Alitek

Two-Sides of the Same Coin

Issue 1

2 Two-Sides of the Same Coin

5 Research from Gartner:
Market Guide for Crisis/Incident Management Platforms

15 Contact Us

Gartner

Two-Sides of the Same Coin

Introduction

When a company experiences a disruption of operations, there are typically two types of responses. The first response is focused on managing the crisis in order to minimize impacts to personnel, assets and any external sources that were affected. This type of response, known as Incident Command (IC) is the standard in Federal, State and Local governments in the US and beyond as well as many regulated industries. It is is becoming more common in industry as the benefits of the response process are understood. The second response known as Business Continuity Management (BCM) is focused on returning the business as a whole to its normal operating condition. This type of response has been standard for those companies that wished to plan for natural disasters, but has become more broad as the scope of disruptions has been expanded to plan for scenarios as civil unrest, IT disruptions and attacks, manufacturing/engineering defects, and operational disruptions, among others.

Increasingly, companies see that these responses are two sides of the same coin. There are pre-planning elements, communication requirements, and a need to balance team structure with the flexibility that evolving situations demand – not to mention the after-action requirements of financial and legal reporting and record keeping. The Gartner Market Guide on Crisis/Incident Management Platforms (C/IMP) highlights the convergence of the traditional two different response groups and the commonalities that benefit from a more comprehensive, integrated software solution can provide.

Incident Command System (ICS) Solutions

ICS is a framework that has been adopted as the mandated standard for federal, state and local agencies. Utilizing a common hierarchy for command and control, ICS defines and guides the process for managing resource and finances and establishes a common communications platform. Because of its widespread adoption by first responders, ICS allows for better interoperation amongst disparate divisions and organizations. First responders are able to quickly get up to speed and move to provide needed resources at the required locations.

Per the Gartner report, companies are quickly realizing that, "The need to align with national emergency/incident response management frameworks is driving other nongovernmental organizations to use C/IMP solutions. Using a C/IMP solution that automates the use of such frameworks can help keep the organization in good standing and in control of their part of the event, and not get federalized by a government agency due to poor event management." By 2020, it is predicted that 45% of all commercial organizations will have implemented a C/IM solution in their BCM programs.

ICS can be complex, especially for organizations that don't exercise and train in it regularly. However, by using a C/IM solution, companies can more easily implement the ICS framework. The best example of an integrated C/IM solution is PrepareRespondTM powered by Alitek.

PrepareRespondTM is a cloud-based ICS, Business Continuity, Crisis Communication and Plan Management tool that can streamline your organization's response efforts. PrepareRespondTM was developed by industry experts including highly experienced Federal Incident Commanders and nationally recognized business continuity specialists.

PrepareRespond allows for:

- tasked based guidance of all ICS forms and response steps,
- information carry forward from one period to the next
- configurable business continuity tasks and forms,
- resource and financial management of all assets entered into the system,
- crisis communications to key stakeholders, executives and media outlets,
- real time situational status and common operating picture through configurable dashboards,
- all in a Software as a Service (SaaS) platform that is cross-browser supported and mobile capable.

Benefits of employing a management tool

It has been said that during a major crisis, "The cheapest thing is money." During any crisis or business continuity event, the most important priorities are protecting lives, protecting the environment and then protecting company assets and shareholder value. When faced with any event, organizations must respond rapidly and this costs money. You can reduce your response cost by implementing an integrated response tool that:

- Helps your people respond to the incident quickly and autonomously,
- Guides resources through your response plan more efficiently with tasks and reminders,
- Giving your response managers up-to-date information on the response actions including what resources are available, on order and currently operating,
- Giving your executives financial insight into to the daily burn rate, projected future costs and total costs to date,
- Speeding the decision making process by getting information onto dashboards in real time.

All of this timely data gives your responders actionable intelligence that they can use to respond faster and with less waste.

Benefits of integration and automation

Business continuity and major crisis events are fortunately not everyday events in most companies. Many will need to respond just once or twice a year. Economics dictate that dedicated teams running BCM and C/IM are kept small and the response efforts are augmented with additional employees as needed. PrepareRespondTM assists this business reality by automating response efforts through online forms, task management and communications. Your resource, who may be new to the position and has never been trained, can quickly sit down in front of PrepareRespond and complete the tasks assigned to them. They will be able to enter data and PrepareRespond workflows automatically, populate ICS forms, resource requests and reports. This leads to a faster response, cutting costs overall.

This is a function of an intuitive interface that has been repeatedly tested with ad hoc teams with little to no prior ICS training. PrepareRespond's ease-of-use also becomes a significant advantage by decreasing training costs and exercise costs for those companies that through policy or regulation see the benefit of enabling front-line personnel.

