

MANAGEMENT 414

SANS +S™

TRAINING PROGRAM

FOR THE CISSP®

CERTIFICATION EXAM

414.5

**Business Continuity
Planning and Law,
Investigations, and Ethics**

Copyright © 2006, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the SANS Institute. User may not copy, reproduce, distribute, display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, without the express written consent of the SANS Institute. Without limiting the foregoing, user may not reproduce, distribute, re-publish, display, modify, or create derivative works based upon all or any portion of this publication for purposes of teaching any computer or electronic security courses to any third party without the express written consent of the SANS Institute.

Preface

The cardinal rule for SANS training is that after you take a course you should be able to apply what you learned directly the day you get back into the workplace. My journey into writing about the 10 Domains started when Stephen Northcutt asked that I lead the development of adding the ISC2 10 Domains of Knowledge into SANS Security Essentials. That is SANS most popular training course and when taught bootcamp style it does an amazing job of helping students become capable of using hands-on techie tools. However, there had been a split in the community whether Security Essentials, which favored technical and pragmatic material, or the ISC2 10 Domains, which favors theory, should be the baseline standard for an information security professional. We were discussing this hotly debated issue in the SANS faculty speaker room over lunch one day and it suddenly dawned on us, why not add the 10 Domains into Security Essentials? Tony Cole, CISSP, was assigned to evaluate Security Essentials and determined that about 60% of the 10 Domains material was already covered in Security Essentials. Clement Dupuis and I were the leads on the project. This was a very successful edit and a number of students have passed their CISSP exams after going through SANS Security Essentials with the ISC2 10 Domains. However, when we added the additional material there was no longer time to cover the application of the material to the workplace; in addition, there are some students who prefer the more formal 10 domain structure.

To best meet the needs of the students, SANS authorized the creation of Management 414, SANS CISSP® 10 Domains +S™, which covers the 10 Domains of Knowledge in a formal 10 domain structure. In the meantime, Clement Dupuis, Stephen Northcutt, Marcus Sachs, Bill Stearns and Joshua Wright are removing some of the 10 Domains material from SANS Security Essentials and returning it back to the original vision for that track, to fully cover the essentials of technical security. Moreover, SANS has insisted that the course teach the application of the 10 Domains in the workplace - something no other 10 Domains course, including ISC2's does. This course meets the SANS promise: what you learn in the course you will be able to apply in the work place. One of the most important things I have learned from Alan Paller, Director of Research, in the years I have been involved with SANS is the importance of community consensus. In order to provide the highest quality training we have recruited experts to review the material and come to consensus on the course content and the application of the information. With the help of Zoe Dias, SANS Faculty Director, we enlisted a total of 68 reviewers from 10 countries. All but two of the reviewers are active CISSP's. The main author for the course, Eric Cole, has been a CISSP for almost 10 years.

SANS enthusiastically applauds the expert work of our technical reviewers/editors:

Monica Anklam, CISSP No. 31995, USA
Alex Arndt, CISSP No. 52343, Canada
Hank Askin, CISSP No. 40792, USA
Anjali Atanacio, CISSP No. 27039, USA
Jason Bevis, CISSP No. 35285, USA
Ron Black, CISSP No. 24245, USA
Anton Bojanec, CISSP No. 24560, Slovenia
Olufremi Bolanle, CISSP No. 51582, Nigeria
Jeff Bontsas, CISSP No. 39135, USA
Derek Browne, CISSP No. 26099, Canada
Sherry Callahan, CISSP No. 21760, USA
Ed Capizzi, CISSP No. 35909, USA
Jim Cate, CISSP No. 37031, USA
Patrick Chan, CISSP No. 40222, Canada
Jerry Chen, CISSP No. 47413, Canada
Daniel Cline, CISSP No. 31366, USA
Chris Cook, CISSP No. 38254, UK

Edwin Covert, CISSP No. 3597, USA
Phil Curran, CISSP No. 31708, USA
Edgar Danielyan, CISSP No. 42834,
UK/Armenia
David Dann, CISSP No. 51571, USA
Gary Delaney, CISSP No. 37636, USA
Sandeep Dhameja, CISSP No. 33585, USA
Joe Dial, CISSP No. 25358, USA
Heinz Durr, CISSP No. 42160, Switzerland
Darin Dutcher, CISSP No. 41299, USA
Rene Evers, CISSP No. 29057, USA
Chris Farrow, CISSP No. 45570, USA
Kenneth Fox, CISSP No. 42293, USA
Roger Fradenburgh, CISSP No. 28099, USA
Brian Freedman, CISSP No. 49504, USA
Donald Glass, CISSP No. 42244, USA
Mark Heinrich, CISSP No. 36190, USA

