



# Corporate Incident Response

Why You Can't Afford to Ignore It

Whether your company needs to comply with new legislation, defend against financial loss, protect its corporate reputation — or a combination of the three — it is crucial that you have a comprehensive incident response plan. This paper explains the need for an effective corporate incident response plan and highlights common problems associated with inadequate incident response. It also discusses the steps you need to take when creating a corporate incident response plan and serves as a general guide to the phases that should be included in a comprehensive plan. If your company does not have a mechanism in place to diagnose an incident and outline a remediation plan with speed and focus, your company is at a serious disadvantage. No organization can afford to have all the necessary security controls to prevent every possible incident, but if you have an incident response program in place, you will be able to respond quickly and minimize damage and downtime when attacks and exploits do occur.

## **What is Incident Response?**

There are no widely accepted incident response standards as yet, and there are many definitions of "incident response." In essence, these definitions all express the same idea: incident response is the set of actions taken once an adverse event has occurred that affects a company's assets or its network. Although every organization attempts to stay in

the "protect" stage of the security life cycle, most security practitioners will agree that, eventually, you end up in the "respond" stage at some point. If you don't, it is probably because you never got to the "detect" stage!

Nonetheless, many organizations neglect to plan for the response stage. There are many excuses for not planning for incident response. Some of these include:

- "We're not a target. Who would want to compromise my network?"
- "We can't be hacked. We have the best network defenses money can buy."
- "We meant to plan but never got around to it. We were always putting out fires."
- "We thought we would just figure it out when the time came."

Although it is possible to recover from an incident, without up-front planning it is much more difficult. Many critical pieces are probably not in place, including notification lists, log files, tools, training,

responsibility matrices, etc. Incident response by its nature, is a reactive process, and some companies do not understand the many steps that can be taken before an incident occurs to foster a more efficient and effective response.

*If your company does not have a mechanism in place to diagnose an incident and outline a remediation plan with speed and focus, your company is at a serious disadvantage.*

## Who Needs It?

To determine whether your company needs an incident response plan, ask yourself this question:

“Does my company have any assets worth protecting—any data, systems, services, or people?” Consider the following:

- Is your organization subject to compliance regulations?
- What if your corporate website was defaced? Would it be detrimental to your company's reputation?
- What if the power to a computer rack in your datacenter failed, and this rack contained the servers used to host critical applications?
- What if backup tapes containing confidential data were lost?

If you don't think your organization has sensitive information, think again. You do not have to look any farther than your human resources systems, which contain your employees' personal information. In general, the three factors that motivate companies to develop formal incident response plans are:

- Compliance
- Business continuity / financial impact
- Brand protection

## Compliance

Currently, there are at least twenty bills in Congress dealing with identity theft. The emerging

legislation requires due diligence<sup>1</sup> and incident notification. In the United States alone, companies reported that more than 9.6 million personal records were lost between February 2005 and

June 2005. This motivated Senate members enough to propose a law requiring businesses that sell personal data to be licensed by the government.<sup>2</sup> How can a company claim due diligence or compliance if they do not have the tools and process established to identify an incident when it happens and to conduct a thorough investigation? A properly designed incident response plan

promotes incident verification in a timely and organized manner. It provides the first responders and/or investigators with the tools, knowledge, and processes to act swiftly and accurately so that they can demonstrate due diligence. Any company that supports the national infrastructure or collects, stores, or processes personal data must pay particular attention to these new laws regulating the need for formal incident response plans.

## Business Continuity

Today's consumers demand twenty-four-hour access to online resources, seven days a week. If they cannot access your site when they want to,

<sup>1</sup> Due diligence is defined as the care that a prudent person might be expected to exercise in the examination and evaluation of risks affecting a business transaction.

<sup>2</sup> Gross, Grant (2005). Congress offers competing ideas on fighting ID theft. *ComputerWorld*, retrieved April 6, 2006, from <http://www.computerworld.com/printthis/2005/0,4814,102613,00.html>

they will go elsewhere for their needs. If you run an e-commerce or online banking site that conducts hundreds, possibly thousands of dollars worth of transactions per hour, you need an incident response team that is not only qualified, but also prepared.

Spending a few dollars up front to prepare for an incident will save you many times that amount in lost future revenue, both direct and indirect. In some cases, the lost productivity or negative effects on your reputation will have a higher impact

than the actual revenue lost due to service interruption, intellectual property loss, and fraud. Anyone who has dealt with a serious incident can tell you that by the time the incident occurs, it is too late to start thinking about what you should do. If proactive measures to develop, implement, and practice incident response are in place before an incident occurs, you can expect to have an organized and effective response resulting in reduced company loss.

## Reputation

A company's reputation is one of its key assets. Whether a company has direct competition or has a virtual monopoly on a market, business will suffer if its reputation becomes tarnished by a loss of customer data, a hacked website, unavailable services, or any revelation of misdeeds or carelessness with data protection. With every

second that passes during an incident, a company's window of exposure opens wider. As the window opens, so does the chance that there will be a negative impact on the company's reputation. An incident response plan that enables

a quick response is likely to resolve the issue before it becomes public knowledge. Also, it will create good communication channels within the organization to ensure that only authorized individuals release information to the public and that the communication plan is well planned.



