



Don't Panic. Respond.

Forming an Incident Management Plan

- *One morning, the CIO arrives at work to find that no customers, employees, or vendors can reach the corporate web servers. The Help Desk is reporting that access to the Internet has slowed to a crawl. What's going on?*
- *A miscommunication with your company's bank prevented the employee payroll from being processed. Over 6,000 employees did not get paid as expected. Many of the employees in the field are upset and are calling the headquarter offices to find out what is going to be done. Well, what is going to be done?*
- *A previously unknown single point of failure in the data center cooling system, believed to be thoroughly redundant, has failed. The temperature of the data center is quickly rising. If the problem cannot be quickly fixed, several systems in the data center will have to be turned off to prevent a catastrophic loss of data. Who should you call?*

All of these scenarios are not only possible, they have actually occurred. The "Code Red" worm brought the Internet traffic of many companies to a halt in 2002. A corrupt file or missing instruction is all that is needed for a payroll authorization to fail. A single valve separating two chillers on a data center cooling system can fail and bring cause the data center to shut down. Knowing in advance how these situations or those like them will be addressed is a matter of thoughtful preparation. If you are not prepared in advance, your reaction is likely to be panic: ineffective, slow and expensive. If you have prepared in advance, your reaction is one of response and recovery.

We Have a Disaster Recovery Plan, Isn't That Enough?

Having an Incident Response Plan is often neglected or is lacking in many companies. Those companies that have a Disaster Recovery Plan or a Business Continuity Plan believe that those plans are sufficient and would likely address these types of events. However, all of the listed events are examples of scenarios that, in their current state, are short of a “disaster” and are not likely to trigger the activation of any of those plans. An interim plan is necessary. Those companies that do not yet have a Disaster Recovery Plan can use an Incident Response Plan as the foundation for their DR plan.

What Does an “Incident” Look Like?

An incident is any event that disrupts normal business activity to a significant degree and for a significant period of time. The definition of what “significant” is will vary by company and the type of incident. During an incident, business activity is likely to continue in a reduced or impacted state in contrast to a disaster when business activity is likely to be interrupted or stopped entirely. Each of the incidents above impacted the business to a significant degree, but the day-to-day business continued in each case. Something that can be resolved by a single phone call or impacts a relatively small number of people is not likely to be an incident.

Once preparation is complete and an incident actually occurs, it is likely to flow through several phases. Knowing what phase an incident is in is a key to resolving it quickly. The Incident Management Plan should detail what action will be taken within each phase.

- •Phase I: **Detection, Discovery, or Awareness** of the problem at the very beginning of any incident is the first phase. It is imperative to gather as many facts as possible to determine the magnitude of the problem: What people or systems are affected? What is the impact to customers? How long has the problem been occurring?

- Phase II: **Control and Containment** of damage to the company is the next step. Efforts should focus on keeping the problem from spreading to other systems or causing additional damage. This may involve nothing more than communication to various constituencies or could involve deploying resources to take specific action. Deploying a work-around solution is one way to control the problem.
- Phase III: **Correcting** the root cause of the problem and providing a permanent solution is the only path to concluding any incident. In this phase, the problem is fixed by patching systems, implementing new systems, putting new people in place, etc.
- Phase IV: **Restoration** is the activity necessary to bring the company back into full service and to resume regular operations. During the incident, systems may have been bypassed, temporary services implemented, etc. Efforts are undertaken to begin the “stand-down” of the Incident Management Team and re-establish normal business activity.
- Phase V: **Lessons Learned** from every incident should be documented and used to improve future responses. This step is often forgotten but is important to improve the plan and ensure that similar problems that reoccur do not have the same impact. Wait a few days after the incident has been concluded before gathering everyone together for this review.

Why Does a Company Need an Incident Management Plan?

