State of Enterprise Risk Management 2019

By STEPHANIE BALAOURAS

Forrester Research and the *Disaster Recovery Journal* have partnered to field a number of market studies in IT disaster recovery (DR), business continuity (BC), and overall enterprise risk management in order to gather data for company comparison and benchmarking, to guide research, and for the publication of best practices and recommendations for the industry. This is the ninth annual joint survey. This particular study focuses on the state of enterprise risk management (ERM). Specifically, we designed this study to determine:

- ERM roles, responsibilities, and reporting structure.
- The relationship of business continuity to ERM.
- Crisis response - including business continuity crises and other brand and reputational crises.
- The solutions firms invest in to facilitate ERM.

More And More Firms Have Formal Enterprise Risk Management programs

According to our study, 36 percent of firms have a formal enterprise risk management program while another 25 percent say they have a single director or head of risk for select areas but not necessarily a broad enterprise program (see Figure 1). More and more firms are making the effort to unite isolated areas of risk management in order to more objectively identify, assess, mitigate, and respond to risks to organizational goals

Figure 1 ERM Program Formalization

Base: 55 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

Heads Of Risk Management Are Reporting Higher Into The Organization

Together with more formalized programs, we see the increasing presence of a chief risk officer (CRO), which has not always been common. CROs first started appearing after Basel I was established in the late 80s early 90s. They were responsible for credit and liquidity risk to make sure financial services firms kept enough capital on hand in the case of major market fluctuations. They then became even more common and prominent as firms had to deal with compliance to Sarbanes-Oxley in 2004 to 2005. In this survey, we found that:

- **At least 29 percent of firms have a CRO or equivalent**. According to our survey, 29 percent of respondents report their highest-ranking risk officer reports into the CRO of the department of the CRO. (see Figure 2-1). As much as the CRO role has gained prominence in the last 10 years, the diversity of responses to this question is also indicative how little industry consensus there is on the necessity of the role itself and where the highest-ranking risk officer should report. The most common response in the Other category was "multiple," meaning the individual had multiple dotted line or reporting relationships.
- **CISOs are taking on more and more risk responsibility**. CISOs are no longer responsible just for technical security operations related to threat prevention, detection, and response. They increasingly lead the firm's efforts related to broad information risk including privacy, cybersecurity, legal, compliance, and ethical risks related to how the organizations collects, processes, stores, and uses data. In our study, 11 percent of respondents reported their highest-ranking risk officer reports into the CRO.
- **The head of risk reports directly into a C-level executive**. It's not only important where you head of risk management reports but how high into the organization. Too far removed from a c-level executive and your head of risk won't have enough influence to affect changes in strategy, operations, and risk mitigation efforts across the firm. He or she will also struggle to garner business participation in risks assessments, response plan development, and response plan simulations. Our survey revealed good news: 68 percent of the heads of risk management report directly into a c-level executive.

ERM Responsibilities Are Increasing

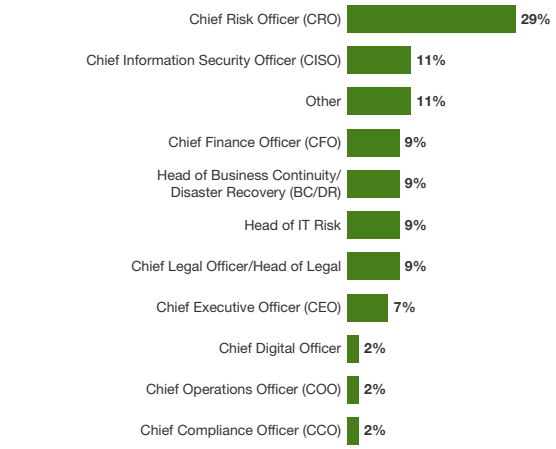
As firms continue to seek formalize their ERM efforts, they are both unifying and taking on responsibility for additional areas of risk management. According to our study, 57 percent are fully or mostly responsible for operational risk. Other areas of notable responsibility include reputational risk (41) and compliance risk (40 percent) (see Figure 3).

ERM And BC Teams Are Working More Closely Together

Historically, BC teams have coordinated with counterparts in risk management but haven't necessarily taken the extra step to begin collaborating closely on core planning processes such as business impact analysis and risk assessments; this is starting to change. Our survey also found that:

Figure 2-1 Functional Head of Risk Management

"Into which executive or department does the highest-ranking risk officer report?"

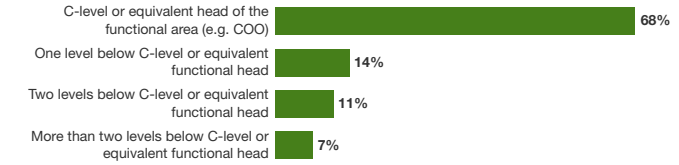


Base: 45 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

148895

Figure 2-2 Reporting Lines for The Head of Risk Mgt.

