The Hidden Cost of Business Interruptions:

How Total IT Incident Management Can Save Your Business

everbridge

The Hidden Cost of Business Interruptions:

How Total IT Incident Management Can Save Your Business

Total Incident Management

Total incident management is vital for any organization that wants to control the total cost of a critical IT interruption. IT incidents can range in scale, but in many cases, are like icebergs. The tip of the iceberg, what you see, is only a small part of what's actually there; when a ship crashes into an iceberg, it’s the hidden part that can sink the ship. Likewise, when an incident occurs, it’s often the hidden costs that sink an organization.

All IT incidents carry the cost of the resources – people and otherwise – needed to fix them. If the response process is poorly designed and/or executed, additional time and money is spent as the time-to-repair is extended. Costs can also include loss of revenue if business transactions are halted, as well as the cost of actual assets and resources lost, damaged, or destroyed. But beyond these basic costs, incidents can also have far reaching impacts that organizations don’t anticipate, like decreased client satisfaction or compliance issues. In extreme cases, these unexpected costs — legal liability, for example – can be so great that they singlehandedly bring down an organization.

In all cases, failure to take accountability for the incident and failure to communicate with affected individuals throughout an incident’s lifecycle can cause long-lasting damage to an organization and its stakeholders. Both the expected and unexpected costs of an incident will increase if an organization cannot respond to the event appropriately.

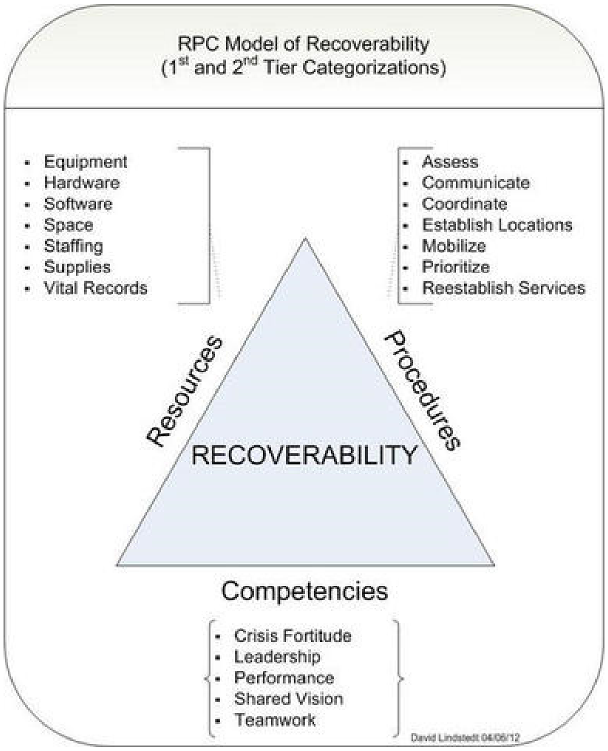
In this paper, we’ll explain how to understand the total cost of incidents, how “hidden” costs can impact your business, and how total incident management can help you both prepare for and better manage IT incidents in the future.

Understanding the Total Cost of Incidents

It is easy to imagine that incidents may have a financial impact on your organization. What's far more challenging — but crucial to incident management investment and preparation — is calculating the actual scope of that impact.

That's why readiness and recovery experts have developed various models to examine both the immediate and long-term effects of incidents. These models help organizations understand how incidents and crises impact organizations, their work teams, and other stakeholders.

In addition, an incident's immediate financial impact, for example, organizations must also consider the cost of recovery. Dr. David Lindstedt's "Resources, Procedures, and Competencies (RPC) Model of Organizational Recoverability" illustrates this point.[1]



The Lindstedt RPC Model describes three elements that are needed to recover from loss (either physical or human):

- **Resources**, or physical assets necessary to provide service
- **Procedures**, required to recover and restore services
- **Competencies**, which allow individuals to function throughout recovery

[1] Lindstedt, David. "Measuring Preparedness and Predicting Recoverability." Readiness Analytics Version 1.0, Revision 3, October, 2012: www.readinessanalytics.com. 15 Aug 2013.

Consider, for example, a significant IT incident like a data breach. The cost of a data breach includes the cost of resources spent identifying and containing the source of leaked data. If the incident stems from the theft or loss of digital media – like devices, hard drives, or computers – the cost of replacement items, must be counted into the cost of the incident as well. These costs can be significant; Ponemon Institute's *2013 Cost of Data Breach Study: Global Analysis* reported that the total cost per data breach incident in the United States was $5.4 million in 2012.[2] In this case, preventative measures, such as investments in security, can reduce both the likelihood of a data breach occurring, as well as the length of time necessary to contain an event that does occur.