Lorna Hutcheson, USA
Lawrence Johnson, CISSP No. 25456, USA
Chaiw Kok Kee, CISSP No. 31589, Malaysia
Darrin Lau, CISSP No. 29948, USA
Eliot Leibowitz, CISSP No. 43782, USA
Steven Leong, CISSP No. 30313, Singapore
Chip Meadows, CISSP No. 10070, USA
Sean Mitchell, CISSP No. 36817, USA
Michael Morrell, CISSP No. 36227, USA
Pamela Nottage, CISSP No. 3758, USA
Sanjay Pandit, CISSP No. 44786, USA
John Pao, CISSP No. 29876, USA
Ariya Parsamanesh, CISSP No. 36074, AUS
Stephen Patton, CISSP No. 49746, USA
Robert Pfau, CISSP No. 21572, USA
Gabriel Proulx, CISSP No. 34018, Canada

Jim Purcell, CISSP No. 34519, USA
Andrew Salzman, CISSP No. 25162, USA
Amarottam Shrestha, CISSP No. 41671, AUS
Michael Solomon, CISSP No. 26517, USA
Robert Sorensen, CISSP No. 48304, USA
George Starcher, CISSP No. 34689, USA
Bruce Swartz, CISSP No. 46522, USA
David Taylor, CISSP No. 55890, USA
Brad Towers, CISSP No. 27957, USA
Jill Treu, CISSP No. 43196, USA
Tim Weil, CISSP No. 44250, USA
Deborah Weinstein, CISSP No. 44411, USA
Melody Wilson, CISSP No. 4130, USA
Steven Winterfield, CISSP No. 38096, USA
Kelli Wolfe, USA
Wayde York, CISSP No. 30404, USA

I have had the privilege of the best seat in the house and have really enjoyed working with the CISSP team. I sincerely hope that you benefit greatly from the information in these books and am very interested in your feedback. Please feel free to send me suggestions, corrections or questions to [mgt414\(5\)sans.orq](mailto:mgt414(5)sans.orq).

Eric Cole, Senior Instructor and Research Fellow
The SANS Institute

8. Business Continuity Planning

10 Domains of Knowledge

This section covers Domain 8, the Business Continuity Planning domain.

8. Business Continuity Planning

- What happens if a disaster occurs?
(DRP: disaster recovery plan)
- How do you ensure that your company can continue operations?
(BCP: business continuity planning)

The key questions that are going to be addressed in this section are the following:

- What is your organizational stance on security? (security policy)
- What happens if a disaster occurs? (The disaster recovery plan)
- How do you ensure that your company can continue operations? (business continuity planning)

Every business - corporate, education, or government - has customers. The customer wants to know that your company can get the job done on time. BCP is concerned with timeliness of production. For every customer, certain exceptions are understandable. They still want to know that the product is going to be delivered and when. Those exceptions (disasters) are things that customers realize are beyond anyone's control. From your customers' perspective, BCP is "business as usual," but your DRP is their BCP. If you cannot handle business problems, your customers will leave you for a better supplier. When your disaster affects their business, customers tend to be a bit forgiving or even helpful..the first time. The key to making the customer happy is having a transparent BCP and a clearly communicated DRP.

Key Terms

- Business continuity plan (BCP)
- Business continuity planning
- Business impact analysis
- Business resumption planning
- Contingency plan
- Continuity of operations plan (COOP)
- Crisis communication plan
- Critical systems
- Critical business functions
- Incident response plan
- Disaster recovery plan (DRP)

The following are key terms that are needed to understand BCP/DRP:

- Business continuity plan (BCP)
- Business continuity planning
- Business impact analysis
- Business resumption planning
- Contingency plan
- Continuity of operations plan (COOP)
- Crisis communication plan
- Critical systems
- Critical business functions
- Incident response plan
- Disaster recovery plan (DRP)

What Is a Business Continuity Plan?

Business continuity planning (BCP) enables the quick and smooth restoration of business operations after a disaster or disruptive event occurs.

Contingency Planning within Your Policy

A critical aspect of security policy for your organization is planning for contingencies. This section gives you an overview of contingency planning - what it is and why you need it - and walks you through the contingency planning lifecycle. By the end of this section, you will be equipped to do this for your organization and have references for further reading.

Overview of Contingency Planning

First, we define what a Business Continuity Plan (BCP) and Disaster Recover Plan (DRP) are and explain why an organization needs them. Subsequently, we dive into the process for developing them.

What Is a Business Continuity Plan (BCP)?

According to the National Computer Security Center, a Business Continuity Plan (BCP) is, "A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation."

Business Continuity Planning

- Minimize the effect of disruptions to business.
- Allow for resumption of normal business processes.
- Prevent financial and other intangible losses.
- Document procedures in time of emergency.

Business continuity planning encompasses the processes and actions necessary to ensure that the most essential business can continue to operate in the event of unforeseen events.