## But We Already Have an Incident Response Plan

The sad truth is that once an incident occurs, many companies find out quickly that their incident response plan is ineffective. The major problems in the way corporations handle incidents are:

- Failure to escalate an incident in an appropriate manner
- Application of band-aids for individual issues, instead of implementation of comprehensive remediation plans
- Inaccurate estimates of resources required to fully remediate issues identified during and after an incident
- Roll-out of remediation plans before an accurate assessment of the incident is obtained

- Poorly defined roles and responsibilities resulting in lack of ownership of an incident
  - Lack of training and experience by staff in handling incidents
  - Lack of testing and dry runs
  - Failure to keep the plan up to date in a changing IT environment
  - Failure to cover all aspects of incident handling (PR, IT, Legal, HR, etc.)
3. The corporate help desk does not have a current and accurate notification and escalation process at their desks ready to use at any time.
  4. The security team has never been trained on proper data-gathering and evidence collection techniques.

### What is included in an Effective IR Plan?

No single incident response plan is going to work for every organization. Every company has a unique political and cultural environment, as well as different resources and security postures that will drive the incident response plan. For example, a large financial firm will most likely have a much different set of resources and stance on security than a manufacturing company. Both companies need an incident response plan, but their response plans will not and should not be identical. It is important to ensure that your company's specific needs are met with your incident response plan. If these requirements are not met, the plan will never be properly implemented, and it will end up collecting dust.

Although each company has a unique environment with unique needs and circumstances, the steps for creating an effective plan and the main components of that plan are essentially the same. The first step in creating a plan is to collect and review all current documentation that relates to incident response policy or procedures. This will

The lesson here is that if you already have an incident response plan in place, make sure it is effective before the next incident occurs. Determine what the top two threats are for your company and do a dry-run incident response exercise for each of them to see how your plans translate from theory to reality. This can be an effective way to make sure your company is truly prepared for the next incident.

*Determine what the top two threats are for your company and do a dry-run incident response exercise for each of them to see how your plans translate from theory to reality.*

### Am I Prepared?

You should now ask yourself whether your company is adequately prepared for an incident.

You are not ready if:

1. The first time your security team meets corporate council is during an incident.
2. Your end users have no idea who to contact if they suspect a security breach has occurred.

give you a general idea of how incidents have been handled in the past, or, at least, how they were supposed to have been handled. Current documentation may also contain several processes and steps that should be carried over into the incident response plan (along with some steps that should be omitted or modified in the new plan). Understanding your organization's history with incident response and taking that into account as you create the incident response plan is essential for getting the plan adopted by management and actually implemented. Also, a close look into the current legislation that affects your company will provide guidance and dictate the elements that need to be included in the plan. At the end of the day, shareholders and employees of the business want the plan to be successful.

Another important success factor is business unit buy-in of the incident response plan. Understanding information security in general and incident response specifically—from the business line manager's perspective—is crucial in making the plan palatable for the organization at large. This can usually be accomplished by setting up interviews with business line managers and discussing with them what really matters in their specific business unit. Once this is completed, a first version of the incident response plan can be written. This is just the first version, because this plan should be a dynamic document that changes with new business or technology needs. It should also be updated to reflect any gaps found in the process either through practice exercises or from real-world incident experiences.

Just as there is no standard definition for incident response, there is no standard for defining the steps involved in proper incident handling. There are many different versions of the incident response process. However, they all express the same concepts regardless of names or titles. A good response plan typically has four or more phases:

1. Preparation
2. Initial response
3. Investigation & Analysis
4. Follow-up

An incident response plan cannot be considered complete if it is missing any of the four major components mentioned here. Jumping into the middle of the response can often be more damaging than helpful. Figure 1 illustrates the phases and steps that comprise an effective incident response plan.

