Gartner

Survey Analysis Word Report

Publication Date:

ID Number: G00292880

Members of the Association of Contingency Planners Report on “What Keeps Them Up At Night”

Roberta J. Witty

Gartner surveyed ACP members during 3Q/2015 on the topics of BCM program management, business resilience and the impact of information security incidents and IT outages on production and recovery activities. This research report presents the results of that survey.

Key Findings❋

- Survey participants believe senior management is not always making the financial investments needed for BCM, even though they understand its importance (64% important vs 37% investing).
- Initially, “Business Resilience” is the new name for Business Continuity Management; however the functional risk disciplines being included in such programs is expanding beyond recovery.
- 41% of survey participants report they haven’t experienced an information security incident - *that they know about*.
- The majority of IT outages (76%) do not result in a disaster declaration.
- 59% of survey participants who are outsourcing IT services are involved in the backup of data for those services.

Recommendations❋

Business continuity management professionals should:

- Inventory how your organization manages and aligns its risk management disciplines defined in this survey so that you can determine what makes sense to be included in your business resilience program.
- Improve their coverage of information security incidents in all recovery plans, and especially business recovery plans because business operations can be greatly impacted for weeks and months.
- Plan to exercise the information security incident BCM scenario within the next six months to be better prepared of the growing threat to every organization.
- Require that their IT outsourcer be part of IT DR exercises so that there are no surprises and delayed recovery efforts when an actual disaster strikes.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Survey Objective*

The purpose of this survey is to explore the perspectives of Business Continuity Management (BCM) professionals on BCM program management, business resilience and the impact of information security incidents and IT outages on production and recovery activities. Results were presented to the ACP member community at the National Business Continuity Summit and Leadership Conference in October 2015.

The results reported in this report were based on questions formed from ACP community feedback in regards to “What keeps you up at night?” from March/2015. The survey was fielded to the ACP membership in July/August of 2015.

Data Insights*

Below are the results of the fifteen (15) questions we asked survey participants to answer. Note that there is a large (38%) Financial Services skew (banking, investment services and insurance) (Figure 18) and for large organizations (Tables 3 and 4).

BCM Program Management

Primary Reporting Responsibility for BCM Activities

Gartner frequently asks clients and survey participants where the different BCM program functions reside within the organization (see the Methodology section to read the definitions of each function). We ask this question because we want to track the reporting relationship of BCM as it is an indicator of program maturity as well as overall risk management.

For the ACP membership who completed this survey (aka survey participants), the following results are reported in Table 1 for the proportion of which role at their organization is responsible for a specific BCM activity. For clarity, a data point is shown only when over 10% of a role has responsibility for that activity.

Table 1. Primary Reporting Responsibility for BCM Activities by Role

BCM Program Function **Role**	**Crisis/ Incident Mgmt** n=137	**IT Disaster Recovery Mgmt** n=140	**Business Recovery** n=139	**Supplier Contingency** n=72	**Program Facilitation/ Mgmt** n=131	**Pandemic Planning** n=106	**Emergency Mgmt/ Public Safety** n=76
CEO or equivalent (1)	15%						
COO or equivalent (4)	14%		17%	10%			11%
CIO or equivalent (1)		**41%**					
CTO or equivalent (1)		21%					
Enterprise or Corporate Risk Management (6)	**25%**		**25%**	17%	**28%**	**27%**	**25%**
Procurement or Supply Chain Director (1)				**29%**			
Director/Manager, Emergency Mgmt-Safety (1)							11%
Director/Manager, BCM (1)					13%		
Human Resources (1)						13%	

Source: October, 2015 Gartner, Inc.

Note: Question: "In your organization, who has primary responsibility for BCM activities?" The Table only shows results for a role that had 10% or more for reporting responsibility. The numbers in parentheses indicate how many instances there are for the particular role.

The enterprise risk management (ERM) role is becoming the natural home for BCM: In at least a quarter of organizations, the ERM role is leading BCM activities, except for supplier contingency and IT DRM. Gartner has seen this trend over the last few years as risk management in general across the organization has taken on more importance as a way to effectively manage risk throughout the organization.

The two BCM activities that have a higher percentage of reporting line are IT DRM (41% to the CIO or equivalent) and Supplier Contingency (29% to Procurement or Supply Chain Director) make sense as these functions require specific skills found in those departments.

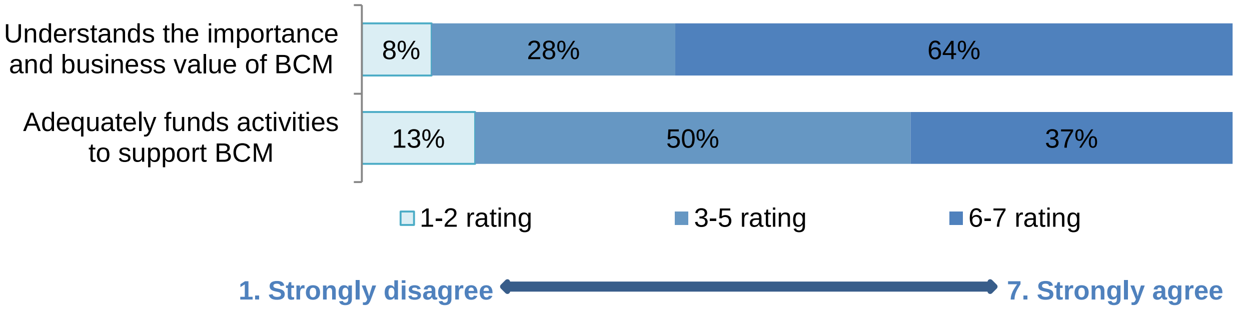
Action Item: Review your BCM program function reporting and align to the ACP best practice approach.

The Degree to Which Senior Management Values and Funds BCM

One of the "What keeps you up at night?" concerns expressed by the ACP membership was not having management support for the BCM program. Therefore, we asked a question to understand how BCM professionals perceive their own management's view on their BCM program.

Survey participants believe senior management is not always making the financial investments needed for BCM, even though senior management does understand its importance (64% important vs 37% investing).

Figure 1. Degree to Which Senior Management Values and Funds BCM



Source: October, 2015 Gartner, Inc.

n=156 Question: “To what degree do you agree or disagree with the following statements about your organization’s senior management?”

Respondents at large-size organizations are less satisfied with BCM funding than respondents at smaller (SMB) or larger (XL) organizations (Table 2). No other significant difference by company employee size or revenue level.

Table 2. The Degree to Which Senior Management Values and Funds BCM: Employee Size

Adequately funds activities to support BCM	**SMB** **(100 to 999 employees)**	**Large** **(1,000 to 9,999 employees)**	**X-Large** **(10,000+ employees)**
Rating 1,2	14%	13%	11%
Rating 3-5	32%	**65%***	48%
Rating 6, 7	**54%***	22%	**38%***

Source: October, 2015 Gartner, Inc.

n=156; * = statistically significant difference

Action Item: Use key performance indicators and BCM key risk indicators to educate senior management as to the importance of continuity of operations within your organization.

Business Resilience: What Is It?