First, to minimize the effects of disruptions, we must first identify the following:

- Events/circumstances/actions that can cause a disruption (that is, threats)
- Cost-effective means of preventing disruptions and their impact (mitigation strategies)
- Ways of transferring or reducing risk (such as buying insurance)
- Recovery strategies that minimize downtime and loss of productivity

Why is continuity planning necessary? To prevent loss to the business of profits, assets, market share, client goodwill, and so on. Regarding loss, financial losses are often the predominate concern in the commercial sector. However, the loss of life, property, or national security might be of greatest concern in some fields, such as healthcare and in many government agencies. Financial loss is usually the easiest to quantify to management. Less tangible losses such as loss of goodwill are more difficult to quantify, but are just as important.

After plans have been developed to ensure continuity of operations, these plans must be documented and distributed to the proper personnel. This avoids confusion, ensures that all participants know what roles they play and what responsibilities they have, and provides an efficient way to quickly return to "business as usual."

What Is a Disaster Recovery Plan?

A disaster recovery plan (DRP)
covers the recovery of IT systems in
the event of a disruption or disaster.

What Is a Disaster Recover Plan (DRP)?

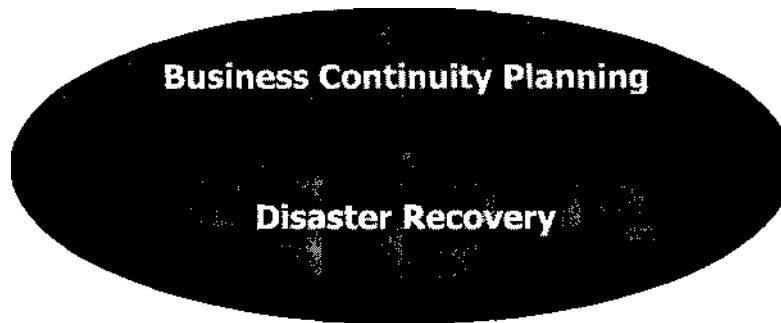
A disaster recovery plan (DRP) covers the recovery of IT systems in the event of a disruption or disaster. It provides the capability to process essential organizational applications, even if they are not operating at 100% efficiency, and the ability to return to normal operations within a reasonable amount of time.

While the terms BCP and DRP are sometimes used interchangeably, business continuity planning and disaster recovery planning are two distinct plans that tackle different areas of the recovery process. Business continuity planning deals with the restoration of the business processes or the continued operation of business processes. Organizational processes can continue without computers. For example, checks can be written by hand. With a continuity plan, the company can reduce the impact a disaster has on the normal business operation. The disaster recovery plan covers the restoration of critical information systems that support the business processes.

Disaster recovery planning involves the following steps:

1. The *recovery of the data center*: Because the DRP relates to the restoration of the information systems, it should address bringing the data center, one of the critical areas, back on line.
2. The *recovery of business operations*: This is sometimes referred to as *user contingency planning*. If a critical computer system is down, this part of the DRP deals with the alternative methods of continuing with the business operations. For instance, if your main payroll system were inoperable, a contingency plan could be to issue the payroll checks manually.
3. The *recovery of the business location*: Part of the business resumption plan, this section deals with the steps required to recover the actual physical business location. Often a disaster is partial, and recovery of the premises might consist first of patching together what is left, followed by backfilling what has been lost.
4. The *recovery of business processes*: Also part of the business resumption plan, this section handles the recovery of all of the various business processes so the company can resume normal business operations. This is the paramount step. The entire purpose of the plan is not about computers, networks, and data, but about the timely continuity and restoration of business processes.

BCP Evolution



In many instances, the terms disaster recovery planning and business continuity planning are used synonymously or, at least, are not clearly differentiated, thereby causing confusion among individuals introduced to this field for the first time.

Disaster recovery planning is an integral part of business continuity planning, but it does not encompass the entire discipline. The complexity of business operations forced disaster recovery planning to evolve into business continuity planning as planners recognized that more was required to ensure business survival than could be encompassed by disaster recovery planning alone.

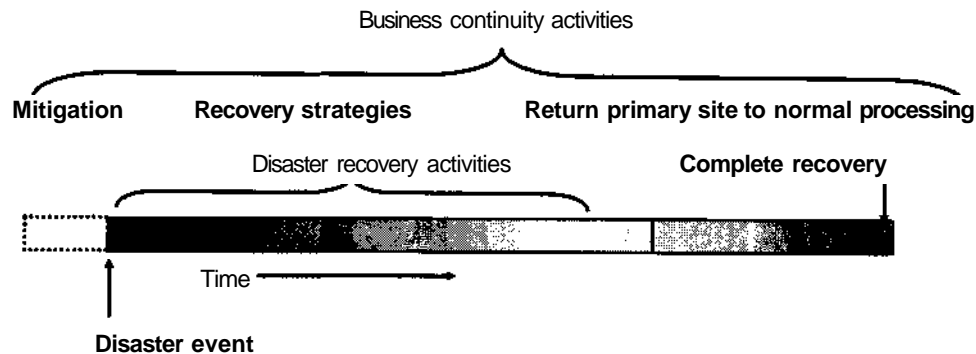
An easy distinction between disaster recovery planning and business continuity planning is:

- Disaster recovery is short-term focused
- Business continuity is long-term focused

This diagram illustrates the temporal relationship between disaster recovery planning and business continuity planning.