PrepareRespond Differentiators

RELIABLE

PrepareRespond was *built by experts for experts* using industry-leading technology that is available 24/7/365. Each client system resides in a redundant, private, cloud-hosted virtual-server ensuring reliable operation and privacy of data. PrepareRespond is be ready when you need it.

- Designed on DoD and NIST compliant technologies;
- Private virtual-servers ensure high reliability and the redundancy assurance provided by multiple data centers;
- Automatic template configuration allows novice users to bring up forms and documents quickly;
- Industry-leading records management and legal hold integration;
- Integration with all leading GIS-modeling and weather systems;
- Cross-platform tested and compliant with all major browsers with mobile device support

INTUITIVE

PrepareRespond system is designed intuitively so that it is easy to master. It provides a logical flow that experienced responders are currently familiar with. From your seasoned responders to the newest members of the team, *our guided workflows keeps all team members working towards one common goal, restoration.*

- Guided configurable "Planning P" and BCP work flows with email / text notifications;
- Simple reporting that shows the status of all assigned tasks and forms;
- BCP and ICS forms automatically feed each other and remain up to date;
- Detailed resource and financial tracking roll up from field to the office;
- Financial data that can track, commercial, local, state and federal assets separately

INTEGRATED

When responding, access to the most current information is key to the response team's success. PrepareRespond offers a fully integrated system that brings plan management, business continuity and ICS into one system built on the latest proven technologies. This enables quicker access to relevant information and allows for all concerned parties to be better informed.

- Automated ICS forms that are configurable to your unique needs
- Plan management for all your facilities in one place
- Information is automatically fed from plans into ICS and BCP forms
- Common Operating Picture of all assets and incidents with key information
- Dynamic Situational Status board display
- Full audit logging of activities and record lock down

FLEXIBLE

Every incident presents a constantly changing dynamic and responders need a system that is flexible enough to meet and adapt to their needs. PrepareRespond *is available online and in real time.* It is built to provide a balance of organizational structure with the need for ad hoc flexibility to meet the fluid nature of the response and locations in which responders must work.

- Fully supported by mobile devices such as phones and tablets -- with a subset of offline capablilties;
- Hosted SaaS offering that does not require any software on devices;
- Live Common Operating Picture (COP) with dynamic data that refreshes all systems in real time;
- Company-specific and configurable business continuity plan support

Summary

The Gartner report recognizes Alitek, with our PrepareRespond providing a proven approach and more complete solution to the C/IM space. Leveraging tested technologies with a forward-looking interface provides a tool that is uniquely intuitive and powerful. The PrepareRespond solution delivers this with a lower total cost of ownership than less-comprehensive solutions.

Source: Alitek

Research from Gartner

Market Guide for Crisis/Incident Management Platforms

Crisis/incident management platforms automate the management of tasks, resources, expenditures, partners, communications and data during a crisis. This Market Guide helps crisis managers understand the capabilities of these solutions for effective management of organizational or public disruption.

Key Findings

- C/IMPs have mainly been used by government agencies, utilities and transportation organizations. However, private enterprises are using them to demonstrate command and control and to align with national emergency/incident response management frameworks.
- The need to align with national emergency/incident response management frameworks is driving other nongovernment organizations to use C/IMP solutions. Using a C/IMP solution that automates the use of such frameworks can help keep the organization in good standing and in control of their part of the event, and not get federalized by a government agency due to poor event management.
- Organizations should also look to the smart city initiatives of which they are a part. Some of the C/IMP vendors support this use case.
- The overlap between BCMP and C/IMP is growing. However, most BCMP solutions are not a full-fledged C/IMP, and vice versa. Over time, the functionality of these two BCM technologies will overlap more and more, but as two modules, not one.

Recommendations

- Determine the full set of C/IMP capabilities based on the seven C/IM disciplines that your organization needs. Be sure to include the national emergency/incident response management frameworks or smart city initiatives that your organization's C/IMP solution must comply with or align to when managing crisis events.
- Determine which C/IMP is right for your organization based on your C/IMP requirements. If you are already using a BCMP, BPM-platform-based case management frameworks or EH&S solution, its C/IMP capabilities may be "good enough" for your needs.
- Use a SaaS/cloud solution as a delivery model to retain external communications and C/IM management capabilities, especially in the face of a targeted cyberattack.
- Assess the maturity of your organization on an annual basis, against the benchmark for your industry in order to ensure you are line with industry best practices regarding the use of C/IMP.