"Which level does the highest-ranking officer report into?"

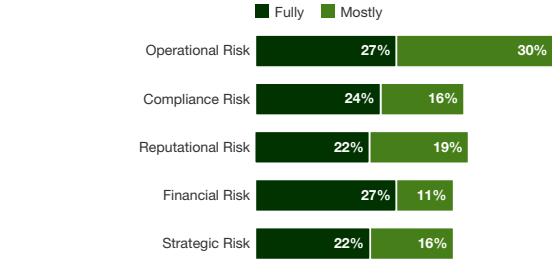


Base: 44 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

148895

Figure 3 ERM Responsibilities

"To what extent is your ERM program or efforts responsible for the following?"



Base: 37 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

148895

- **Twenty-nine percent say their BC teams report directly into ERM**. An additional 31 percent say they work closely with risk management to share information. We expect this trend to continue regardless of whether the highest ranking risk officer reports into the CRO or CISO.
- **Seventeen percent say they no longer have a dedicated BC team**. Meaning they treat historical BC risks such as extreme weather, IT disruptions etc. the same as any other disruption to the business so there is no needed for a dedicated team. As firms continue to consolidate operational risk domains under a single umbrella and make less and less of distinction between the category of risk to the business and how to identity and prepare for it, we'll see a unified approach to planning from business impact analysis and risk assessments to plan development and testing.

A Majority Have Invoked A Response Plan During The Last Three Years

Individuals not involved in enterprise risk management often view risk mitigation efforts and response plans as expensive insurance policies their firms will rarely, or ever, use. However, as is often the case, conventional wisdom is wrong. According to our study, 62 percent of respondents have experienced a critical risk event at least once during the last three years (see Figure 5-1). According to our study:

- **IT failures, extreme weather, and intellectual property theft were the most common**. Security pros often remark that there are two types of companies, those that have been breached, and those that don't know yet. It's an apt saying when you consider that three of the top ten most frequent critical risks events relate to security from IP theft to malicious cyberattacks to customer privacy abuses. (see Figure 5-1). When we asked respondents which risk events are the most worried about in the future they ranked cyberattack, IT or business system failure and theft of IP as their top concerns for the next three years.
- **Operational efficiency and employee productivity suffered the most after the event.** Add new text (see Figure 5-2)

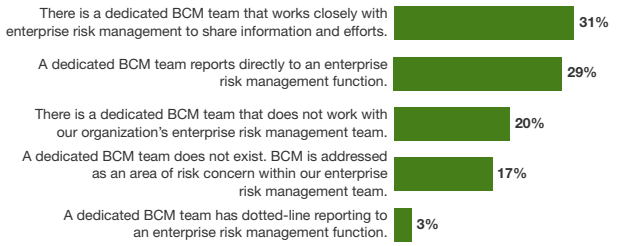
Technology Investment Focuses On Core Planning And Communication

Unfortunately in risk management, there is no single solution that provides all of the capabilities that you need to for: 1) the upfront planning (business impact analysis and risk assessment); 2) the plan development (document, maintain, and test plans); and 3) the incident or crisis response itself (real-time collaboration, communication, and decision-making based on internal and external information). Even with these areas, there are tools that specialize in delivering specific functionality, for example, automated communication solutions that provide reliable mass and two way, communication or a dedicated command center software with geospatial risk mapping and visualization that can also overlay multiple data feeds (e.g., social media, weather data, surveillance cameras, access points, etc.) to add risk context during incident/crisis response. In our survey:

- **New investment is going to BC planning software and response**. For some time, investment in BC planning software had plateaued because there wasn't much innovation in the software, most vendors focused on delivering the core planning capabilities but lacked real-time incident/crisis management functionality. Planning still remains the core value proposition but

Figure 4 ERM And BC Relationship

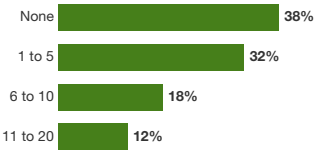
"Describe how you approach business continuity management (BCM)?"



Base: 36 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

Figure 5-1 Frequency Of Critical Events

"How many discrete critical risk events (where there were significant financial or business impacts) has your company suffered in the past three years?"
Critical risk events include, but are not limited to: active shooters, natural disaster/extreme weather, IT failures of business-critical systems, supply chain disruptions, cyberattacks, etc.