A data center outage can also be costly. Ponemon Institute found that the average duration of data center outages for global organizations was 91 minutes between 2010 and 2012.[3] The duration correlates to the average organization's lack of resources and planning — only 38 percent of study participants agreed that they have enough resources to keep their data centers running if an unplanned event occurs. Understanding the cost of resources that would be needed to maintain continuity, compared to the cost of recovering from an outage that does occur, can guide smart upfront investments that help prevent these incidents from occurring.

In both of these cases, proper planning and an understanding of the resources needed to recover can help reduce the duration, and resulting costs, of the incidents themselves. But in both of these examples, direct costs of loss and recovery aren't the only costs to consider. Both data breaches and data center outages can have a negative impact on a company's ability to service their customers, and incidents can damage company brand, consumer trust, and profitability.

How an organization manages a data breach, data center outage, or any other incident or crisis can be a major factor in the extent of this second category of costs. How does an organization resolve the issue at hand? Can the organization communicate with affected individuals until the incident is fully resolved? Does the organization take responsibility for the problem and proactively seek answers? Or does the organization shy away from the issue entirely, leaving stakeholders to resolve the problem on their own?

[2] "2013 Cost of Data Breach Study: Global Analysis." Ponemon Institute, May 2013: www.symantec.com. 8 Jan. 2014.
[3] "2013 Study on Data Center Outages." Ponemon Institute, Sept. 2013: www.symantec.com. 9 Jan. 2014.

Throughout an incident's lifecycle, communication breakdowns can cause panic and misinformation, resulting in longer-lasting damage to an organization and its stakeholders. To avoid further damage, a proactive approach is crucial. Without a total incident management plan in place, an organization will struggle to resolve the incident while it is happening or prevent it from happening in the first place — and calls into question its regard for life and property. But the converse is also true. When an organization informs and instructs affected individuals on how to manage an incident, it shows that it places a high value on providing outstanding support when it matters most.

Prepare for the Unexpected Costs of Incidents

What are the unexpected costs of an incident? They are the not-so-obvious consequences of a purchase, event or action. The Library of Economics and Liberty classifies unexpected costs under “Cost-Benefit Analysis,” and defines them as the unintended consequences of an action or event.[4]

The unexpected costs of an incident affect an organization in several ways, including:

- Brand
- Customer Service
- Efficiency
- Paperwork
- Productivity
- Reputation
- Supervision
- Training

Unexpected costs typically extend beyond an organization's bottom line and may take a course that has or has not been well researched. As a result, the "effects" of these costs may not "affect" everyone the same way. Don Boudreaux, Professor of Economics at George Mason University, describes an important corollary with unintended consequences as: "***intentions*** are not ***results****.*"[5] The *intention* of many organizations is to maximize their profits and minimize the expenditures for stakeholders. But when an incident occurs, if the response is poorly designed and implemented, the *result* is damage to these stakeholders, along with the organization's bottom line, and its reputation.

[4] "Cost-Benefit Analysis." Library of Economics and Liberty, 2012: www.econlib.org. 9 Jan. 2014.
[5] "Unintended Consequences." LearnLiberty, 29 June 2011: www.learnliberty.org. 9 Jan. 2014.

Consider how your stakeholders view your organization's ability to manage an incident. Would they say your organization has done its due diligence in planning for several possible incident scenarios? If not, you could face numerous unexpected costs, including litigation fees, productivity slowdowns, and trust issues.

Canada defines due diligence as: "reasonable care to protect the health and safety of their workers." Failure to do so can have serious consequences. In Alberta, for example, the penalty for a first offense can be up to six months in jail and $500,000 in fines. These penalties double for second or subsequent offenses.

The need for due diligence and a total incident management plan was vividly on display during a recent Amazon.com outage. On August 25, 2013, Amazon's homepage was down for at least 45 minutes.[6] The outage affected all of Amazon's U.S. and Canadian customers. Amazon-owned websites such as Diapers.com and Zappos.com were also inaccessible to customers — all of which combined likely cost Amazon millions of dollars in sales. During the downtime, Amazon apologized to visitors who tried to access its homepage. But Amazon did not explain the source of the outage — potentially hurting its reputation even more and losing future business — or how it was trying to fix the problem. Instead, it merely offered tips to help visitors troubleshoot and resolve the issue on their own.

On the other hand, a well-prepared and executed total incident management plan can have the opposite effect. It enables an organization to control an incident (and gain customer goodwill) rather than have the incident control it (and lose goodwill). Consider Yahoo's response to a recent IT outage. On December 9, 2013, Yahoo Mail stopped working due to a hardware problem at one of Yahoo's mail data centers.[7] The IT outage affected thousands of Yahoo Mail users worldwide who could not access their email accounts for several days. For Yahoo, communication with affected individuals was paramount, and the company provided frequent Twitter updates until the issue was fully resolved. In addition, Yahoo CEO Marissa Mayer publicly apologized for the IT outage, and accepted full responsibility for the incident. She explained how the outage occurred and what her organization would do to prevent it from happening again.

