinions of the global Ernst & Young organization or its member firms. Moreover, they should be viewed in the context of the time they were expressed.

www.ey.com

IT Risk Management at Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers and more focused and faster in responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective IT risk management helps you to improve the competitive advantage of your IT operations, by making these operations more cost efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contacts

Global

Norman Lonergan (Advisory Services Leader, London)	+44 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com

Advisory Services

Robert Patton (Americas Leader, Atlanta)	+1 404 817 5579	robert.patton@ey.com
Andrew Embury (Europe, Middle East, India and Africa Leader, London)	+44 20 7951 1802	aembury@uk.ey.com
Doug Simpson (Asia-Pacific Leader, Sydney)	+61 2 9248 4923	doug.simpson@au.ey.com
Naoki Matsumura (Japan Leader, Tokyo)	+81 3 3503 1100	matsumura-nk@shinnihon.or.jp

IT Risk and Assurance Services

Bernie Wedge (Americas Leader, Atlanta)	+1 404 817 5120	bernard.wedge@ey.com
Manuel Giralt Herrero (Europe, Middle East, India and Africa Leader, Madrid)	+34 91572747	manuel.giraltherrero@es.ey.com
Troy Kelly (Asia Pacific Leader, Hong Kong)	+85 2 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Chiyoda-ku)	+81 3 3506 2411	stagno-gvnn@shinnihon.or.jp