Strategic Planning Assumption

By 2020, 45% of BCM programs at maturity Levels 3 through 5 will be using crisis/incident management platforms to manage their business disruptions, up from 6% today.

Market Definition

An organizational crisis is defined as a situation that threatens or is perceived to threaten the organization's workforce, business operations, physical/virtual assets and/or the general public, resulting in serious interruption to business services, damage to reputation and brand, or negative impact to shared value. Even small events can get out of control very quickly because of a number of factors:

- They are usually a surprise.
- You have insufficient information regarding the event, and therefore have limited decision-making ability.
- Events often get misdiagnosed — the initial thought is that it is small and not important, and as analysis is conducted or more information comes in, the event should be reclassified, but is not.
- There is usually an escalating flow of events that take the organization beyond its normal, day-to-day operating procedures.

In an Associated Press interview with Sony Pictures Chairman Michael Lynton on 8 January 2015 about the targeted cyberattack they experienced in November 2014, Mr. Lynton stated:

"There's no playbook for this, so you are in essence trying to look at the situation as it unfolds and make decisions without being able to refer to a lot of experiences you've had in the past or other peoples' experiences. You're on completely new ground."

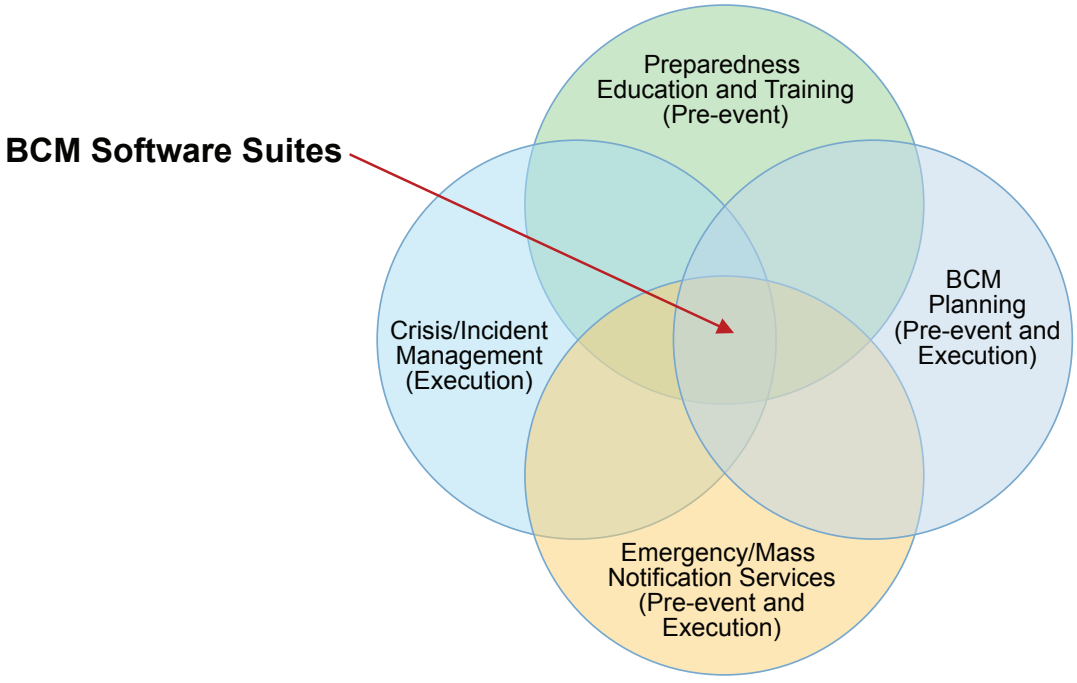
- There is fast and often inaccurate scrutiny and conclusion drawing from outsiders and some insiders, resulting in your reputation being assessed in the public arena.
- Management can adopt a "siege mentality" and therefore isolates itself, resulting in an unwillingness to share information, which only contributes to a poor response to the event.
- Management and employees can panic, which can lead to saying things that are inaccurate, inflammatory or excessive, thereby not supporting the organization's situation.
- Depending on the scope of the impact, organizations quickly lose control of the situation (or at least the storyline) due to a number of factors.

Sony Pictures' targeted cyberattack was unprecedented in its impact, and few organizations are prepared for such a crisis. However, for a strong crisis/incident management (C/IM) program, it doesn't matter the source or trigger of the crisis: Organizations must be prepared for both the large and small business disruptions. Therefore, they need to develop a crisis management program and exercise its procedures multiple times.

The goal of a C/IM program is to contain and minimize the impact of a business disruption that has escalated to the level of a crisis/incident (see Note 1) on individuals, localities, businesses, public agencies, the environment and public safety. Damage can also be measured by the effect of a crisis on an organization's reputation, operations and revenue streams. Also, the C/IM program helps guide a response that meets the government's standards.