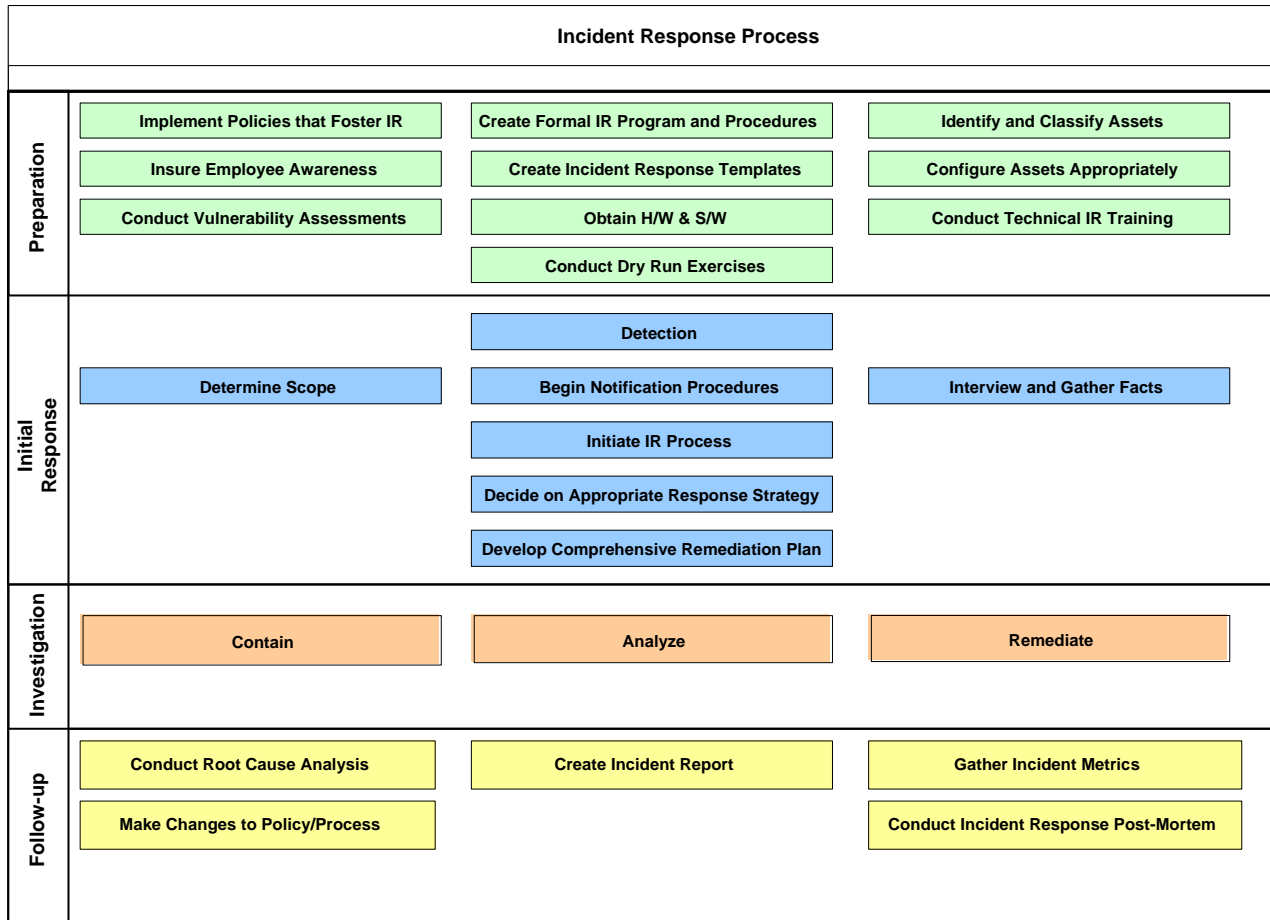


Figure 1 - Incident Response Process

As illustrated in Figure 1, there are several steps that can be taken to prepare for an incident long before it is detected. These steps include creating the actual incident response plan and making sure that all employees know the role they play. Also, ensuring that all hardware, software, and templates that may be needed during a response are purchased, licensed, and readily accessible saves valuable time once an incident is detected. Preparation also includes configuring all assets to allow for an audit trail, which fosters a proper and thorough investigation. Technical training should be completed by all responders for proper data-

gathering and analysis. Responders also need to learn how to present the data in a meaningful and succinct manner. In order to minimize the number and severity of incidents before they even occur, employee security awareness training should be conducted. Finally, network vulnerability assessments should be completed regularly. The initial response phase refers to all of the actions taken once an incident has been detected to prepare for the investigation phase. This is a crucial phase because it prevents knee-jerk reactions that may cause evidence destruction,

redundancy of work, and ineffective remediation steps.

This phase promotes taking the necessary time before diving into a response to notify the appropriate people, gather nontechnical data, and construct a strategic response and remediation plan that aligns with your corporate objectives.

The investigation phase is what most companies typically think of when they hear information security incident response. They have visions of their IT personnel imaging drives and using special software to read deleted files and e-mail. No matter what technical steps are necessary for an investigation, the key to this phase is making sure that all evidence is preserved and the processes used to obtain the data are clearly and completely documented. This is an exercise in meticulous note taking and organization.

In the follow-up phase, the company implements the strategic remediation plans devised during the initial response and investigation. Also, no response is complete without a report. This is the point at which the notes and details gathered during the investigation are transformed into a detailed report that delivers relevant data in a way that is meaningful to the intended audience, which include your legal department, internal audit, risk and regulatory compliance team, business units, and even the general public.

Also, it is important to conduct a post-mortem after each response, including a review of what worked and what did not work during the response. Analyzing the root cause of the incident and recommending changes in the process are

also extremely important steps that are often overlooked. Commonly, investigators and management move on to the next fire once the current incident has been resolved without capturing the lessons learned. This sets up the organization to repeat the same mistakes when future incidents occur.

## **Conclusion**

Most likely if your company needs to comply with new legislation, defend against financial loss, protect its corporate reputation — or any combination of the three — you cannot afford to be caught short without an incident response plan. If you have assets to protect, think of a proactive incident response plan as a form of insurance. By spending a few corporate dollars up front, you are likely to save precious time and resources when it really counts — during an incident.

## **About Foundstone Professional Services**

*Foundstone® Professional Services, a division of McAfee, Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.*