BCP versus DRP

Response versus recovery:



Disaster recovery provides a response to disruption, whereas business continuity planning implements the recovery. The preceding figure shows that the disaster recovery activities have a short time span, but business continuity activities are much more pervasive and long-lasting.

Note: Business continuity activities form an umbrella over a crisis situation, while disaster recovery activities are a *subset* of business continuity activities.

The goal of BCP/DRP is to make the response time to a disruption as short as possible and to minimize the time required for complete recovery.

During disaster recovery activities—that is, when a disaster has stricken an organization—almost all normal business activities are heavily modified, reduced, or completely suspended. Only critical business processes resume—and usually at an alternate site.

As repairs are completed, normal business activities resume as the business continuity plan dictates. Recovery is complete after all normal business processes return to "business as usual."

Why Have a BCP/DRP?

- Plan for the worst; hope for the best.
- Maintain business operations:
 - Or, at least, restore operations quickly
- Minimize the effect on customers or stakeholders.
- Understanding of the business is key.

Why Have a BCP / DRP?

Continuity planning might be likened to insurance: it is an expense consciously made to significantly reduce the impact of something bad occurring. You hope that nothing bad occurs. Even if it does not, the insurance premium and the expense of continuity planning were not wasted because they purchased certain assurances as a key component of the organization's risk management. As the slide says, "Plan for the worst; hope for the best."

Going through the process of identifying your customers (both internal and external) helps to define which business processes are the most important to your organization's survival. You must know who your customers are to properly prioritize business process restoration. For example, if a hospital's surgical center had a backup generator for the floor but the rest of the hospital was without power, many patients in intensive care could die as a result. If air conditioning were unavailable, more people could die from the heat even if they were not originally at risk (as recently happened in Europe). Power outages would prevent cafeteria workers from fixing patient meals, and staff would not even be able use most of the vending machines. Additionally, if power to the ambulance dispatch center was also impacted, requests for assistance could be affected; external customers might also suffer. This is an unlikely scenario, but it gets the point across: look at all the stakeholders, not just the most visible.

Why Have a BCP/DRP? (2)

A BCP is a business's last line of defense against risks that cannot be controlled or avoided by other risk management practices.

A BCP is a business's last line of defense against risks that cannot be controlled or avoided by other risk management practices. Business continuity and disaster recovery planning are not the places for having an "ignorance is bliss" attitude.

Organizations are often so reliant on key resources, such as technology, that they cannot operate without them. The most vital resources of all are human resources - that is, people who operate the organization's processes, including its recovery processes. The most important aspect of the BCP is to protect the lives of your employees. Yes, the name of the document is the Business Continuity Plan. In essence, however, unless you operate a company without people, employees are your most valuable asset. Consider the situation of the bond trading company Cantor Fitzgerald. During the September 11, 2001 terrorist attacks on the World Trade Center in New York, Cantor Fitzgerald lost over 700 of their 1,000 employees. Even if they had been able to get their computer systems up and running, they would not have had the personnel to continue business.

Disruptive Event

Any act, occurrence, or incident— whether intentional or unintentional — that suspends normal operations.

- Utility failures
- Fire/smoke
- Natural disasters
- Heat/humidity
- EMI
- Terrorist attacks

The types or categories of disruptive events are many. Some events, while unexpected by the organization, are intended to cause damage or at least interfere with operations. These can include hostile code, such as viruses, worms, Trojans, logic bombs; sabotage; vandalism; theft; and terrorist attacks. Examples of other disruptive events include power outages or fluctuations, natural disasters, severe weather, chemical spills, toxic contamination, accidents, or outages caused by human error.

Environmental problems and people (whether intentional or not) cause disruptions. Sometimes equipment simply fails; utilities fail, resulting in loss of power, cooling, and humidity control. Fires start, causing direct and indirect (for example, smoke) damage. Natural disasters occur with flooding, high winds, and structural damage.

User access can be disrupted even when data center equipment is operational. In many organizations a power failure takes down the desktop clients while leaving the servers that run on uninterruptible power supplies (UPSs) operational. Always analyze the dependencies when planning contingencies. Remote users might depend on the data center and the network connectivity between them being operational. Even if local users are down because of a local power outage, it is possible that remote users (where power has remained up) can continue to work *if the* plan ensures that the network equipment is also power protected.