A key component of a C/IM program is C/IM technology to help manage and analyze the changing conditions during a crisis. C/IM solutions are one component of the overall business continuity management (BCM) solutions marketplace (see Figure 1).

FIGURE 1 The BCM Solutions Marketplace



Source: Gartner (December 2015)

The C/IM marketplace is composed of seven technologies in the overall crisis management technology ecosystem (see Figure 2) that deliver automation assistance during a crisis event.

The focus of this Market Guide is on the C/IM platform (C/IMP) and capabilities.

This Market Guide does not address the common services that support the C/IM technology ecosystem (see Note 2), nor the following markets:

- Business continuity management planning
- Travel risk management
- Business process management (BPM)-platform-based case management frameworks
- Physical security/recovery and restoration equipment and services (Gartner does not research these technologies)
- Humanitarian disaster relief
- Environmental, health and safety (EH&S; Gartner does not research these technologies)

Not all solutions would be used by every organization; for example, if your organization is not involved in business operations that would impact the environment, health or safety of the workforce and public, you would not use EH&S solutions. Or, if your organization is not directly involved with public safety, you would not use humanitarian disaster relief solutions (the exception is Google Crisis Response, which is a tool for both consumers and organizations to use to register displaced people or find needed resources after a disaster).

FIGURE 2 The Overall Crisis/Incident Management Technology Ecosystem

Source: Gartner (December 2015)

Also, vendors in the BPM-platform-based case management frameworks market support the C/IMP critical capabilities (noted below). However, many do not deliver these capabilities in a prebuilt manner; rather, they are custom-built to address the specific needs of the customer.

BCM planning (BCMP) solutions have a C/IMP module that can be used to exercise plans as well as manage many aspects of the invocation of response and recovery plans during a real event. However, they are not considered full-fledged C/IMP. Over time, the functionality of these two BCM technologies will overlap more and more, but as two modules, not one.

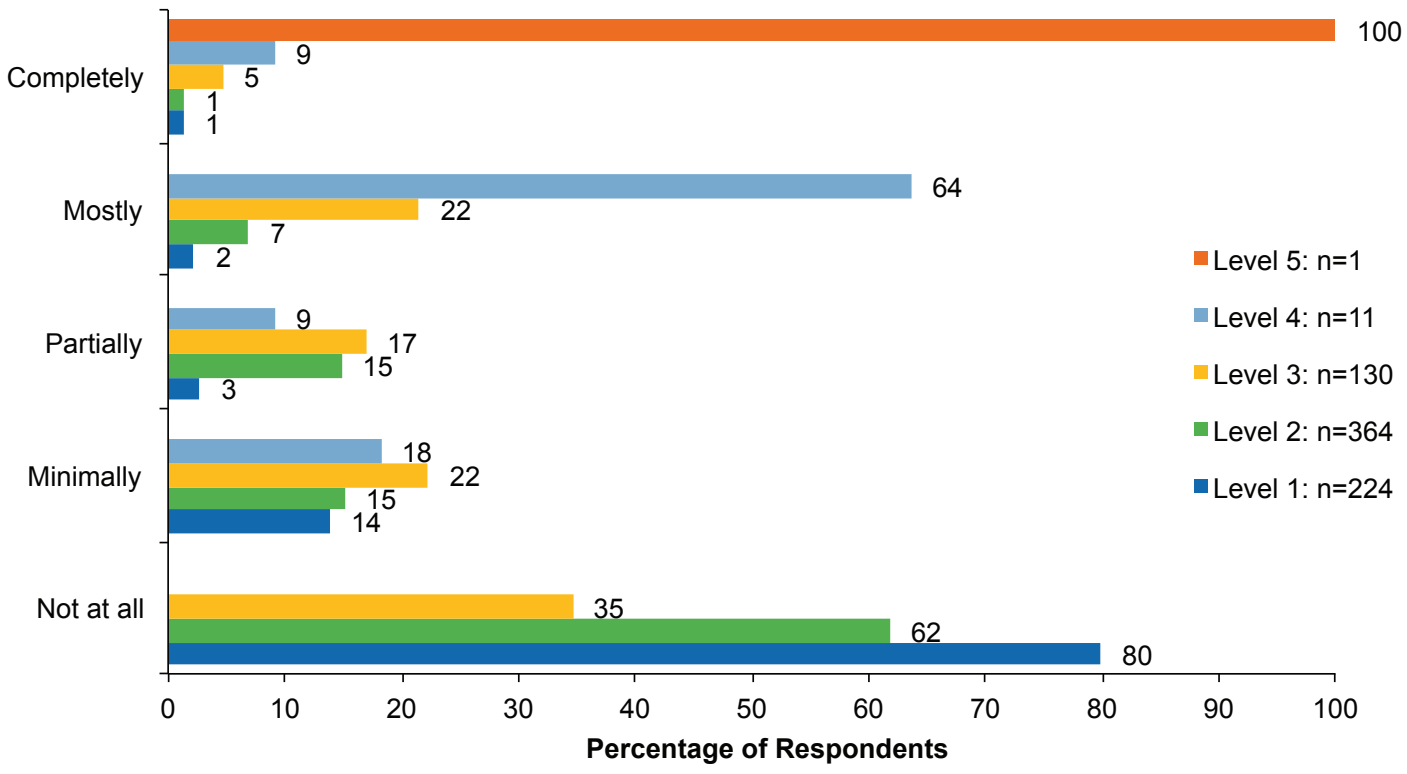
Most C/IMPs are generalized for the management of any type of crisis/incident; however, some are specialized to the operations of one industry — for example, government, utilities, healthcare, transportation, aviation, or oil and gas.