Base: 34 Enterprise risk management decision makers

Figure 5-2 Types Of Critical Events

"Which of the following risk event types did your company experience in the past three years?"
(Top 10)

1. IT failure of a business-critical system or application
2. Extreme weather or natural disaster
3. Theft of intellectual property
4. Cyberattack (data breach, ransomware, DDoS attack, etc.)
5. Critical infrastructure failure (power, water, transportation, etc.)
6. Customer privacy abuse, data breach, or fraud
7. Supply chain disruption/failure
8. Geopolitical events/social unrest
9. Customer backlash/adverse media exposure/social activism
10. Workplace misconduct

Base: 21 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

many vendors have begun expanding focus to include vendor risk management and improve their relevance in incident/crisis response. According to our study, 56 percent of plan to expand or upgrade existing implementations and 6 percent are planning to implement in the next 12 months (see Figure 6). In addition to software, firms are planning investment in the response teams themselves – a recognition that it's a matter of if, not when, a crisis is likely to occur.

- **… followed by GRC software and automated crisis communication tools**. Firms tend to invest in automated crisis communication and notifications services because the scale, reliability, and other functionality of these solutions is almost impossible to duplicate with internal tools. In addition, communication is also one of the areas that firms struggle with the most during an incident or crisis. For those firms seeking to consolidate risk management functions under a single umbrella, GRC solutions are attractive. Usually deployed to help firms deal with compliance and general risk, these vendors have been adding dedicated BC planning modules that have been competitive with dedicated solutions.

Study Methodology

In the fall and winter of 2018, Forrester Research and the *Disaster Recovery Journal* (DRJ) conducted an online survey of 55 DRJ members and Forrester clients. In this survey:

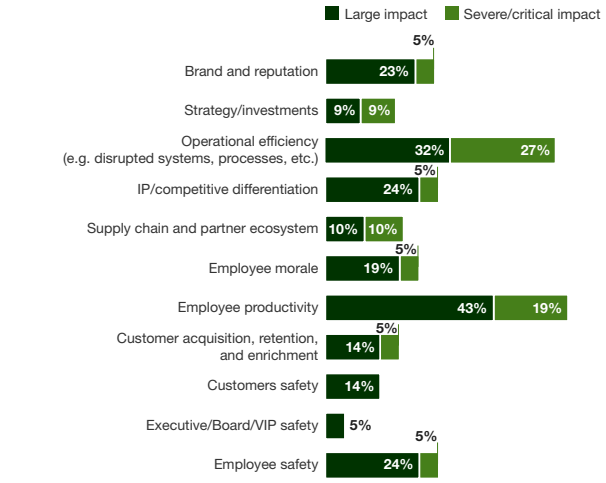
- **All respondents** indicated that they were decision-makers, influencers, or contributors to their firm's risk management activities.
- **Respondents were from a range of company sizes**: 40 percent had 1 to 999 employees; 22 percent had 1,000 to 4,999 employees; 24 percent had 5,000 to 19,999 employees; and 14 percent had 20,000 or more employees.
- **Respondents were from companies with a range of revenues**: 44 percent of respondents were from companies with revenues of less than $500 million; 10 percent were from companies with revenues of $500 million to $999 million; 22 percent were from companies with revenues of $1 billion to $4.99 billion; 6 percent were from companies with revenues of $5 billion to $10 billion; and 18 percent were from companies with revenues of more than $10 billion.
- **Respondents** were from a variety of industries.
- **Respondents were primarily from North America** but there was representation from Europe, the Middle East, Africa, South America, and Asia. Many companies had business operations in multiple regions: 83 percent of respondents had locations in North America; 32 percent had locations in Europe, ; 27 percent had locations in Asia; 16 percent had locations in the Middle East or Africa and 12 percent had locations in South America.

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

Stephanie Balaouras, is a vice president, research director of security and risk for Forrester Research.

Figure 5-3 Most Significant Impacts

"Looking back on your most critical event, how severe was the impact in each of the following categories?"

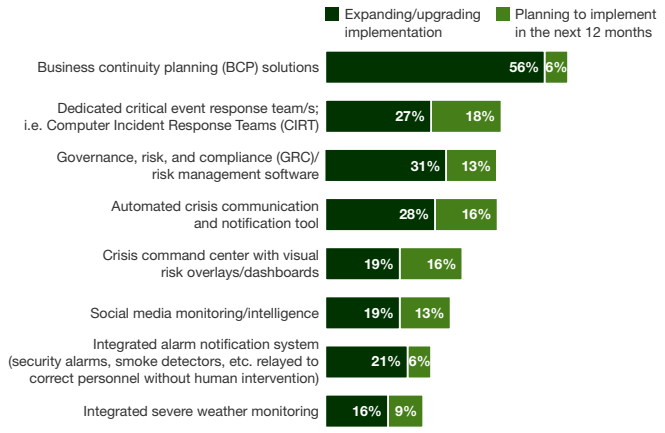


Base: 21-22 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

148895 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 6 Technology Solution Adoption For ERM

"What are your plans to adopt the following solutions and/or capabilities to help you identify, analyze, mitigate, and respond to risk?"



Base: 31 to 33 Enterprise risk management decision makers
Source: Forrester/DRJ Survey 2019

148895 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.