How a company reacts during an incident can have dramatic results to the bottom line of the business as well results in the community to the reputation of the business. By having a plan of any sort in place, the time necessary to address an issue is lessened and, in turn, reduces the cost of correcting any damage that has resulted. The image of the company by the public is also likely to suffer less

damage if the company responds to an incident in a calm and effective manner. Some incidents actually require a specific, legal response that can cause significant penalties, including financial penalties, if they are not handled correctly. During a crisis, details can be lost and specific actions to take in an emergency can be forgotten. Having a plan in place which delineates responsibilities and specific tasks to address within a plan ensures that these items will be addressed and not forgotten in the heat of an incident.

What Would a Good Incident Management Plan Contain?

The key to success is to have a plan in place that is:

- Supported and utilized by executive management within the organization
- Sufficiently broad to address a wide variety of scenarios (such as the ones listed above)
- Flexible to address a wide variety of likely or probable scenarios with one plan
- Specific enough that it provides a framework for specific action to be taken
- Addresses a wide variety of likely or probably scenarios
- Informative to a point that it contains the information needed in a central location
- Structured to allow situational assessment, decision making and execution at the same time
- Empowered for decision making within a single incident management team with the authority to carry out actions needed to solve the problem
- Inclusive of a communication plan to keep internal and external constituencies informed throughout the incident
- Sufficient to progress through all phases of an incident from the realization that an incident has occurred to resumption of normal operations

- Rehearsed in advance of an incident and corrected as much as possible in preparation for the incident

Who Is on the Incident Management Team?

The team is comprised of one leader who is ultimately responsible for the team and making the final decisions for the team. They will lead the team throughout the incident. Additionally the team will be comprised of multiple cross functional/cross country team members. Representation on the Incident Management Team will vary according to the type of incident. For example, some incidents will require that the Legal Department be informed but not involved throughout the incident. In other scenarios, the involvement of the Legal Department could be required every step of the way. Any Incident Management Plan, however, should always have several departments involved and available to participate in the management of any incident. Organizational areas to consider in forming the team would include:

- Information Technology
- Human Resources
- Legal
- Public Relations
- Investor Relations
- Information Security
- Risk Management

Smaller companies that may not have staff in each of these areas should consider representation from their outside representatives on the team. For example, if Risk Management is provided by a company's insurance carrier or agent, the carrier should be briefed on the plan and their participation confirmed in advance of any incident.

Sidebar: Lessons from the Trenches - Incident Management

1. Assemble the team in advance; know the people you will rely on for performing in an emergency.
2. Remember to include administrative support for gathering office supplies, ordering meals, and taking notes through an incident.
3. Split into more than one team; one group manages the incident and makes decisions, the other group follows their direction, provides information, and fixes the problem.
4. For incidents that continue for many hours, plan to rotate the team members in and out of the incident to allow for fresh minds and fresh bodies throughout.
5. Designate a single person with ultimate responsibility for managing the incident within the Incident Management Team. While the team is there to provide assistance, advice, and input, effective incident decisions cannot be made by committee.
6. Give the Incident Management Team the authority to carry out activities necessary to address the incident and deploy resources as needed.
7. A strong communications plan is vital in successfully managing any incident. One person should speak officially for the team. Keeping customers, employees, investors, and executives informed on the status of the incident and resolving it actually will reduce the efforts of the Incident Management Team.
8. Manage an incident from a single, central location (e.g. a conference room) that provides enough room and resources for the team to carry out their responsibilities.
9. Leave titles and status at the door. The team is managing the incident and a VP may need to take direction from a manager during the incident.
10. Revisit the incident after it is resolved to gain valuable lessons learned for the next one.

About the Author: *Pat Hellman, Arrow Partner*

Patrick has over 20 years experience in Information Technology in both the public and private sectors in a variety of senior IT positions most recently as CIO of Mercury Companies. He has also held senior management positions at JD Edwards, PeopleSoft, and the University of Colorado Health Sciences Center. He has an extensive background in systems operations, business process development, strategic planning, information security, compliance and auditing. Patrick has taught graduate level classes in telecommunications and strategic planning and is a frequent public speaker to various organizations regarding information security and IT business systems. Patrick holds CISSP (Certified Information System Security Professional) and CISA (Certified Information Systems Auditor) certifications.