Market Direction

Based on the results from 2010 to 2015 of the Gartner ITScore for Business Continuity Management maturity self-assessment tool, 20% of organizations use C/IMP either completely or mostly in BCM programs (Figure 3). Gartner predicts that by 2020, 45% of BCM programs at maturity Levels 3 through 5 will be using crisis/incident management solutions, up from 6% today.

Note: The 6% and 20% figures were calculated as shown in Table 1.

FIGURE 3 Use of a Crisis/Incident Management Solution: By Maturity Level



n = 730. Cumulative results from Gartner IT Score for BCM, September 2010 through June 2015.
Source: Gartner (December 2015)

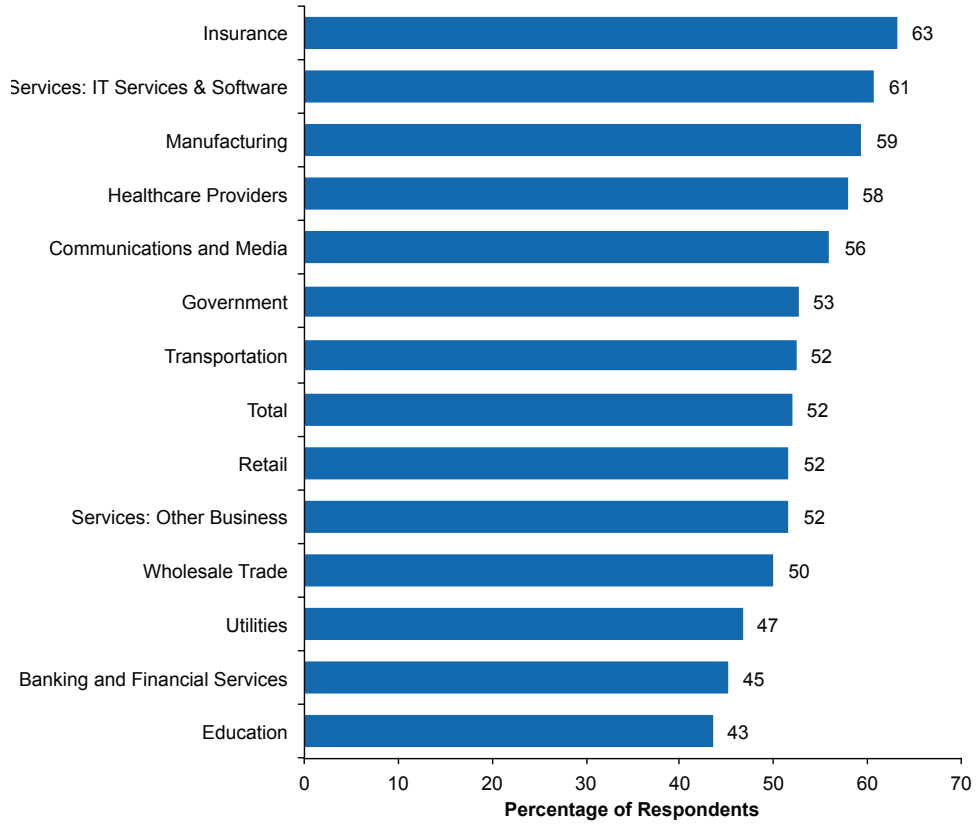
Table 1. Calculating the Percentage of C/IMP Usage