Key Disasters

Data Pro study of likely attacks:

- Errors and omissions: 50%
- Fire, water, electrical: 25%
- Dishonest employees: 10%
- Disgruntled employees: 10%
- Outsider threats: 5%

People make mistakes and sometimes intentionally disrupt operations. This covers a wide spectrum of threats, from human error to malicious software or network intruders, and ultimately to armed conflict, such as a terrorist attack. Perhaps surprisingly, human errors and omissions account for half of the disasters that actually occur! A study conducted by Data Pro breaks down the numbers as follows:

- Errors and omissions: 50%
- Fire, water, electrical: 25%
- Dishonest employees: 10%
- Disgruntled employees: 10%
- Outsider threats: 5%

Contingency planning is an organization's attempt to mitigate these threats, as we discuss next.

Basic Elements of Continuity Planning

- Define the plan's goals.
- Define why the plan is important.
- Provide a set of priorities.
- Write a statement of organizational responsibilities.

Basic Elements of Continuity Planning

The key components of a Business Continuity Plan are as follows:

- Assess: Identify and triage all threats through a Business Impact Analysis (BIA).
- Evaluate: Assess the likelihood and impact of each threat.
- Prepare: Plan for contingent operations .
- Mitigate: Identify actions that might eliminate risks in advance.
- Respond: Take actions that are necessary to minimize the impact of risks that materialize.
- Recover: Return to normal as soon as possible.

The Continuity Plan should define the goals of the plan and why the plan is important. Writing a plan without understanding the goals is almost as bad as not having a plan at all. The plan should provide a clearly defined set of priorities and a statement of urgency, based upon the Business Impact Analysis. While developing the plan, you should be asking the following questions:

- Why is a business continuity plan important to my organization? That is, what would the impact be if we had a disaster and no plan for how to handle it?
- What are the most important business functions (and/or IT systems) that must be recovered quickly, before you lose the ability to continue business operations?
- Is the plan's goal simply to prevent further damage, or to actually stop and fix the problem?

Basic Elements of Contingency Planning (2)

- Include a statement of urgency.
- Include information on vital records.
- Define an emergency response procedure.
- Define emergency response guidelines.

The plan should clearly define organizational responsibilities, emergency response procedures, and emergency response guidelines. It is critical that roles and responsibilities be clearly and unambiguously defined. Time is too precious during disaster recovery for turf wars, inadequate empowerment, or lack of clarity regarding who is in charge. Security controls might need to be altered during recovery, and the empowerment of certain personnel might have to be increased. Definitions for when and under what circumstances such changes from normal procedure begin and end must be clear. This should all be documented clearly to avoid any misunderstandings, security violations, or delays in recovery.

Information about vital records must be included in the plan. This is often the bulk of the documentation and might include lists of people and how to contact them, inventories of equipment, software and data - including off-site back-ups and how to obtain them - vendors and how to contact them, information about emergency services, network diagrams, media contacts, and so on. This is where the planners' imagination becomes evident. We become very used to the information within our systems and take access to it for granted. Think about this question: "When I cannot use my system(s), what information that I normally rely on is no longer available?" Some needs might be different during recovery than normal. For example, electronic communications needs can change as a result of users or systems being relocated. But these needs can also be inventoried. Site-knowledgeable personnel are the most important recovery component. This is especially so because disasters are usually only partial losses; and initial recovery consists of patching together what is left, including business processes. This takes knowledgeable people.

Fortunately, extensive information on contingency planning is available. Other sources include:

- The MIT Business Continuity Plan: <http://web.mit.edu/security/www/pubplan.htm>
- University of California Campus Business Continuity Planning: <http://www.ucop.edu/facil/eps/continuity.html>
- Treasury Board of Canada BCP: http://www.cio-dpi.gc.ca/emf-cag/busconplan/bconplan_e.asp
- University of Sydney Business Continuity Plan: <http://www.personal.usyd.edu.au/~stephen/network/disaster3.shtml>

Continuity Planning Evolution

- Initially consisted of disaster recovery only
- No longer only about numbers
- As much an art as a science
- Highly business-dependent

Business continuity planning is a newer term than disaster recovery planning. It evolved from the practice of disaster recovery. In its early stages, disaster recovery planning was more of a science than anything else.

Disaster recovery planning usually only dealt with the backup and recovery of business systems, where planners could measure a solution's effectiveness against its cost and offer recommendations based on their company's needs and budgetary constraints. It was a scientific, number-crunching discipline.

