

How to Design a Useful Incident Response Policy

Timothy E. Wright 2001-10-02

How to Design a Useful Incident Response Policy

by *Timothy E. Wright*

last updated September 18, 2001

Perhaps you're the Information Security Officer for your company. Or, maybe you're a technology auditor. Maybe you're in charge of data security for your university's computing department. Regardless of your title and circumstances, you've been working on implementing an information security program (you have been working on your program, right?!) Such an endeavor has a tremendous scope, requiring great feats of perception and planning. This article aims to help you with an important facet of any information security program: the incident response policy.

Policy: Does Anybody Read This Stuff?

Policy: lifeblood of bureaucrats! But does anyone actually read policy? In truth, any properly constructed information security policy can perform several worthwhile services. First, it acts as an informed guide for your organization's information activities: good policy can help an organization manage its security risks better. Next, it brings structure to chaos: sensible rules and recommendations, tailored to your organization, can resolve confusion about handling information under different circumstances. Finally, it streamlines activities in the face of a security issue. If people know what to do and when to do it, they will be able to protect their organization through decisive and correct responses.

In addition to these pragmatic functions, there is, in fact, another benefit that good information security policy can perform. Good policy can demonstrate that an organization has thought through its information security needs, and has properly configured itself to meet these needs. In some instances, there may be a legal requirement for this! For example, the [Gramm-Leach-Bliley Act \(GLB\)](#) states very clearly that "...each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." (In fact, GLB requires that financial institutions document and implement a full-blown information security program.) In other situations, an organization may have to present a cogent information security program in order to conduct business.

Towards a Useful Policy

Having established the reasons for devising information security policies, we can now consider the elements of truly useful policy. Good information security policy should be succinct, understandable, practicable, cooperative, and dynamic. Let's consider each of these in turn.

Succinct

By succinct, we mean that the policy should be clear and concise. It should be stated as briefly as possible without omitting any vital information. Long winded policies are more difficult to understand, less likely to be read, and harder to implement.

Understandable

When we say a good policy is understandable we mean that the policy's text actually makes sense within the context of the organization. As the aphorism from the world of business an aphorism states, there are two types of people: those who don't manage what they understand, and those who don't understand what they manage.

In the realm of information security, sense can only be achieved if the person writing the policies has a grasp of information security concepts as well as their organization's structure and purpose.

Practicable

Regardless of how succinct and understandable a policy might be, if it isn't possible to practice it's worthless. A great example of this issue would be the implementation of a policy prohibiting the connection of modems to server machines in an organization that has a service contract in place whereby a software vendor must dial into a server to do maintenance. An example related to incident response might be a policy stating that members of a response team have to be reachable 24 hours a day, even though no reliable means of contact is provided by the company except when the members are at work. Policies that aren't practicable are not only, by definition, ineffective, they are also quickly ignored by an organization's employees.

Cooperative

A good information security policy is cooperative in that it is crafted and maintained with the input of all relevant departments within an organization. In general, information security can only succeed when everyone participates. Where incident response is concerned, departments such as Legal, Human Resources, Public Relations, Audit, and Information Technology all have to contribute to the creation and review of policy documentation. During an incident response it's very likely that some or all of these departments will play a significant role in the management of the situation. If relevant departments haven't given their endorsement for a policy, the policy is sure to experience problems during implementation.

Dynamic

Finally, any useful information security policy is dynamic in that it is capable of changing and growing with an organization. The rate at which technology changes is immense. And while organizations may or may not keep pace with this, they inevitably must make changes and minor course corrections as a result of the technologies they deploy. It would be negligent to create an information security policy and believe that the needs it serves today will be adequate in the long run.

Incident Response: Where the Rubber Meets the Road in the Information Security Program

Much of an organization's information security program is passive. Policies that prescribe how systems are to be used, passwords to be managed, and system audit activities to take place are all designed to prevent something bad from happening. In contrast, items like disaster recovery and incident response are entirely action oriented. In fact, in many ways, responding to an incident is similar to responding to a disaster: money, public relations, and time are all considerations. Of course, for incident response, the level of success is inversely proportional to the degree of public relations exposure.

No organization wants to appear as though they have a weak information security posture. Such an appearance can tarnish the corporate image, precipitate law suits, attract unwanted hacker attention, and damage good will. Yet, there is no such thing as fool-proof security: sooner or later, all organizations must respond to a security incident. The speed and decisiveness with which an organization can mount its response will determine whether or not a serious incident turns into a nightmare. If the response is methodical and well orchestrated, invariably the incident will be controllable.