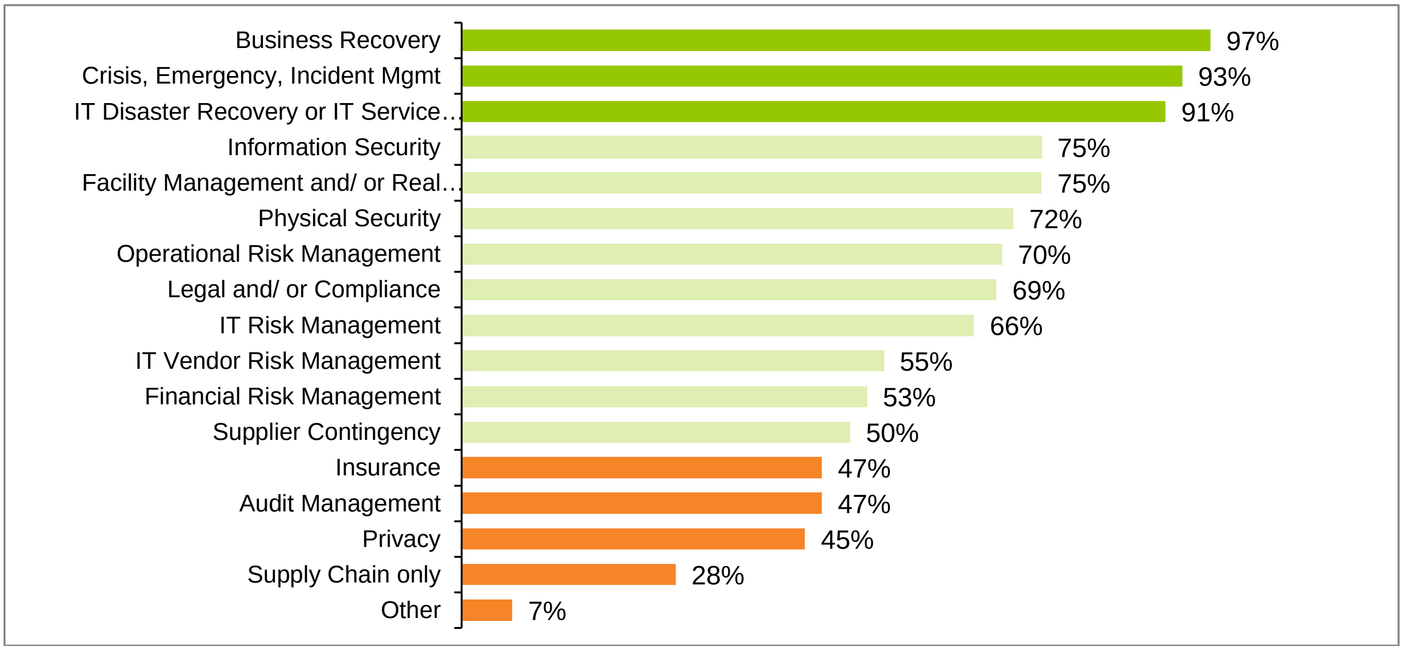
Gartner has historically considered resilience as a goal of an organization rather than a specific business unit. Obtaining resilience is an indicator of a more mature organization because it includes not only preparing to respond and recover from a business disruption, but it includes the organization taking an explicit effort to mitigate known risks before they become exploited, including the investment in people, tools, processes and facilities.

Disciplines Covered in a Business/Operational Resilience Program

Based on survey results, the term “business/operational resilience” seems to be the new name for the BCM program (Figure 2): almost all programs include the key BCM activities of business recovery (97%), crisis/emergency/incident management (93%) and IT DRM or IT service continuity management (91%) as part of the program. However, many organizations include other enterprise risk activities under the umbrella of business resilience, for example, information security (75%), facility management/real estate (75%) and physical security (72%).

As organizations include more activities under the “business resilience” umbrella, the function becomes similar, or synonymous to, operational risk management, as it becomes the focal point within the organization to manage, coordinate and create synergies across multiple risk disciplines.

Figure 2. Disciplines in business/operational resilience program



Source: October, 2015 Gartner, Inc.

n=137, multiple responses allowed, Question: “Which business disciplines does your organization have or plan to include in its business or operational resilience program?”

The one exception in Figure 2 is the inclusion of legal and/or compliance. We don’t think that this business function would ever be under the business resilience umbrella from a reporting perspective; however, we do think that covering legal and compliance impact makes sense for inclusion.

Action Item: Inventory how your organization manages and aligns its risk management disciplines defined in this survey so that you can determine what makes sense to be included in your business resilience program. Consider the culture of your organization as well as the industry when developing the disciplines to be included in the program.

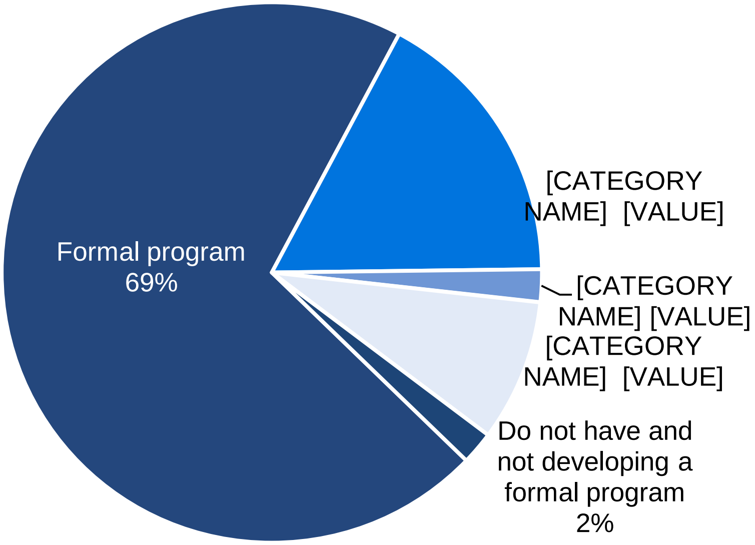
Maturity of the Business/Operational Resilience Program

The high level of maturity (69% have a formal program in place) regarding “business resilience” is in alignment with the high percentage of organizations including BCM as the key activity in the program (Figure 3). This high level of maturity can also be because:

- Survey participants are members in a BCM professional organization; and

- The Financial Services industry skew of 38% - this industry historically has had a higher level of maturity for their BCM programs.

Figure 3. Maturity of a Business/Operational Resilience Program

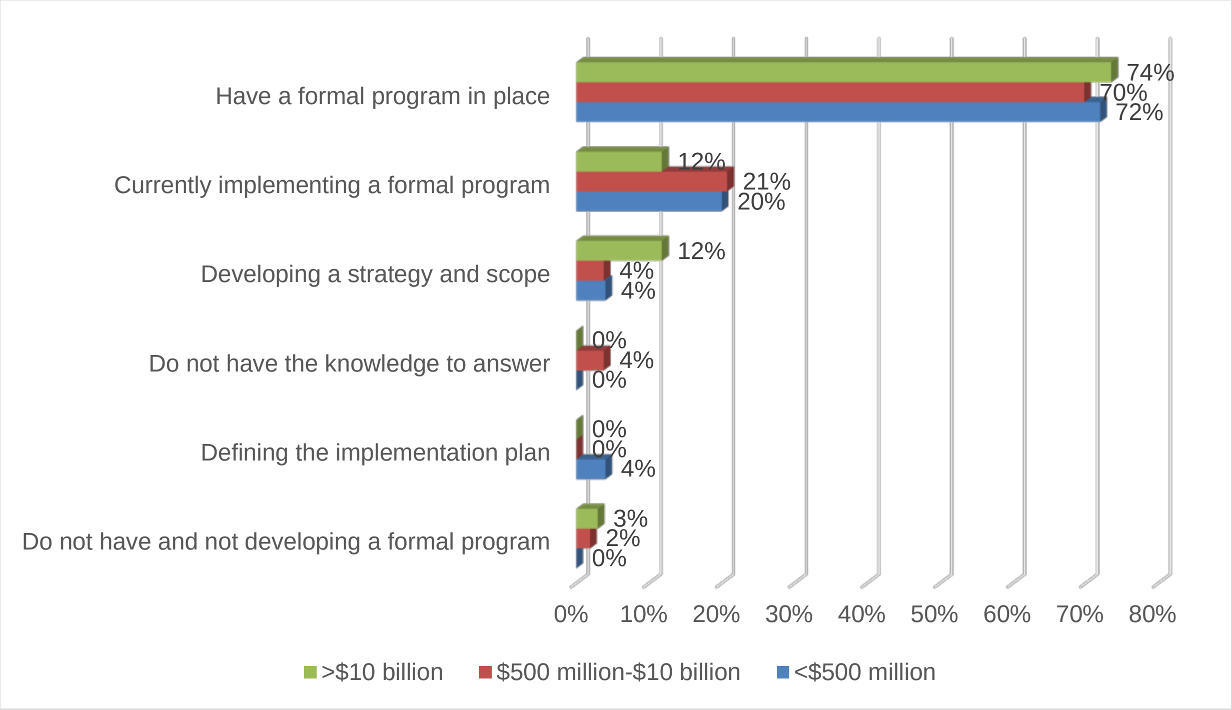


Source: October, 2015 Gartner, Inc.

n=156, Question: “What is the current state of your organization’s business or operational resilience program?”

Revenue level nor employee size vary the maturity level (Figures 4 and 5).