Although this formulaic approach was specific, easy to document, and favored anal-retentive, type A personalities, business continuity planning evolved into a strategic business concern that incorporates more than hard numbers, charts, and graphs. This is not to say that the scientific approach is not important or that it is an unnecessary aspect of business continuity planning - far from it. However, factors relating to a corporation's survival are many and varied; as the following list illustrates, some aspects are difficult to quantify and/or measure:

- If the equity in a brand is somehow tarnished, can the company calculate how much it would cost to regain lost equity?
- How much would it cost to launch a marketing campaign to regain lost customers?
- How much is a customer list worth?
- How much does it cost to build a customer base?
- How much does it cost to build a *loyal* customer base?
- How much would it cost to retain your employees who were ignored, shortchanged, or otherwise hurt by the company's inability to respond to a disruption?
- How long does it take to build experience relating to the business's processes?
- How much is a veteran worth?
- How quickly can we train other employees if our experts leave?

Resistance to Building a Plan

- "It cannot happen to us."
- "We are too small to be noticed by a hacker."
- "It is too expensive."
- Saying that you can recover from a disaster requires admitting that you are vulnerable to one.

Most people believe that disaster will not happen to them; it will happen to someone else instead. This belief is normal, but it represents perhaps the greatest resistance to building a business continuity plan because, at some fundamental level, we do not want to bet against ourselves. By thinking that bad things *might* happen, we believe we *make* bad things happen. By not thinking about bad things, we preclude Fate's attention. Of course, reality is immune to such superstitions.

Although probabilities do much to assuage our fear regarding the frequency of tragic events, even the most in-depth cognitive analysis never quite overcomes our para-rational uneasiness, no matter how conclusive or definitive statistics might be. Again, it harkens back to not betting against ourselves. However, BCP is not about betting *against* ourselves; it is about betting *for* ourselves.

Unfortunately, uneasiness is a far louder voice than reason or rational thought alone. We often hear such irrational thinking as:

- It cannot happen to us.
- We are too small to be noticed by a hacker
- It is too expensive to implement a solution; and besides, it probably won't happen anyway.
- It has never happened before.
- It will never happen here.

It's as if some people believe that obtuse statements invoke a magical talisman immunizing the corporation from harm or hazard. The greatest resistance to building a continuity plan is simply the reluctance of management to see potential disaster. Ironically, many in corporate leadership positions perceive the ability to recover from a disaster as a confession that the business *is vulnerable to a disaster in the first place*, a wholly unacceptable admission indeed.

You Cannot Do it Alone

- Involve senior management.
 - Support from above is a must.
 - They approve the final plan.
- Teams are essential.
 - There is a lot of paperwork.
 - The more complex the business, the more help you need.

Understanding resistance is one thing, but overcoming resistance is another thing altogether (and a book unto itself). There are two prerequisites to building a business continuity plan:

1. Never do it alone
2. Get C-Level support

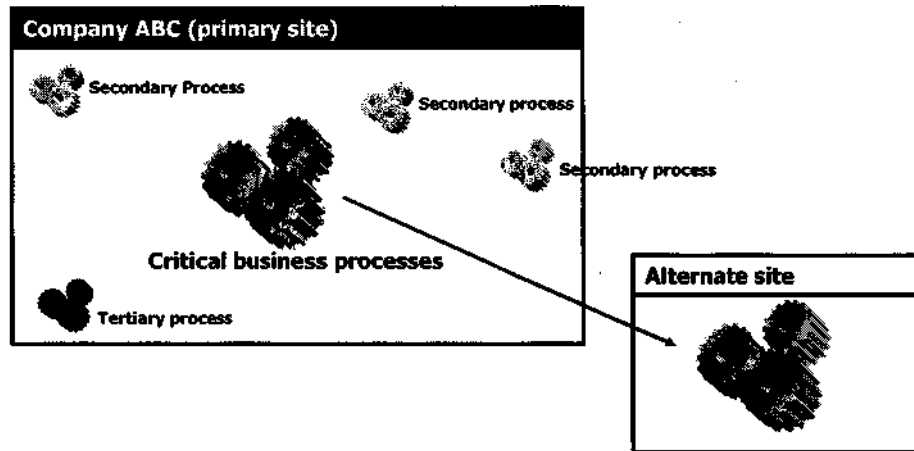
C-level support refers to the "Chief level positions within a company: CEO, CFO, COO, CIO, and so on. Without senior-level support, most business endeavors - the least of which is a business continuity plan - are bound to fail and thus hamper your job stability. Senior-level approval is mandatory, especially before any BCP activities, because it assures resource commitment and management attention (and awards). Although it is important to show initiative as a security manager, senior management must ultimately understand, support, and even drive the goal of developing a business continuity plan.

The security manager should not approach senior management alone or attempt to construct the plan as an isolated entity. You cannot do it alone— without senior management support—nor can you do it without the support and input of the other members within the corporation.

Also, the complexity of the business model—the number of production centers, the network topology, the corporation's geographic distribution, internal and external dependencies—might make generating a business continuity plan an onerous and overwhelming task if you try to do it yourself. The chance that you will overlook a critical aspect of the business' moneymaking machinery will dilute and even nullify the purpose and intent of business continuity planning.