A poor response capability equals financial and public relations trouble. How is this risk managed? By devising an effective incident response policy from the outset. Such a policy's documentation will consist of the following sections: background, definitions, incident classification, reporting, business continuity, process flow, and example incidents.

Background

All policies need to have a background section in order to explain the motivation and purpose driving the policy. For incident response the objective is somewhat obvious: to adequately respond to electronic incidents that take place within an organization's purview. This background not only identifies the objectives of the incident response policy, it provides the context within which those objectives will be met.

Definitions

Here, the policy will need to define exactly what an electronic incident is. Are we talking about computer fraud and computer abuse (the difference being that computer fraud is a crime whereas computer abuse is a policy violation)? What about incidents that are accidental on the part of the organization or a vendor? Does this type of activity warrant an incident response or something more low-key? Unfortunately, this article cannot answer these questions, since the answers will be contingent upon your organization's goals and priorities. A good tip, however, would be to carefully read through any regulations (e.g. GLB, FERPA, etc.) that apply to you and grasp the totality of what they are requiring.

Another item that requires definition is that of the Computer Emergency Response Team (CERT). An incident response policy won't be practicable unless there is someone who puts that policy into action during an incident. The CERT must be a highly skilled and available group. Members should represent expertise within the various information systems belonging to an organization, be on call twenty-four hours a day, and be capable of responding within a nominal amount of time. There should be backup available for when members are out of town or on vacation. Members of the CERT need to be familiar with the [fundamentals of gathering and handling computer evidence](#).

Incident Classification

To be effective in managing its incident response process, an organization should create an

event classification system. Such a system will enable the filtering of background noise from items that are more serious: for example, does an organization really need to respond to every port scan. One effective approach is to assign events a degree of urgency and then further assign a priority ranking to anything of high urgency. Incidents that fall into the low and medium urgency classes may be logged, with medium events being examined later on by a system administrator. High urgency events would be treated immediately. This response would require the attention of other relevant departments and groups.

An escalation list should be used for all incidents. Such a list designates responsibilities for incidents in which the degree of urgency increases as the incident progresses. As an event increases in urgency and priority, an appropriate individual further up the escalation list is contacted. Ultimately, for incidents of the highest urgency and priority, the CERT is activated.

As an incident escalates, it is likely that departments other than network administration will need to become involved. Executive management will have to be very careful to not hamper the CERT's ability to do its job (e.g. by assigning it unreasonable or time consuming chores). The Legal and Public Relations departments may also need to become involved. If the situation warrants it, executive management should be prepared to contact law enforcement.

Note that an organization's information system vendors should be included on the escalation list. In particular, relevant vendors should provide a twenty-four hour contact and be given such a contact at the organization. It is also recommended that some type of information security service level agreement be included in any contract between an organization and its vendors.

Reporting

Before, during, and after an electronic incident, various kinds of data will be gathered. How will these data be processed, and to whom will they be presented? Very little beyond intrusion detection system and server audit logs will be available for reporting during normal business operations. However, when an incident is being managed there is a great potential for additional information. For example evidence that might be collected, additional log data, and documentation of the incident can all contribute to the data available. After an incident has passed there will no doubt be new information pertaining to the aftermath: what the incident has cost the organization, what resources will be needed to fully recover, etc. It's important for the incident response policy to outline when reports are generated, what they will contain, and