Figure 4. Maturity of the Business/Operational Resilience Program: By Revenue Level

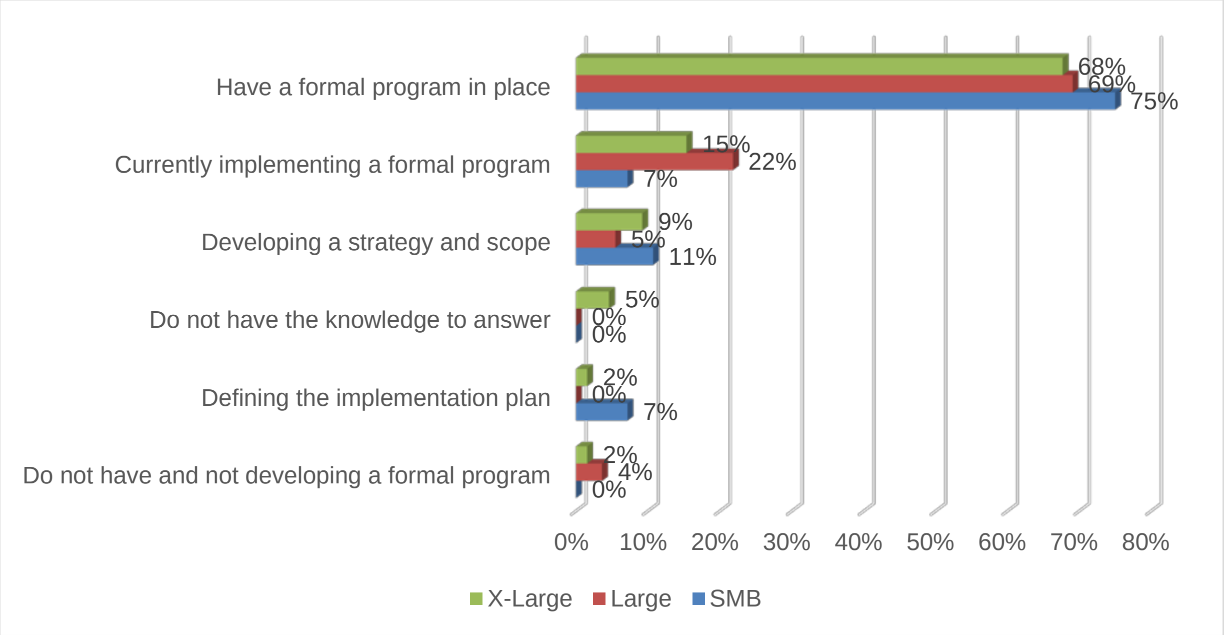


Source: October, 2015 Gartner, Inc.

n=112 total: $500 MM n=25, $500M-10B n=53 and Over $10B n=34

Note: because some respondents didn’t provide revenue data, the revenue breakdown is of a smaller sample. That’s how the percentage of “formal” in this table is higher than the overall (69%).

Figure 5. Maturity of the Business/Operational Resilience Program: By Employee Size



Source: October, 2015 Gartner, Inc.

n=148 total: SMB n=28, Large n=55 and X-Large n=65

Action Item: Use Gartner's ITScore online maturity self-assessment tools to establish a baseline and future maturity level roadmap for many of the risk disciplines included in a business resilience program.

Information Security and BCM Program Alignment

According to the Price-Waterhouse-Coopers (PwC) report entitled Global State of Information Security® Survey 2015, there is a 48% year-over-year increase between 2013 and 2014 in the number of security incidents. This report also states that preventive measures are inadequate to fully detect, mitigate and repair the impact of Information security incidents and will continue to fall short. They are necessary, but not sufficient and they fail too often. Monitoring is always after the fact and can take too long. According to the Mandiant ® "M-Trends® 2015: A View from the Front Lines" Report, 69% of victims were notified by an external entity.

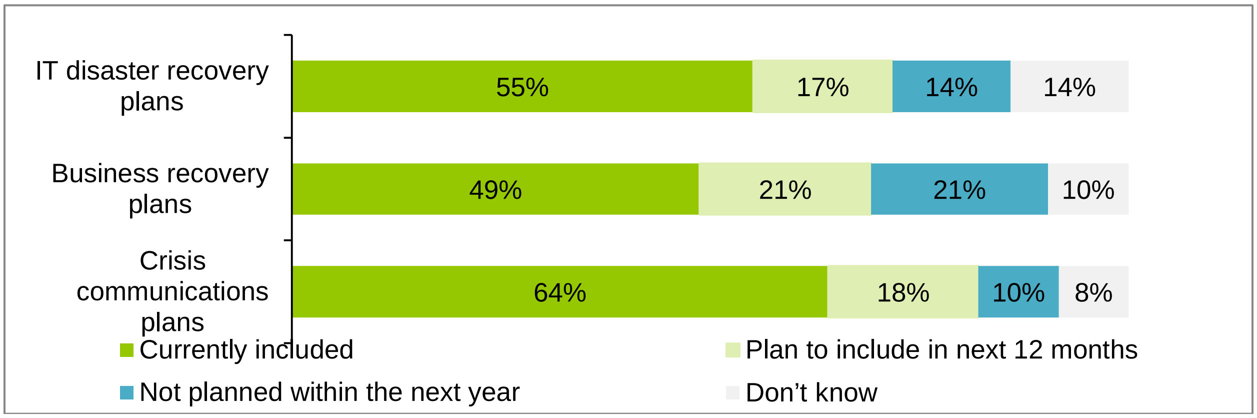
Therefore, we wanted to understand how the ACP membership aligns its information security and BCM programs. To start, we asked how many survey participants have experienced an information security incident: Thirty-one percent (31%) of survey participants report that they have experienced an information security incident within the last three years (question: "Has your organization experienced a cyber-attack or an IT outage?"). However, 41% report that they did not; our response to that position is "that you know about". The remainder of the respondents have either had an incident over three years ago (8%) or are not sure (20%) (which is different than the 41% who report that they definitively have not).

Organizations must be prepared to respond to the impact of an information security incident. In support of this preparedness approach, executives are clearly recognizing that cyber threats have become a serious enterprise risk-management issue: according to the PwC 2014 Global Economic Crime Survey report, almost half (48%) of respondents to PwC's said the perception of cybercrime risk to their organization had increased in the past year, up from 39% in 2011.

Information Security Incidents as a BCM Scenario

The growing awareness by executive teams is reflected in the response to the question regarding the inclusion of information security incidents as a BCM scenario: survey participants reporting that they currently include or plan to include information security incidents as a BCM scenario (Figure 6) in their IT disaster recovery plans (55% and 17% respectively) and crisis communications plans (64% and 18% respectively). Gartner is a bit surprised with the high percentages, however, this can be reflective of the large financial services skew in survey participants.

Figure 6. Information Security Incidents as a BCM Scenario



Source: October, 2015 Gartner, Inc.

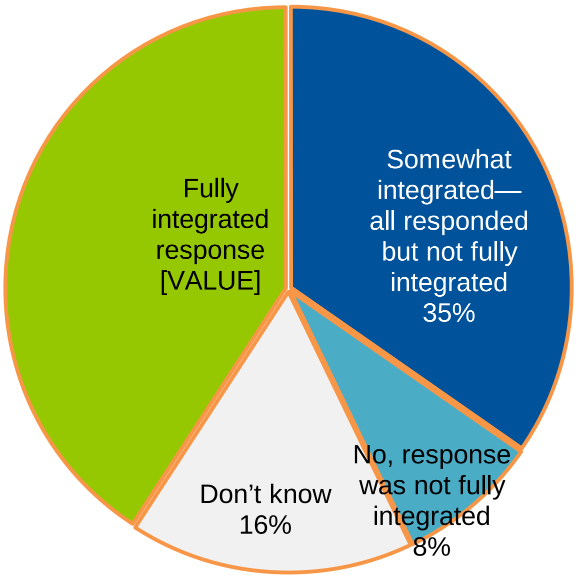
n=156, Question: "In the following plans, does your organization include information security incidents as a scenario?"

Action Item: Organizations should improve their coverage of information security incidents in all recovery plans, and especially business recovery plans (49% and 21% respectively) because with the impact of recent events such as those at Sony Pictures and the French TV5 TV station, business operations can be greatly impacted for weeks and months. The business needs to be prepared to work without essential IT services for longer than the recovery time objectives (RTOs) defined for the BCM program; reverting to alternative manual and semi-automated procedures may be required.

Information Security Incident Response Team Integration with BCM

The responses to the question regarding Information security incident response team integration (Figure 7) is a good start with 41% reporting a fully integrated response team, although Gartner is a bit surprised with the high percentages, however, this can be reflective of the large financial services skew in survey participants as well as the need for strong crisis management during an information security incident. Even so, it reflects a more siloed management process than what is needed for continuity of business operations with 35% reporting a somewhat integrated response team. It would be a good follow-up with the ACP membership to go deeper into this integration so that we understand how it works and areas for improvement.

Figure 7. Information Security Incident Response Team Integration with BCM



Source: October, 2015 Gartner, Inc.