Even in a small business where you might wear the hats of security officer, IT manager, and help-desk technician, get someone else involved in continuity planning. You are surveying the topology of your corporation; the more eyes, the better.

Continuity: The Big Picture



There is a critical business process at the center of the corporation's money-making machinery. It might be the production floor of an automobile manufacturer or the Web servers of an e-commerce firm.

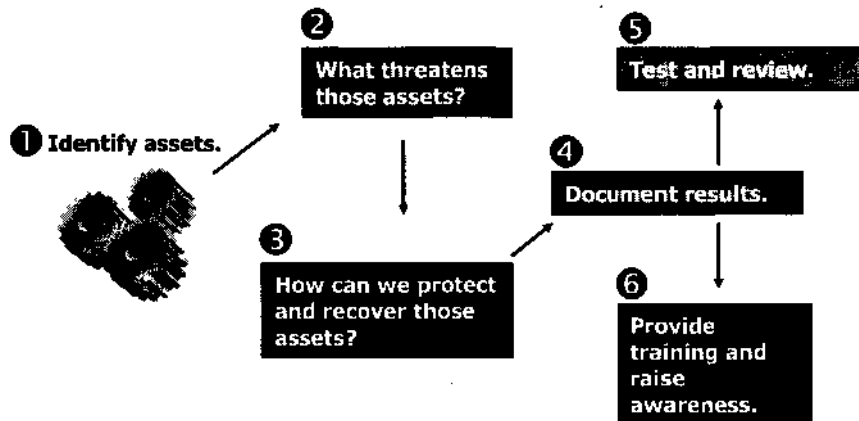
Whatever the process — and whatever technology supports it — you must identify the process and ensure its continued operation. This is not to say that you should ignore the secondary and even tertiary processes — only that you prioritize in the grand scheme of things.

Some business processes, if disrupted for only a moment, can rob the enterprise of valuable income or market agility, whereas other processes might tolerate disruption for several days without any adverse affect. The big picture of business continuity is making sure your business keeps making money.

In this diagram, Company "ABC" conducts business at a primary site; that is, the critical business process is in operation at the critical facility. Additionally, secondary and tertiary processes surround the critical business process.

Company "ABC" constructed an alternate site where the critical business process can be moved or continued if the primary facility is unavailable for any reason. Note that the alternate site does not provide any support for secondary or tertiary business processes; this might not always be the case.

Continuity: The Process



The nice thing about pictures is that they make everything look so simple. Although the preceding figure makes the process of continuity planning look straightforward, the details are numerous. However, keeping the big picture in mind will help you maintain perspective, regardless of how complicated the actual construction of the business continuity plan becomes. Note that this process has many variations.

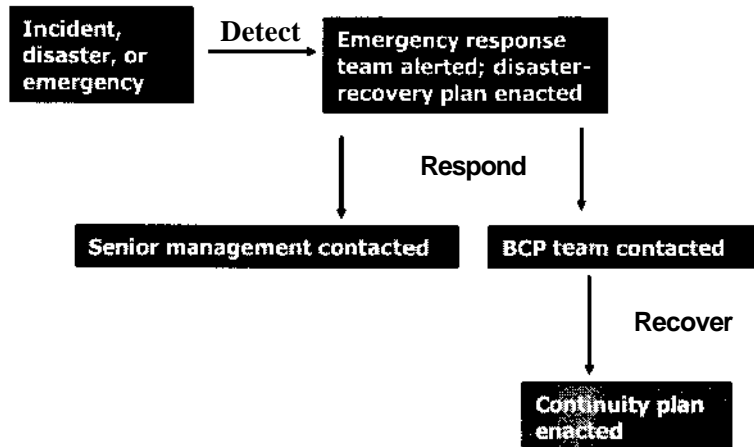
The following list outlines the business continuity plan steps and the questions you must ask for each step:

1. Identify assets.
2. What threatens those assets?
3. How can we protect and recover those assets?
4. Document the results.
5. Test and review.
6. Provide training and raise awareness.

The good news is that in the process of building your security program, you have probably already accomplished steps 1, 2, and 3. What you probably have not covered is how to recover in the event protection fails. Step 4 involves creating the business continuity plan itself: the documentation that you will print and distribute to all appropriate personnel.

Step 5 involves testing and reviewing the continuity plan. There are many different ways to ensure that the continuity plan actually works, ranging from inexpensive and nonintrusive to cost-prohibitive and extensive. It is important to create a continuity plan that is testable; with that said, there are some industries that might not be able to test their plans because of operational constraints. Surprisingly, this is not uncommon with casinos, trading floors, and other high-paced entities. Most corporations, however, can test at least some part of the plan, if not the entire thing. Testing makes sure that the assumptions and ideas with the continuity plan are sound and sufficient. Reviewing the continuity plan is another critical aspect of continuity planning. If the plan does not properly reflect the current state of the corporation, the continuity plan might be, for all intents and purposes, useless.