The ability to effectively manage an incident impacts both the event's expected and unexpected costs. By devoting the necessary resources to incident management, and accounting for the total cost of incidents, an organization can control an incident throughout its lifecycle.

[6] Tweney, Dylan. "Amazon's website goes down for 40 minutes, costing the company $5 million." VentureBeat, 19 Aug. 2013: venturebeat.com. 23 Dec. 2013.

[7] Mayer, Melissa. "An Update on Yahoo Mail." Yahoo, 13 Dec. 2013: yahoo.com. 19 Dec. 2013.

It can be hard to measure the cost of brand damage and lost revenue, but in some cases, the hidden costs of IT incidents, while unexpected, can be very real and very quantifiable. In May 2014, New York-Presbyterian Hospital (NYP) and Columbia University Medical Center (CU) together agreed to pay a record-breaking $4.8 million to settle alleged HIPAA violations after the electronic protected health information of 6,800 patients wound up on Google in 2010[8].

In another example, Knight Capital Group, a global financial services firm, lost $457.6 million due to a computer error that occurred on August 1, 2012.[9] A software malfunction caused this company, one of the largest traders of U.S. shares by volume, to submit numerous erroneous orders for equity exchanges. Not only did the incident impact the prices of various securities listed on the New York Stock Exchange, but it also pushed Knight Capital to the brink of bankruptcy as the company's shares plunged 75 percent in the two days following the incident.

Knight Capital also suffered a massive power outage after a backup generator failed during Hurricane Sandy.[10] The outage shut down Knight Capital's equities trading on Halloween. Due to the outage, company officials were forced to ask customers to seek trading alternatives until the issue was resolved the next day.

In each of these incidents, the “hidden” costs far outweighed the expected costs of resolving the incident. The expected costs — like all costs — hurt the affected organization's bottom line. But the unexpected costs — the brand or reputational damage, litigation costs, lost productivity, and loss of trust — stretched far beyond an organization's control, impacting organizations and their constituents.

The ability to control an incident and its unintended consequences is key. While an organization may implement systems to control the expected costs of an incident, understanding an event's total costs allows an organization to accelerate and improve its incident management efforts. The ROI of successful incident management is clear — with a total incident management plan in place, an organization can prevent long-term harm to its brand, reputation, profits and stakeholders.

[8] Walsh, Beth. “$4.8M HIPAA fine sets new record.” Clinical Innovation+Technology, 7 May 2014. clinical-innovation.com. 12 May 2014.

[9] Mehta, Nina and Saijel Kishan. "Knight Asks Clients to Send Orders Again as Power Fixed." Bloomberg, 1 Nov. 2012: www.bloomberg.com. 9 Jan. 2014.

[10] McCrank, John and Jessica Toonkel. "Power outage hit Knight Capital, cuts off trading." Reuters, 31 Oct. 2012: www.reuters.com. 9 Jan. 2014.

Total IT Incident Management

Community Priorities		Corporate Priorities
1	Health and Safety	7
2	Natural Environment	6
3	Social Environment	5
4	Cultural Environment	4
5	Technical Considerations	3
6	Financial Considerations	2
7	Economic Considerations	1

The total (expected + unexpected) costs of an incident must be managed before, during, and after the event. With the ability to control total costs, an organization can increase its total savings.

Globally recognized incident preparedness counselor James Lukaszewski built a priority model that studies the results of failing to protect and enhance corporate trust and prolonging the agony of crisis victims. He pointed out that an inherent conflict exists between corporate and community priorities and suggested that an organization must ***immediately*** adopt the community's priorities during incidents.[11]

In addition to managing incident response, a key part of managing both expected and hidden costs is managing the communication surrounding an incident. When an incident does arise, you need to ensure that the right experts are engaged as quickly as possible and are communicating with the most up-to-date information. Faster awareness of and response to IT problems, and faster collaboration to identify the source and solution for problems, ultimately leads to faster resolution of incidents.

[11] Lukaszewski, James E. "Strengthening Corporate Trust In Times of Crisis (Part 1)." Ethikos, June 2009: www.e911.com. 9 Jan. 2014.

Clear communication strategies for customers, stakeholders, and the public can also help organizations maintain trust and minimize brand damage as the result of an incident. In a *2012 Global Reputational Risk and IT Study* by IBM, researchers found that 64 percent of companies stated that they are focused on improving their reputations.[12] Meanwhile, 75 percent of firms noted that they recently increased their IT budgets as part of their efforts to counter damage to their reputations. "Underestimating the cost of reputational [risks] substantially exceeds the cost of protection," said one IT manager of a U.S. energy and utility company. "Being proactive is preferable to being reactive."