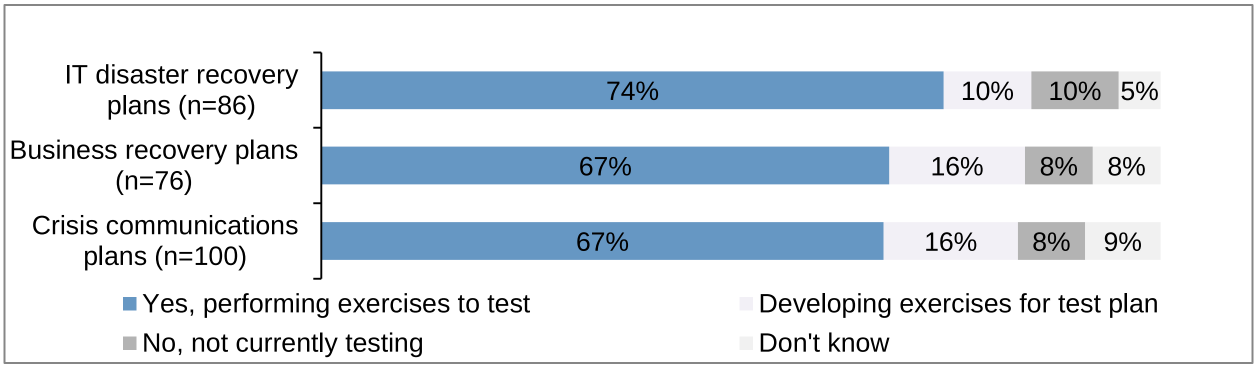
n=49; base= organizations with an information security incident in last 3 years Question: "Was you organization's response to its most recent cyber-attack or information security breach an integrated effort between Information Security, IT, IT DRM (IT Disaster Recovery Management) and BCM?"

Action Item: BCM program offices should work with their computer security incident response teams (CSIRT) to determine the integration points and procedures, and then exercise them.

Inclusion of Information Security Incidents in BCM Exercising

Without exercising your recovery plans, you have no sense of their effectiveness. The high percentage of survey participants reporting that they do exercise the information security incident scenario is an excellent position (Figure 8), although again, Gartner is a bit surprised with the high percentages, however, this can be reflective of the large financial services skew in survey participants.

Figure 8. Inclusion of Information Security Incidents in BCM Exercising



Source: October, 2015 Gartner, Inc.

Base: Survey participants reporting that they include information security incidents as a BCM scenario
Question: “In the following plans, does your organization perform exercises that test its information security incident procedures?”

Action Item: Organizations should plan to exercise this scenario within the next six months to be better prepared of a growing threat to every organization.

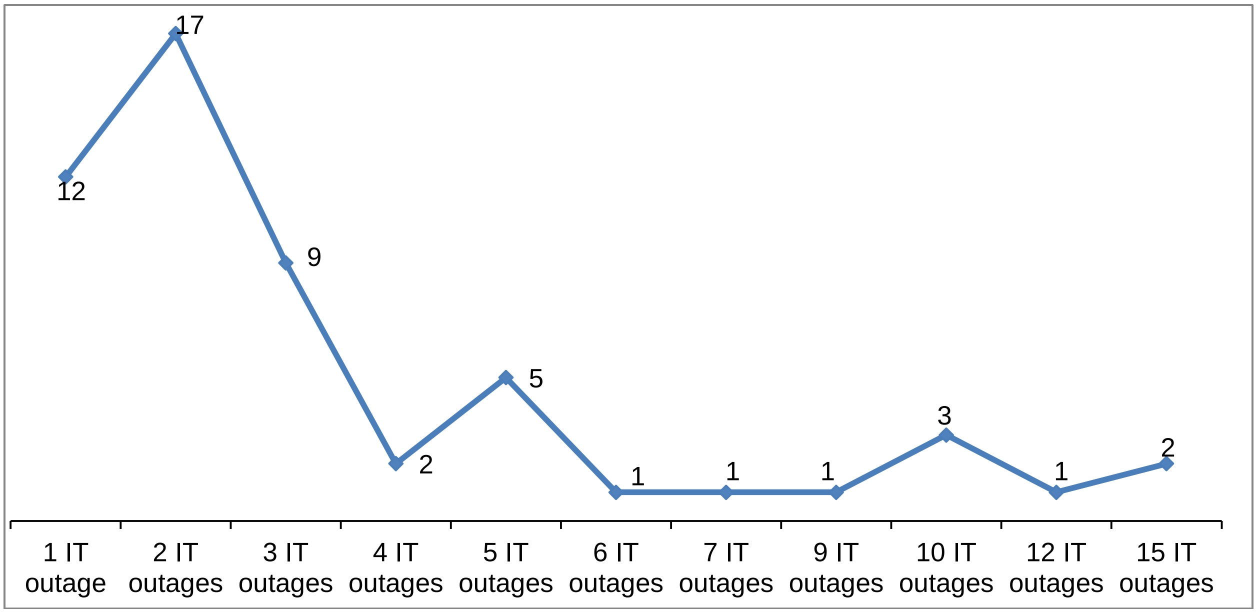
IT Disaster Recovery Management

IT outages are the traditional type of scenario that every BCM program must address. The ACP survey is no different: Survey participants report that 61% of them have experienced an IT outage within the last three years. Figure 9 reports the actual number of IT outages experienced by survey participants. One respondent noted 50 outages (with 3 declared disasters).

Number of IT Outages and Declared Disasters in the Last Three Years

EDITING: CAN YOU COMBINE FIGURES 9 and 10?

Figure 9. Number of IT Outages Experienced in the Last Three Years

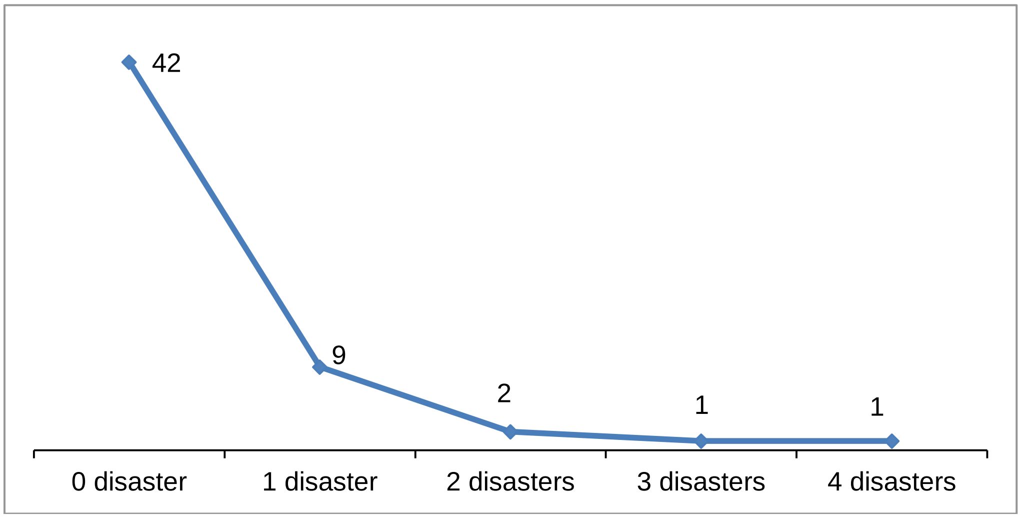


Source: October, 2015 Gartner, Inc.

n=55; Base=IT outage in last three years, excluding don't know Question: "In the last three years, how many IT outages has your organization experienced?"

What is interesting to see is that not every IT outage results in a declared disaster. Figure 10 shows that the majority of IT outages (76%) do not result in a disaster declaration. We don't think this is an unusual situation as most IT outages can be resolved through the major IT incident process within the timeframe required by the business so as not to have to declare a disaster.

Figure 10. Number of Disasters Declared in the Last Three Years



Source: October, 2015 Gartner, Inc.

n=55; Base=IT outage in last three years, excluding don’t know Question: “And of those IT outages experienced in the last three years, how many were declared disasters?”

Action Item: Maintain an inventory of all IT outages to document root cause and eventual outcome. This inventory can be used to educate management when additional funding for IT DRM is required.

IT Disaster Recovery Solutions

We wanted to understand how organizations deliver IT disaster recovery solutions in alignment with recovery requirements. Therefore, we asked two questions to determine the answer: what backup and recovery (formally known as data protection) solutions they use and what recovery approaches (where they recover) they most use. We wanted to see the answers to this question by recovery tier because each tier has different recovery requirements, e.g. short (i.e. under 4 hours) RTOs and RPOs are usually assigned to mission-critical business services while longer RTOs and RPOs (i.e. 24 hours or more) are usually assigned to less-critical business services. The approaches and solutions implemented to meet these different recovery requirements are also different.