Maturity Level	N	Combined Percentage Completely or Mostly Using a CIM Tool	Result
1	1	100%	1
2	11	73%	8
3	130	27%	35
4	364	27%	98
5	224	3%	7
Subtotal	730		149
Percent of Total			***149/730 = 20%***
Percent of Levels 3 to 5		(used for the Strategic Planning Assumption)	***44/730 = 6%***

n = 730. Cumulative results from Gartner IT Score for BCM, September 2010 through June 2015.
Source: Gartner (December 2015)

Historically, C/IMPs have been used by government agencies, utilities and transportation organizations to manage the large public safety concerns of a crisis. However, private enterprises are using them (see Figure 4) due to the growing need to demonstrate command and control across all stakeholders during business disruptions, and to align with national emergency/incident response management frameworks.

FIGURE 4 Use of a Crisis/Incident Management Solution: By Industry



n = 356. Results from Gartner Security and Risk Management Survey, 2015
Source: Gartner (December 2015)

Regional and national disasters require enterprise-based C/IMP for the critical infrastructure sectors to interact — at least at the level of status reporting and communicating with one another and with local, regional, tribal, national and international government agencies. The Federal Emergency Management Agency (FEMA)'s XchangeCore project (a middleware framework to tie together many disparate technologies used for C/IMP) helps to remove some process barriers in place today, as well as provide meaningful situational-awareness information to public and private organizations. In the U.S., government and regulatory agencies, such as the U.S. Occupational Safety and Health Administration (OSHA) and the United States Coast Guard (USCG), are driving more organizations to follow the FEMA National Incident Management System/Incident Command System (NIMS/ICS) model while integrating more automation in the response process. These agencies can federalize (Merriam-Webster defines "federalize" as "to cause [something] to be under the control of a federal government") any large-scale incident that impacts the public safety or the environment, if the organization experiencing the incident is not following FEMA's NIMS/ICS model properly.

Organizations should also look to the smart city initiatives of which they are a part. Some of the C/IMP vendors support this use case.

Using a C/IMP that automates the use of such frameworks can help keep an organization in good standing and in control of their part of an event. Organizations should determine the national emergency/incident response management frameworks and smart city initiatives that their organization's C/IM program must comply with or align to when managing crisis events.

Today, Gartner rates the use of C/IMP as having a high benefit to organizations, a market penetration rate of 5% to 20% and early mainstream in adoption. We predict that the C/IMP market will come into mainstream usage within five years.

Market Analysis

A C/IM program helps organizations manage the following actions taken in response to a critical event or disaster that interrupts the delivery of goods and services:

- Improve the organization's ability to protect public safety and to restore business services as quickly as possible
- Improve the efficiency of crisis/incident command and related emergency responses by continual communication and progress assessment when responding to a disaster
- Ensure the recovery of expenses incurred during the disaster from liability and business interruption insurance policies
- Protect the reputation of the organization in the eyes of all stakeholders — employees, shareholders, customers, citizens, partners and suppliers, auditors, and regulators

In recent years, specialized C/IM software solutions originally designed for government agencies and utilities have been commercialized for the private enterprise. C/IMPs are used for the following specific purposes:

- Educate all emergency/crisis/incident management personnel on C/IM processes, procedures, forms, reports and so on
- Provide automated guidance in the usage of all C/IM forms that need to be submitted to national authorities
- Provide a records management system for crisis-related data, including the logging of all data creation, updating and deletion for event management analysis
- Manage relationships with all organization stakeholders (internal and external)

- Manage response and mobilization of resources, recovery and restoration actions for the crisis, incident or situation through task and workforce management
- Manage media communications, including national services and social media traffic
- Communicating information internally and externally, typically via emergency/mass notification services
- Provide postevent lesson-learned reviews of the crisis/incident for regulatory training, reporting and BCM process improvement efforts
- Provide role-based access management to enable user access to creation, editing and deletion of crisis-related data

Overall, using a system that imposes a standardized best practice model extends uniform managerial controls across the organization and with external stakeholders. It also reduces staff training time and ensures better integration with the broader internal and external community involved in recovering from a disaster. Fully integrated systems that guide business responders through the response process lead to a more streamlined response that government agencies can easily follow.

C/IMP Marketplace

C/IMPs are used by crisis, emergency, work safety, business operations and BCM managers, and other response and recovery professionals to manage the workforce, response equipment and key stakeholders to support any crisis response operation or business interruption. Many of the C/IMP vendors also support the information security/cybersecurity attack use case from an orchestration perspective. These solutions help guide the organization in a consistent response manner to minimize the impact to people's safety and the damage to the environment, and the disruption, and to return to normal operations as soon as possible.