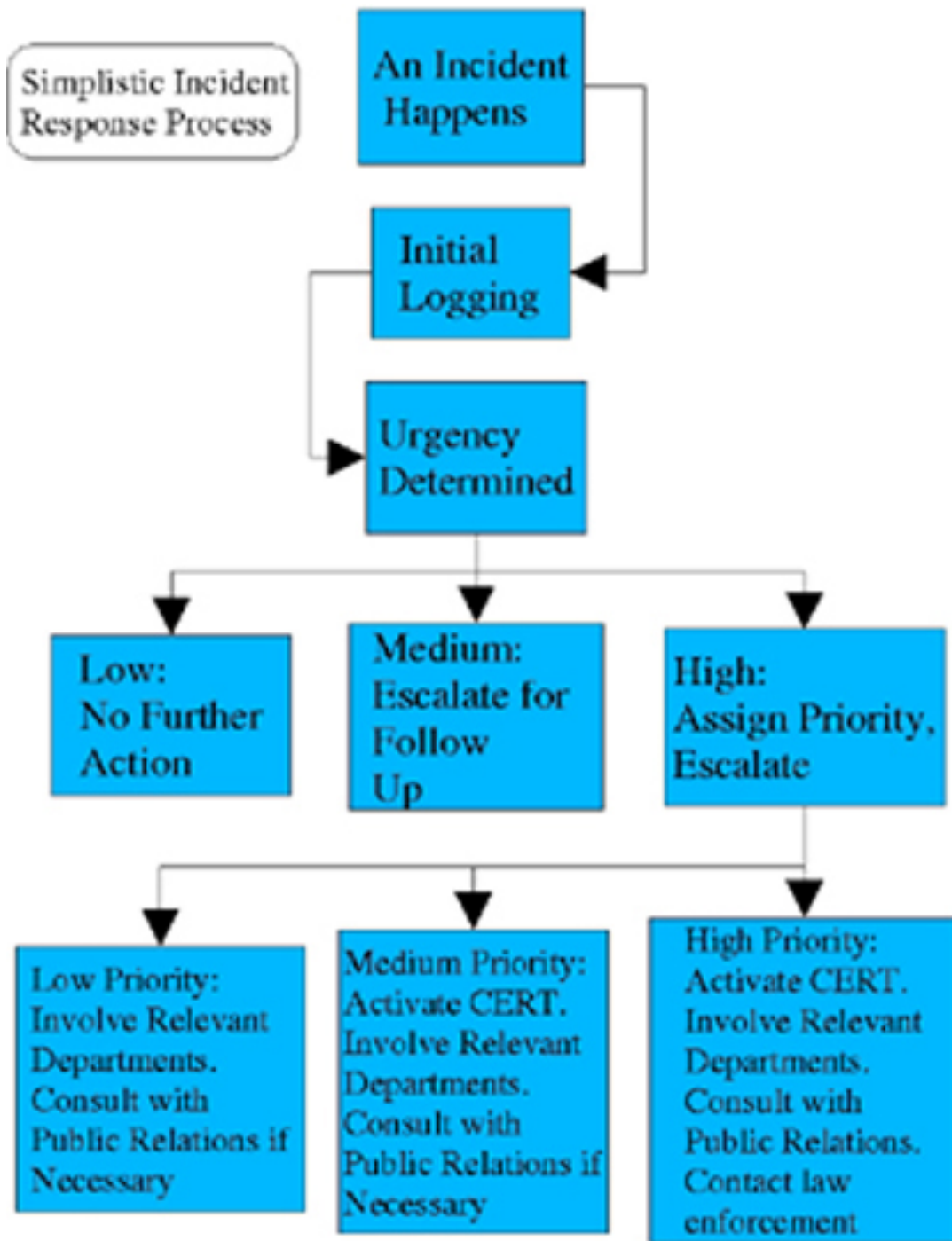
to whom they will be made available.

Business Continuity

A crucial element to consider in a useful incident response policy is that of business continuity. In the event that a serious incident should take place, a decision to halt certain information systems may need to be made. For example, during a denial of service attack it may be better to undergo a self-imposed service outage rather than wait for an overwhelming flood of service requests. Who should be responsible for determining when to pull the plug on a service, and under what circumstances is this an option? This needs to be set out in the Incident Response Policy. The converse is also of importance: who should be allowed to re-enable a service, and under what circumstances? As with other difficult policy questions, answers will vary from organization to organization.

Process Flow

Now we come to the heart of the incident response policy; it is within the process flow that the steps for response are outlined. The flow should start wherever an incident comes into being, and then trace the incident via the classification system up to the point where the CERT and other departments are notified. It's a good idea to use both a written description and diagram to describe the incident response process. Also, be sure to include a means for dealing with incident response at a vendor's site. Here is a very simplistic process flow that follows the classification system discussed above.



Example Incidents

The last element to be included in a useful information security policy is a table of example incidents and responses. The concept here is to provide sample incidents of varying degrees of nastiness, along with brief response summaries. The effect of such a table is two-fold. First, it will help you to think through the application of your response policy in a variety of situations. This is a great way to search for inadequacies within a policy's process. Second, a table of examples will anchor an incident response policy to the real world. It will allow an organization to better comprehend why the policy is needed.

Conclusion

By now, Information Security has become part and parcel of most organizations' business processes. This entails the development and deployment of useful policies to control and monitor information systems, and respond to electronic incidents. Without an incident response policy an organization will be unable to properly respond to an information security event. This can lead to a loss of money, bad public relations, and even additional security risks. The ingredients of a useful incident response policy include the following components: background, definitions, incident classification, reporting, business continuity, process flow, and example incidents.

For the past several years, [Timothy Wright](#) has been working within the computer security field: first as a Senior Technology Investigator, and now as an Information Security Officer. Previously, he worked as a lead developer within the financial industry, designing and building web-based home banking software. He holds an M.S. in Computer Science, and a B.A. in Philosophy.

[Privacy Statement](#)

Copyright 2006, SecurityFocus