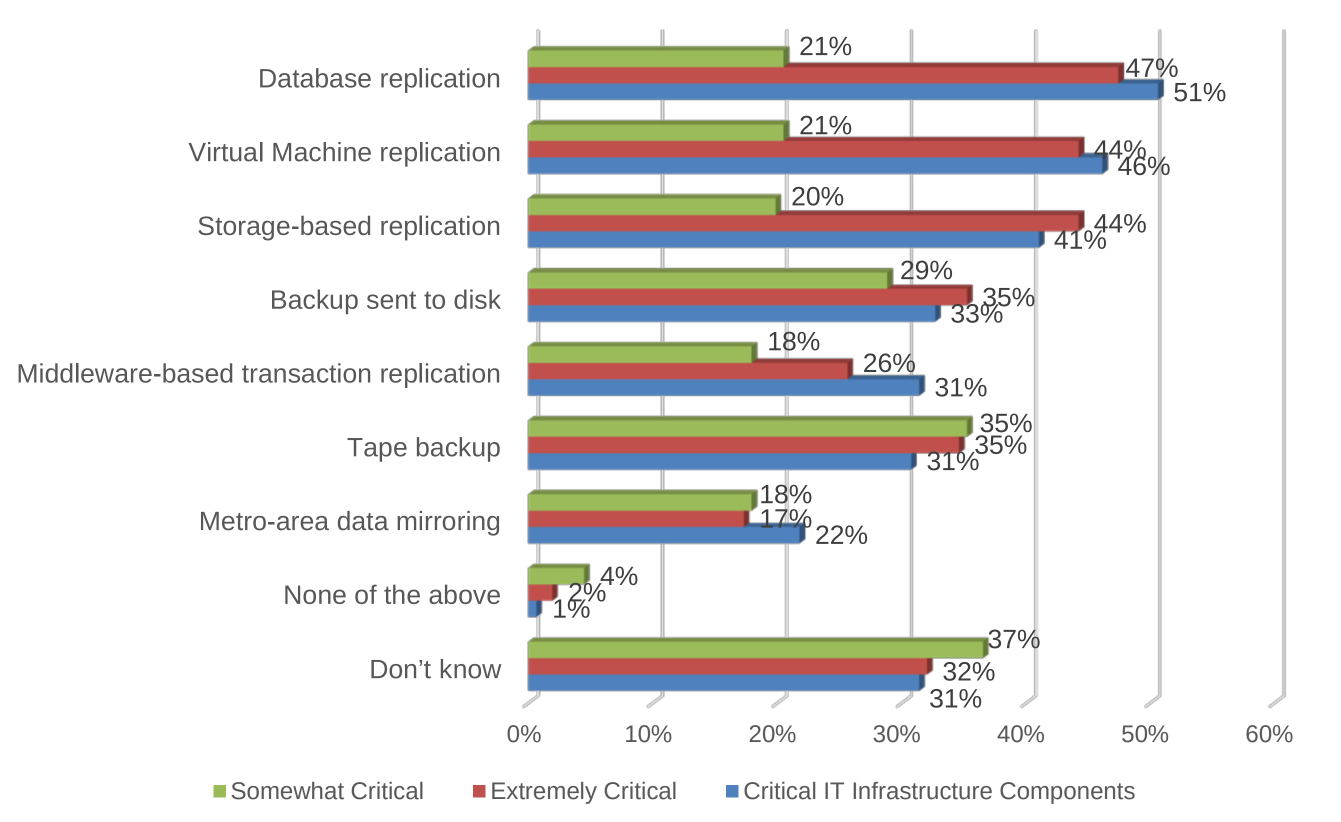
Note: the high percentage of “Don’t Know” responses to both questions is reflective of the higher number of BCM-specific professionals completing the survey as opposed to IT DRM-specific professionals; however, a manager or director of BCM should understand their high level approach to IT DRM.

Backup/Data Protection Solutions Used by Recovery Tier

Figure 11 reports on survey participant usage of backup/data protection solutions by recovery tier (Note 2). The results for the solutions that support short RTOs and RPOs (i.e. database (51% and 47%), virtual machine (46% and 44%) and storage-based replication (41% and 44%)) are consistent with what Gartner sees for the recovery of critical IT infrastructure components as well as IT services identified as extremely critical.

Tape backup is higher than expected for these two recovery tiers: 31% and 35% respectively.

Figure 11. Backup/Data Protection Solutions Used by Recovery Tier



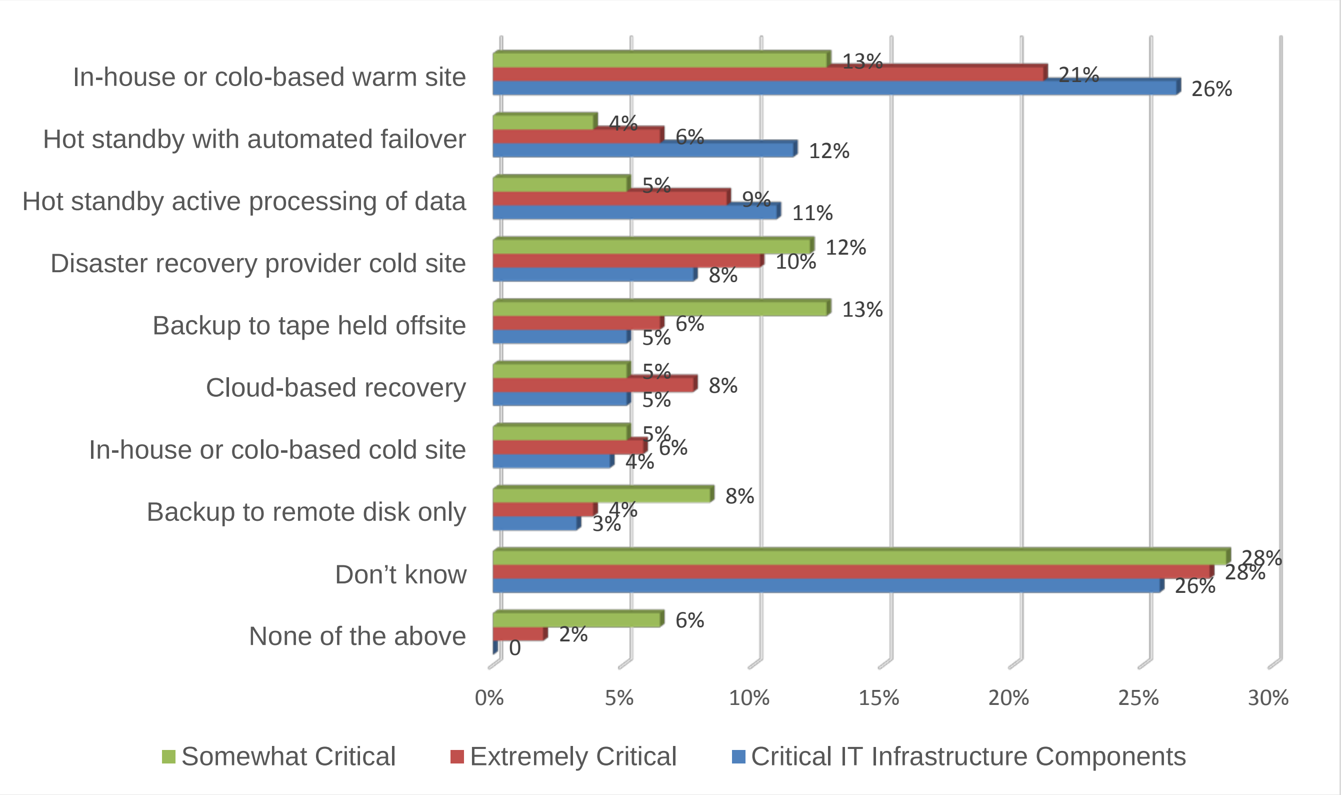
Source: October, 2015 Gartner, Inc.

Somewhat Critical n=99 Extremely Critical n=107 and Critical IT Infrastructure n=106, multiple responses allowed Question: "For this recovery tier, which data protection solutions does your organization use?"

Most-Used Recovery Approaches for IT Services

Figure 12 reports on survey participant usage of recovery approaches. In-house or co-location based warm site is the most common recovery sourcing strategy: 35% for critical IT infrastructure and 29% for extremely critical IT services. This result may be reflective of the financial service skew of the survey participants – financial services organizations often have multiple data centers across which they can build in recovery themselves, rather than using a third party disaster recovery service provider.