C/IMP Critical Capabilities

To be classified as a C/IMP, the technology must have prebuilt, out-of-the-box functionality to support situational awareness and a common operating picture that follows the C/IM life cycle, including these steps:

- Plan and prepare response, recovery and restoration tasks to a crisis/incident
- Invoke a new incident, including the incident definition, impact and criticality
- Communicate with all stakeholders engaged in the crisis/incident (the list and scope of stakeholders is based on the impact of the crisis/incident)
- Coordinate and collaborate with all response, recovery and restoration personnel, including activating plans; tracking response, recovery and restoration task progress; viewing activity logs with all actions taken and decisions made; filtering, analyzing and acting on incoming information, ongoing incident status and reporting activities (over a timeline basis)
- Demobilize (close down) an incident after action reporting

Key critical capabilities include:

- Workflow to support the entire C/IM life cycle management, which include a guided crisis response capability, task reminders and so on
- Task management (task assignment and tracking), including support for multiple incidents occurring at the same time
- Document management, including response/recovery plans, photo repository, audio/visual files, maps, procedure manuals, contact lists and water data
- Workforce management and rostering

- Response equipment asset management, covering the procurement and scheduling of internal and external response equipment and support services
- Communication and collaboration, including a contacts repository, teleconferencing, white rooms, two-way emergency notification, and chat and support for varied communications resources, such as radio, TV, Internet, live cameras and sensors (e.g., traffic, sensitive buildings)
- Expense and financial management
- Map management and analysis, including GIS and geospatial support from sources such as Esri, Google Maps and other digital mapping tool integration
- Data management and analytics for overall incident management dashboarding, real-time situational analysis, operational event management and historical event analysis. Data sources can include public information sources and critical infrastructure information, including police, fire, emergency medical service (EMS), emergency operations centers, hospitals, distribution centers, public-safety answering points (PSAPs), schools, shelters, bridges, tunnels, roadways, government buildings, waterways and population statistics
- External information links, including external information integration (via RSS), media reporting, hazards alerting, weather alerting, medical management and utilities management
- Application integration, including enterprise directories, human resources systems, supplier management, emergency/mass notification services (EMNS), traffic management, environmental, health and safety (EH&S), IT asset management, BCM planning (BCMP) solutions for recovery plan activation, remote sensor integration and live video integration
- Visualization and color-coding of C/IM information, including dashboarding
- Mobile device app support with real-time task management and communication
- Postclosure follow-up activities, such as gap identification and management, lessons learned, and out-brief
- Information security and audit, including strong role-based access management, strong user authentication and audit logs of incidents managed, accompanied with all related tasks/activities performed by all stakeholders over the incident's life cycle
- Reporting capability including predefined reports, including NIMS/ICS forms, as well as ad hoc report generating capability and exporting of data for reporting and external management and government reporting
- Multichannel and application viewing to allow support for the entire C/IM life cycle, many data sources and multiple incident management
- Time/date-stamped log of all activities taken in response to the incident
- Templates for response/recovery plans, workflow, reports, forms and other collateral
- Planning for training/drill/exercise management

Nice-to-have features include:

- Response and recovery plan integration from BCMP solutions or office automation tools
- Social media analysis
- Media/press management, including logging media communication, creating media content, and creating, approving, publishing and viewing press releases

Optional features, or those that may be specific to a particular industry or C/IM task, include:

- Next-of-kin management
- Victim management
- Shelter management
- Volunteer management
- Pet management
- Elder management
- Mutual aid management
- Hazard spill and air release modeling
- American Red Cross integration
- Transportation management, including road, marine/waterway, train management
- Public works/construction integration

At this time in C/IMP evolution, the three most important distinguishing features are:

- **Mobile device app support:** C/IM takes place where the event occurs. Therefore, personnel need to perform and report on tasks in the field. Therefore, mobile devices are the tool of choice for emergency and recovery staff members.
- **Real-time analytics:** Every crisis/incident is unique and emergency and recovery teams are working with limited information in the early stages of the event. Therefore, having as much data as possible to manage the crisis/incident is a great desire. As a result, lots of data integration points are a requirement in a C/IMP with the ability to manage and make sense of the data for effective decision-making is of utmost importance.
- **SaaS/cloud:** Leveraging the development and operational aspects of a SaaS/Cloud solution are leading capabilities of a C/IMP. In addition, having the solution running in a data center that is outside of the impact area is a benefit from the implementation and operational aspects of an IT solution — if your data center is the cause of the outage, or if you are the object of a targeted cyberattack, your C/IMP solution may not be available to you.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Table 2 lists vendors that deliver a C/IMP solution.