The IBM study also highlighted the role of social media for organizations, and showed that digital tools are important for organizations that want to reduce risk and increase ROI. Quickly identifying and correcting social media rumors or threats is essential, especially during incidents and crises.

"The [social media] community is talking about you whether you participate or not, and you have to decide what kind of positioning you're going to take," said David Boroevich, Vice President of Marketing at Canada's Alpha Technologies. "Otherwise, people will do it for you."

[12] "Insights from the 2012 Global Reputational Risk and IT Study." IBM, 2012: http://www.ibm.com. 9 Jan. 2014.

Recommendations

An organization that wants to manage the total cost of an incident must manage the confusion and tension that cause the hidden costs of an incident to rise. There are four key areas that determine an organization's ability to manage an incident, and its expected and unexpected costs: preparation and planning, assessment, response, and delivery. Organizations can use the following checklists as a starting point for assessing preparedness in each area:

Preparation and planning

- √ Are procedures in place to communicate with clients, employees, families, first responders, media representatives, and other stakeholders before, during and after an incident?
- √ Is there a documented plan in place to protect your business, clients, and employees before, during, and after an incident?
- √ Is there a communication plan for numerous scenarios and each stage of an incident?
- √ Is there redundant technology in place for warning and alerting clients, employees, and other stakeholders?
- √ Are there message templates that cover potential incidents and contain clear, actionable messages?
- √ Is there a documented training and testing plan in place?

Assessment

- √ Are communication plan and incident procedures tutorials provided to clients, employees, and other stakeholders?
- √ Do you have a complete list of stakeholders to contact and multiple devices to use for communications?
- √ Are you able to initiate incident management system communications and receive responses using a mobile device that will work if power is lost?
- √ How long does it typically take to notify all of your stakeholders after an incident is reported? Is that time within acceptable levels?
- √ Is there an incident management system in place that will operate redundantly from a remote location? Could communications still be delivered if the primary location was damaged or compromised?

Response

- √ During an incident, what contact methods would be used to get messages to stakeholders, employees, and other stakeholders? Can you ensure that key contacts can be reached quickly, at all times?
- √ Which audiences would receive communications during an incident? Can you confirm that the resources needed to fix the problem have received the message, and are working on the issue?
- √ When you notify recipients of an incident, can you capture responses and information such as status, location, and photos in response?
- √ How are external and internal sources of information leveraged during an event to guide decision-making? Is third-party data being leveraged to guide decision-making?
- √ Is there a plan and procedure for automatically escalating notifications if there is no response from the primary contact(s)?
- √ Can you easily communicate with other parties in your region?

Delivery

- √ Have you established methods for assessing the overall effectiveness of your communication processes and systems after an event?
- √ Do you have a process to test or exercise your plans, maintain stakeholder awareness, and continuously improve message delivery rates?
- √ What steps can executives take to improve incident management and communication procedures?
- √ Is there a clear plan for reviewing after action reports and tuning your communication plan based on the results?

To effectively manage an incident and reduce its expected and unexpected costs, an organization must implement an incident management plan that accounts for the total cost of an event. In addition, it is crucial for an organization to understand the hidden savings of incident management. Examining the costs of incidents, and the savings provided by total incident management, ensures an organization can maintain or increase its profitability and the trust of its constituents — regardless of the incident.

About Everbridge

Everbridge provides a unified critical communication suite that helps clients be better prepared, make better decisions, and respond quickly and confidently during disruptive events. When an incident happens, whether it’s a natural disaster or an IT service outage, we automate communications to ensure that the right messages get to the right people at the right time.

Widely recognized by analysts as the market leader, Everbridge solutions are trusted by clients in all major industries and government sectors to connect with over 50 million people around the world.

THE ONLY END-TO-END PLATFORM

- **Planning**: Everbridge is easy to set up, maintain, and organize, meaning that you’re always ready for a quick, coordinated response. Everbridge ensures that the right messages get to the right people - with the most advanced opt-in portal on the market, streamlined integration with internal and external data sources, and simple group and contact management.

- **Assessment**: When trouble strikes, you need rich insight, presented simply - so you can quickly assess potential impact and make an informed decision to avoid loss. Everbridge offers the only solution on the market that meets these demanding requirements, with the most advanced interactive dashboard in the industry.

- **Response**: In critical situations, ease-of-use can mean the difference between an effective response and a mistake that carries serious consequences. Everbridge is engineered to be simple to use under pressure, with a user interface that accelerates time-to-message and reduces the likelihood of errors.

- **Delivery**: Even during large-scale disruptions, Everbridge stays on. The most advanced platform in the industry ensures that you reach your contacts - every time. And with worldwide coverage and capabilities, including globally local calling infrastructure and data storage, we’re ready to support you wherever your people are in the world.

Visit www.everbridge.com to learn more.