Figure 12. Most-Used Recovery Approaches for IT Services



Source: October, 2015 Gartner, Inc.

n=112: Somewhat critical n=113: Extremely critical n=116: Critical IT infrastructure components

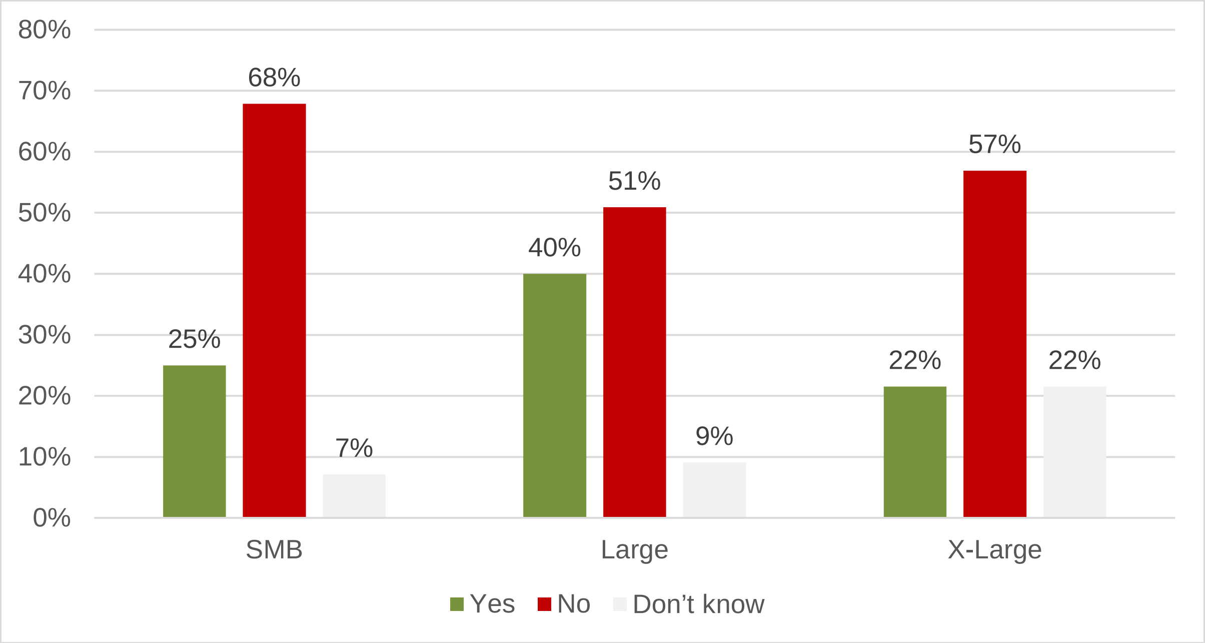
Question: "To ensure maximum availability for IT services for your organization, which of the following recovery approaches does your organization use most for each recovery tier?"

Action item: Establish an application tiering model that maps RTO, RPO, service level agreement, backup solutions and recovery approaches to each tier. This model can be used to rationalize the investment in IT DR solutions as well as to manage the recovery needs of new IT services.

Recovery of IT Services Outsourcing

We wanted to understand how organizations manage IT disaster recovery for their outsourced IT services. Therefore, we asked two questions to determine the answer: "How is data backup handled for outsourced IT services?", and "Does the IT outsourcer participate in the IT DR exercises that the organization conducts?". Only 28% of survey participants (44 in number) report using outsourced IT services for data processing. Figures 15 and 16 reflect this base number. Figures 13 and 14 show the difference by employee size and revenue level.

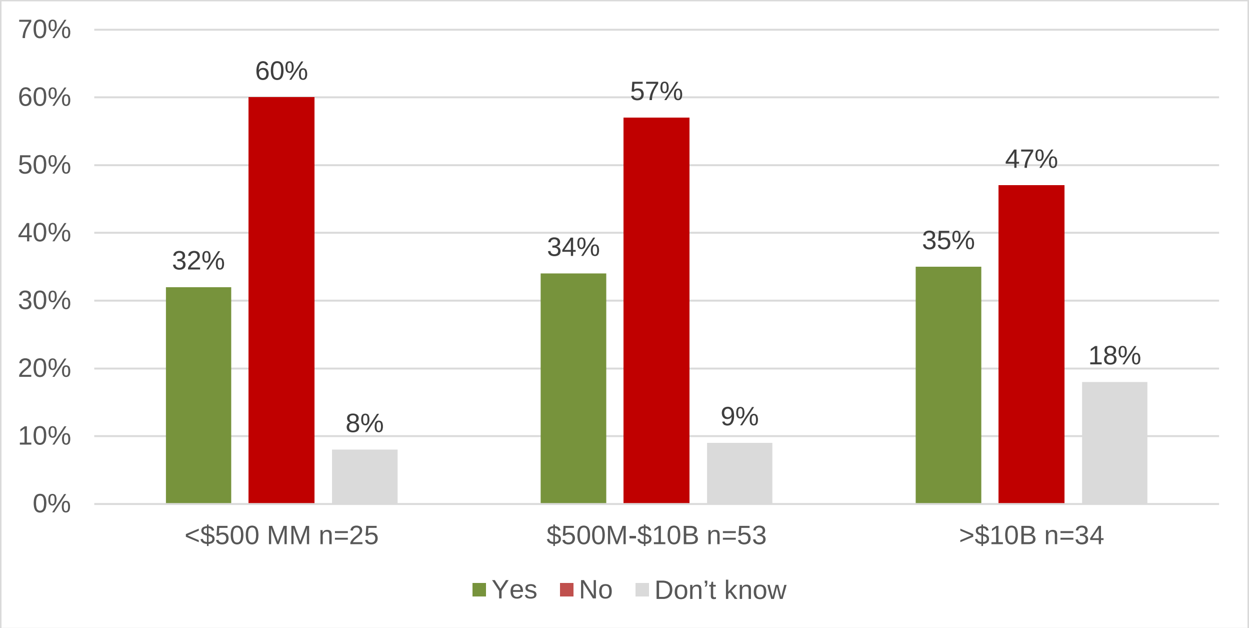
Figure 13. Use of IT Services Outsourcing: By Employee size



Source: October, 2015 Gartner, Inc.

n=148 total: SMB n=28, Large n=55 and X-Large n=65

Figure 14. Use of IT Services Outsourcing: By Revenue Level



Source: October, 2015 Gartner, Inc.

n=112 total: $500 MM n=25 $500M-10B n=53 and Over $10B n=34

Backup Data Protection for Outsourced IT Services

Figure 15 reports on how survey participants manage backing up of data processed by outsourced IT service providers: Of those survey participants outsourcing IT services, 59% are involved in the backup of data processed by outsourced IT service providers:

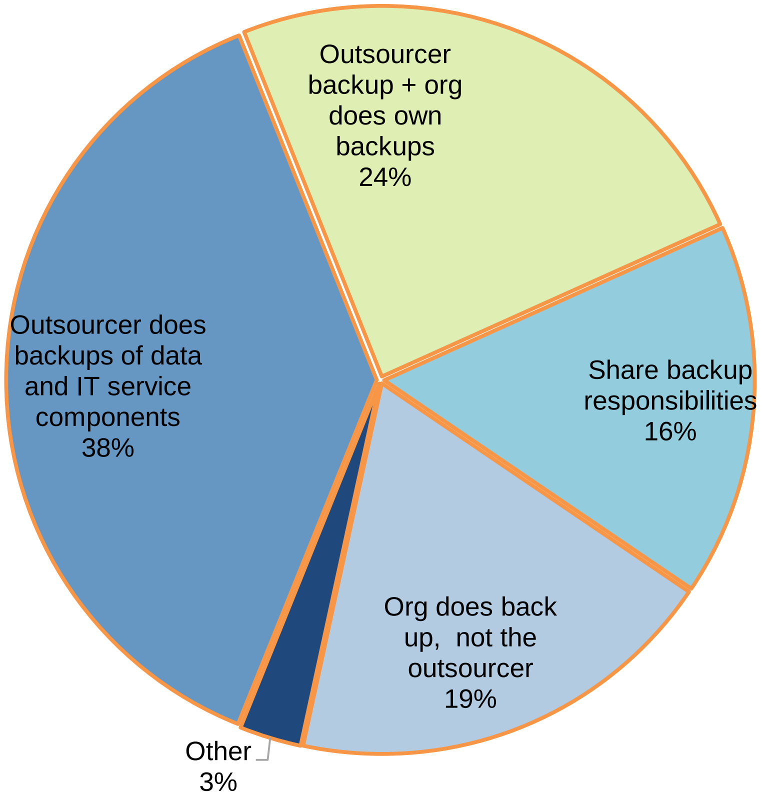
- 24% report that they backup the data in addition to the outsourcer;
- 16% report that they have shared backup responsibilities; and
- 19% report that they perform the backups only.

These results are in alignment with what Gartner reports is a contractual requirement from some of the large IT outsourcers. The example below is from the Amazon Web Services (AWS) click-thru agreement:

> *“4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content.”*

This is not necessarily true in enterprise licenses where the terms are more in depth and more negotiable.