Table 2. Representative List of C/IMP Vendors

Vendor	Headquarters	Product Name
4C Strategies	Sweden	Incident and Crisis Management Suite
Access Intelligence	U.K.	Virtual Incident Manager
Alitek	U.S.	Prepare Respond
Badger Software	U.K.	Clio Manager
Crisis Commander	Sweden	Crisis Commander Connect
eBRP	Canada	CommandCentre
Global AlertLink	U.S.	Crisis Management
Grey Wall Software	U.S.	Veoci
IBM	U.S.	IBM Emergency Management Center
IDV Solutions	U.S.	Visual Command Center
Intermedix	U.S.	WebEOC
IntraPoint	U.S.	Crisis Manager/Operations Manager
Ixtrom Group	Canada	Emergency Management and Response
Knowledge Center	U.S.	Knowledge Center Incident Command System
MissionMode	U.S.	Situation Center
NC4	U.S.	E Team/E-SPONDER
Noggin	Australia	Incident Manager
Prepared Response	U.S.	Rapid Responder
Previstar	U.S.	Incident Manager
Response Group	U.S.	Crisis Management Software
Siemens	Switzerland	Incident Management System
VirtualAgility	U.S.	WorkCenter
Witt O'Brien's	U.S.	CommandPro

Source: Gartner (December 2015)

Market Recommendations

Organizations should define their C/IMP capabilities across the seven C/IM disciplines that they need. Be sure to include the national emergency/incident response management frameworks and smart city initiatives that your organization's C/IMP solution must comply with or align to when managing crisis events.

Based on these C/IMP requirements, determine which C/IMP is right for your organization. If you are already using a BCMP, BPM-platform-based case management frameworks or EH&S solution, its C/IMP capabilities may be "good enough" for your needs.

A SaaS/cloud solution is the recommended delivery model so that in the face of a targeted cyberattack, you will have external communications and C/IM management capabilities.

Evidence

Cumulative Gartner ITScore for BCM results from September 2010 through June 2015 were used for the data reporting in Figure 3 and Table 1.

Results from the 2015 Gartner Security and Risk Management Survey were used for the data reporting in Figure 4. Gartner surveyed organizations in seven countries between 25 February 2015 and 2 April 2015 to help Gartner understand how risk management planning, operations, budgeting and buying are performed, especially in areas such as risk and security management, security technologies and identity and access management (IAM), business continuity management, audit and compliance, and privacy. In all, 964 respondents participated in the U.S. (n = 153), Canada (n = 151), U.K. (n = 152), Germany (n = 151), India (n = 152), Australia (n = 53) and Brazil (n = 152). Country and security and risk management discipline area quotas were established to enable the comparison and contrasting of key trends. Organizations from all industries qualified. Qualifying organizations were large organizations with at least $50 million USD equivalent in total annual revenue for fiscal year 2014 and a minimum of 100 employees. Qualified participants must report being extremely involved in one of five risk and security management disciplines, or be a team member in at least two of five areas. Interviews were conducted online and in the native language (English, German or Portuguese). The sample universe was drawn from external panels of IT and business professionals. The survey was developed collaboratively by a team of Gartner analysts who follow these IT markets and was reviewed, tested and administered by Gartner's Research Data Analytics team.

Note 1
When Does a Business Disruption Escalate to a Crisis/Incident?

A business disruption escalates to a crisis/incident that needs to be managed when it can no longer be handled by standard operating procedures, or threatens the reputation or viability of the organization. Examples of such events include earthquakes, power outages, transportation delays, product failures, market shifts, adverse management activity, workplace violence, fires, floods, collapsing bridges, severe weather conditions, terrorist attacks, chemical spills and accidental discharges.

It should be noted that the term "incident" is specific to both the U.S. FEMA NIMS and a security breach that threatens the normal operations of the organization. Information security events are usually handled by a specialized team under the chief information security officer (CISO), but may turn into a larger incident that can impact business operations to the point that a disaster is declared. In those cases, the computer/cyber incident response management would transition to the broader C/IM team.

Note 2
The Common Services That Support the Overall Crisis/Incident Management Technology Ecosystem

Common services that support the overall C/IM technology ecosystem include location-based services, video streaming, mitigation and cleanup procurement, hazard risk analysis, and others.

Source: Gartner RAS Core Research Note G00274941, Roberta J. Witty 28 December 2015

Contact Us

For more information:

www.alitek.com
www.prepareerespond.com

Alexander Flenner

Principal | Alitek
Phone: 713-446-5197
Email: aflenner@alitek.com

Peter Kaleda

Partner | Alitek
Phone: 832-628-9840
Email: pkaleda@alitek.com