Figure 15. Handling of IT Services Backup/Data Protection



Source: October, 2015 Gartner, Inc.

n=37, excluding 16% don’t know Base: Organization uses outsourced IT services for data processing Question: “How does your organization handle the backup of its IT services that are managed by the outsourcer?”

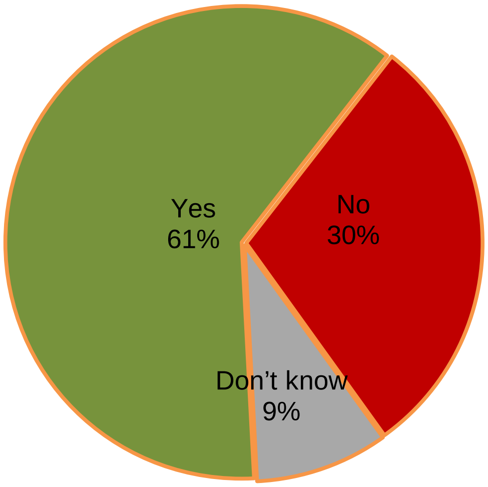
The sample sizes for this questions were too small to show any meaningful differences or alignment by employee size and revenue level.

Action item: Review your IT outsourcing contract to determine what the outsourcer is responsible for in regards to backup/data protection. Determine if their responsibility is in alignment with your organization’s backup/data protection requirements and take action to improve your ability to continue business operations in the face of an outsourcer’s disaster or one going out of business.

IT Outsourcer Participation in Customer IT Disaster Recovery Exercises

Figure 16 reports on how survey participants report IT outsourcer participation in customer IT DR exercises: 61% report that the outsourcer does participate in such exercises. This is a strong position to be in for both the customer and the IT outsourcer.

Figure 16. Vendor Participates in Disaster Recovery Exercises



Source: October, 2015 Gartner, Inc.

n=44, Base: Organization uses outsourced IT services for data processing
Question: “Does your organization participate in coordinated disaster recovery exercises with its IT services outsourcer?”

Action Item: Organizations should require that their IT outsourcer be part of IT DR exercises so that there are no surprises and delayed recovery efforts when an actual disaster strikes.

Methodology*

Gartner surveyed ACP members in the U.S. (see Note 1) during 3Q/2015 to help Gartner understand the perspectives of Business Continuity Management (BCM) professionals on business resilience and the impact of IT on production and recovery activities. 156 respondents participated. Organizations from all industries qualified; qualified participants must have reported being involved in and able to give detailed feedback on BCM activities at their own organizations. Interviews were conducted online. The survey was developed collaboratively by a team of ACP personnel and Gartner analysts who follow these IT markets and was reviewed and tested by Gartner's Research Data Analytics team and administered by ACP.

For purposes of this survey, we used BCM as the common term across all industries. Other terms you may use instead of BCM include: business continuity planning (BCP), continuity of operations (COOP), contingency planning or business contingency. Each BCM component defined below requires risk mitigation, planning, exercising, responding, recovering and restoring activities.

- ***Crisis or Incident Management:*** *Establishing command and control over the incident, ensuring life and/or safety, crisis communications (internal and external)*
- ***IT Disaster Recovery:*** *Recovering IT services for the organization (internal and external)*
- ***Business Recovery:*** *Recovering the business processes for the organization including the workforce, special equipment, non-electronic vital records et al*
- ***Supplier Contingency:*** *Recovering from a supplier's own outage*
- ***BCM Program Facilitation and Management:*** *Managing and governing the BCM program and its components across the organization*
- ***Pandemic Planning:*** *Pandemic planning is a unique scenario to manage. It may have different reporting responsibilities and tactics versus traditional BCM*
- ***Emergency Management and Public Safety:*** *Ensuring the life and/or safety of the public by government agencies*

There were three screening questions:

1 involvement in their organization's BCM activities;

2 their ability to provide detailed feedback; and

3 Role within their organization - vendors of BCM-related products and services as well as consultants were excluded because we wanted the focus to be on professionals practicing BCM in their own organizations.

There were fifteen (15) questions asked of each qualifying survey participant categorized as follows:

1 Sense of management's commitment to BCM in their organization

2 Their view of what business resilience means

3 The alignment of Information security incidents with BCM

4 The level of involvement that their organization has with outsourced IT services.

Definitions

[Press the Ctrl key and click inside this text to include market or technology definitions, if needed; for guidance about this section, please click the Methodologies Guidelines button in the Authoring Tools section of the Home tab in the ribbon above.]

Gartner Recommended Reading❋

Some documents may not be available as part of your current Gartner subscription.

BCM Program Communications: What to Report to the Board of Directors and Executive Management

Use KPI and KRI Mapping to Make the Business Case for Business Resilience, G00280981

ITScore for Business Continuity Management

Foundations of Business Continuity Management

Learn From the Experiences of Mature IT DRM Leaders

Attack on Sony Pictures Is a Digital Business Game Changer

Use IT Disaster Recovery Tiering to Build a Recovery Strategy That Works

Acronym Key and Glossary Terms

Evidence*

Gartner surveyed ACP members in the U.S. between July 10, 2015 and August 5, 2015 to help Gartner understand the perspectives of Business Continuity Management (BCM) professionals on business resilience and the impact of IT on production and recovery activities. 156 respondents participated. Refer to the Methodology section above for the detail behind the survey.

Note 1
Survey Participant Profile

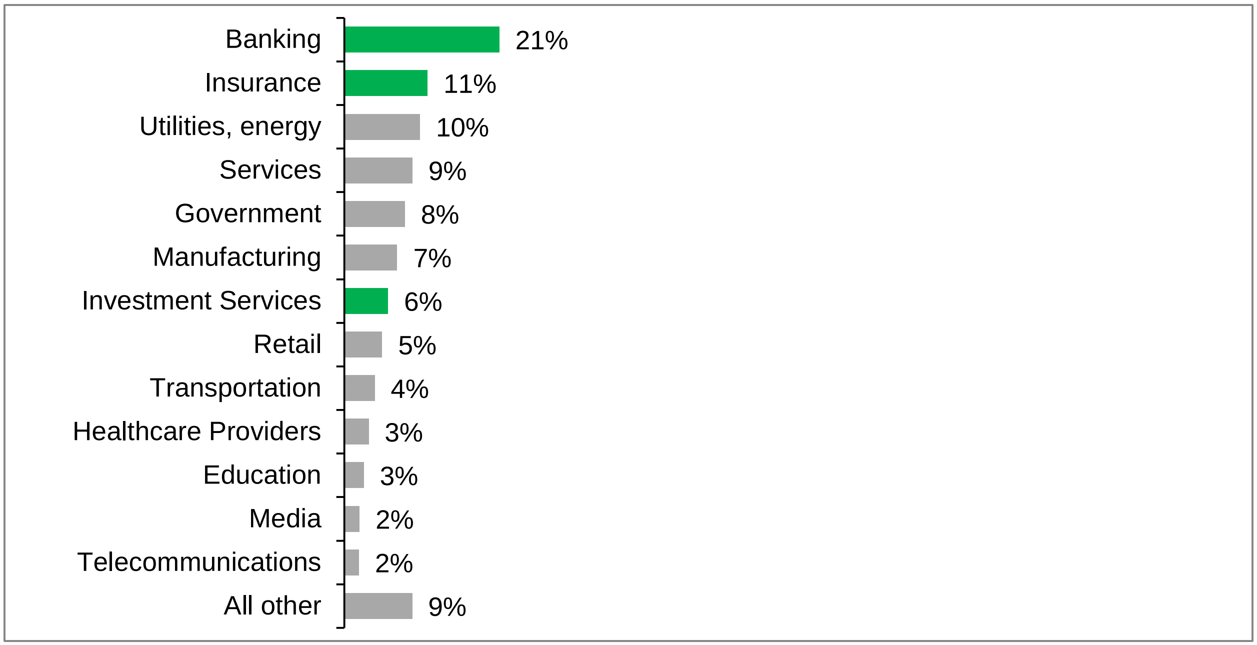
The profile of the joint ACP/Gartner BCM survey is defined by four ways: industry, employee size, revenue level and role. There are three important things to note:

1 There is a large skew from Financial Services at 38% including banking, insurance and investment services (Figure 17);

2 There is a large skew from large organizations: 37% with revenue at $3 billion or more and 42% with 10,000 employees or more Tables 3 and 4); and

3 Gartner performed an extensive rationalization process on the explicit roles submitted by survey participants. For example, we grouped manager and director as one role, advisor, analyst and specialist as one group, and so on (Figure 18).

Figure 17. Survey Participant Profile: Primary Industry



Source: October, 2015 Gartner, Inc.

n=156

Table 3. Survey Participant Profile: Revenue Level

Revenue Category	Percentage of Survey Participants
<$500 million	16%
$500 million to $1 billion	9%
$1 billion - $3 billion	10%
$3 billion to $10 billion	15%
$10 billion or more	22%
Don’t Know/Refused	28%

Source: October, 2015 Gartner, Inc.

n=156

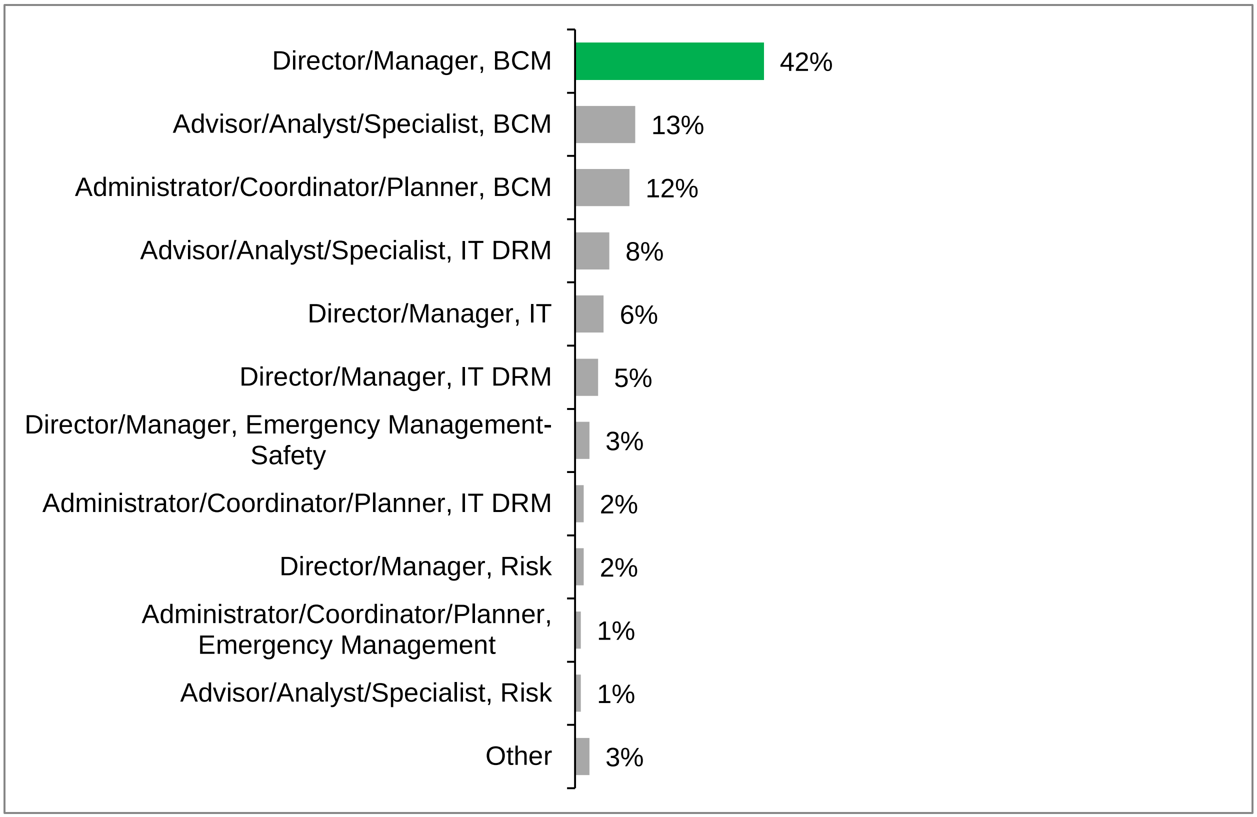
Table 4. Survey Participant Profile: Employee Size

Employee Size	Percent of Survey Participants
<1,000 employees	21%
1,000 – 9,999 employees	35%
10,000 or more employees	42%

Source: October, 2015 Gartner, Inc.

n=156

Figure 18. Survey Participant Profile: Role within their Organization



Source: October, 2015 Gartner, Inc.

n=156

Note 2

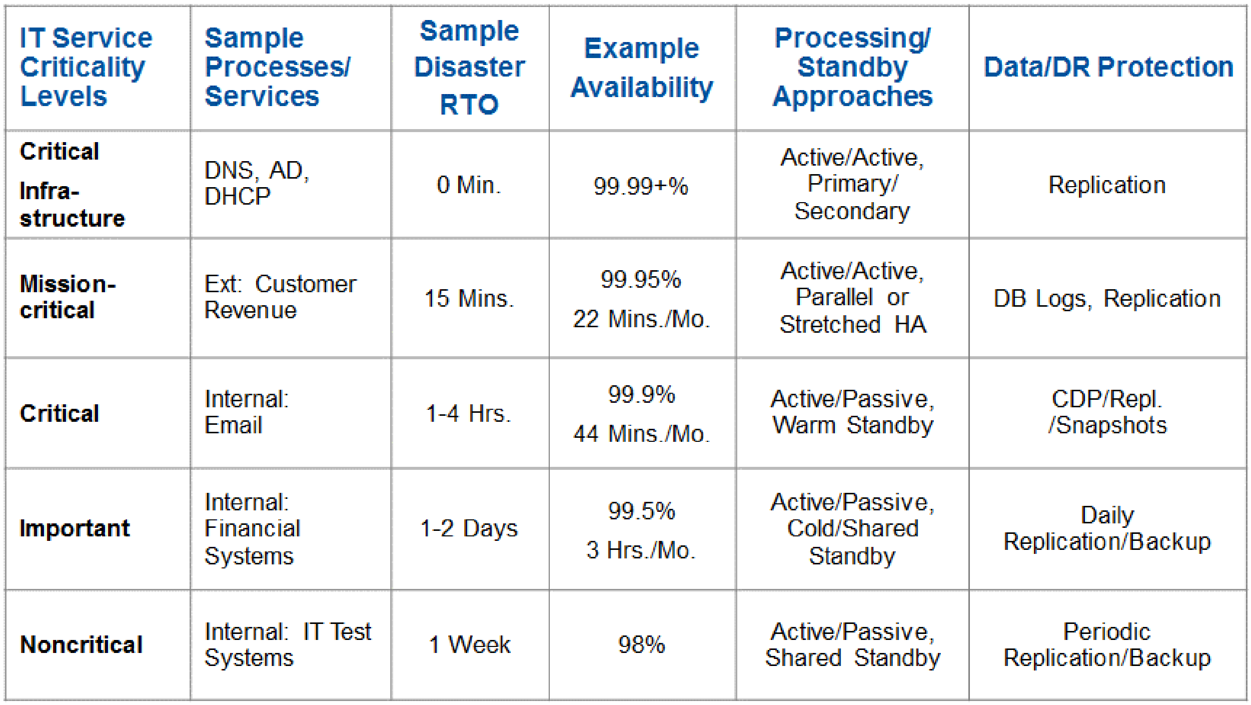
Recovery Tiers

For this survey, we used three tiers to define the criticality of applications:

- Critical IT infrastructure: the IT infrastructure that needs to be recovered before any other application can be recovered. Examples include: the network, telephony, enterprise directory, security solutions such as firewalls and identity and access controls, emergency/mass notification services, BCM planning software et al.
- Extremely Critical: Applications that are extremely critical for operations of the business to continue. These applications typically have short RTOs, e.g. less than 4 hours.
- Somewhat Critical: Applications that are important for operations of the business to continue, but their recovery can wait for more than 24 hours.

Figure 19 is an example of a recovery tier model using five tiers.

Figure 19. Recovery Tiers & Supporting Technologies



IT Service Criticality Levels	Sample Processes/ Services	Sample Disaster RTO	Example Availability	Processing/ Standby Approaches	Data/DR Protection
Critical **Infra-structure**	DNS, AD, DHCP	0 Min.	99.99+%	Active/Active, Primary/ Secondary	Replication
Mission-critical	Ext: Customer Revenue	15 Mins.	99.95% 22 Mins./Mo.	Active/Active, Parallel or Stretched HA	DB Logs, Replication
Critical	Internal: Email	1-4 Hrs.	99.9% 44 Mins./Mo.	Active/Passive, Warm Standby	CDP/Repl. /Snapshots
Important	Internal: Financial Systems	1-2 Days	99.5% 3 Hrs./Mo.	Active/Passive, Cold/Shared Standby	Daily Replication/Backup
Noncritical	Internal: IT Test Systems	1 Week	98%	Active/Passive, Shared Standby	Periodic Replication/Backup

Source: October, 2015 Gartner, Inc.