Continuity: The Activity



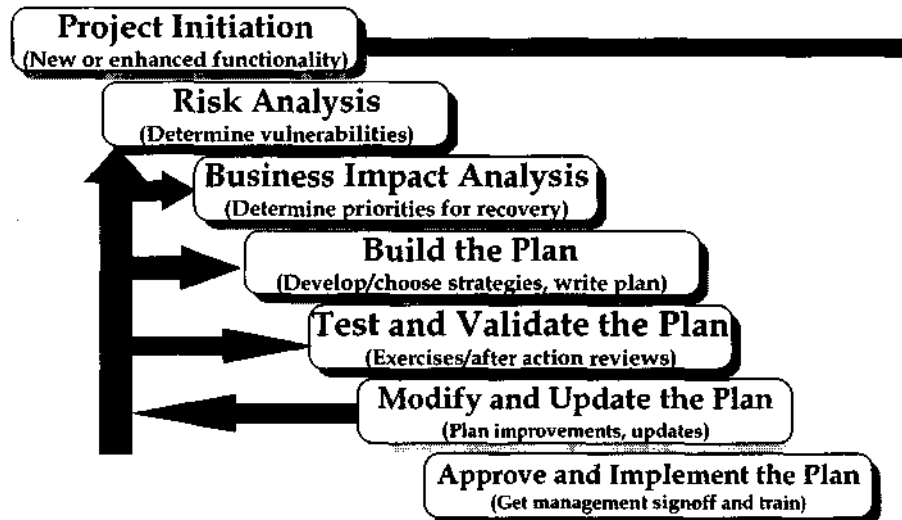
Again, a diagram offers a simplistic view of the response mechanism for a corporation; however, it does give you a good idea of the intent of the business continuity process before discussing BCP in detail.

When a disruption occurs, it is detected and the emergency response team (ERT) is contacted in some predetermined manner (documented in the BCP of course).

The emergency response team assesses the situation and determines whether an emergency exists and whether BCP/DRP activities are required. If so, ERT contacts both senior management and the business continuity team members and apprises them of the situation.

In collaboration with the business continuity team members, the emergency response team determines the affected business functions and enacts relevant sections of the business continuity plan.

BCP-DRP Planning Process Lifecycle



BCP-DRP Planning

This slide shows the basic steps that are necessary when developing a BC/DR plan. We start with Project Initiation, for which new or enhanced functionality is required. At this point, you must get management approval to start the project. Management is instrumental in making sure that you have access to the resources that are required to get the job done. The next sequence of steps in the process concerns the company's vulnerabilities, their significance to the company, and what the company is going to do about them.

First, the company determines its vulnerabilities through a Risk Analysis. The company then assesses the impact that each of these vulnerabilities represents for the company by completing a Business Impact Analysis. Realistically, no organization has the resources to deal with every vulnerability. Instead, in this step, the company prioritizes the vulnerabilities based on their likelihood and impact. Those vulnerabilities that represent greater risk to the company are identified so that steps to avoid their occurrence can be planned. In the event that those plans fail, the prioritized vulnerabilities can also be given priority in terms of recovery of affected operations.

Remember, not all losses are directly associated with loss of money (although it will most likely affect the company financially in the long run). Do not forget to include the "intangible" losses, such as customer satisfaction or loss of consumer confidence. For instance, if a major e-commerce shopping site is down for a long time, consumers will become frustrated and will perhaps begin shopping somewhere else. At that point, it does not matter what caused the problem: earthquake, flood in the data center, or denial of service attack. The fact is that the site was down. The faster the company is able to recover, the better. Conversely, professional handling of a disaster can actually improve an organization's reputation with its customers and other stakeholders.

Steps to Business Continuity

- **Project initiation**
- Risk analysis and reduction
- Recovery strategies
- Developing the continuity plan
- Exercising and maintaining the plan
- Training and awareness

Business continuity planning comprised of multiple steps, beginning with project initiation. The following sections introduce each step in as much detail as permissible.

As a final note before beginning our discussion, the business continuity plan itself- that is, the finalized and published document - might not be organized identically to the steps presented. We address the format of the business continuity plan later.

Project Initiation

- Appoint project manager
- Establish executive support
- Build the team
- Scope the project
- Define objectives and deliverables

Project initiation involves the following tasks:

- Appointing a project manager
- Establishing executive support
- Building a team
- Scoping the project (prioritizing)
- Defining the objectives and deliverables

Appoint Project Manager

- Good leadership skills
- Understands business processes and management
- Experienced in IT and security management
- Strong project management skills

As in any business project, you must appoint a project manager as the lead for the business continuity plan. This individual acts as the enterprise-wide point of contact for continuity planning issues and interfaces with executive management. As the security officer, you are the ideal candidate to take on this role; but do not be surprised if the company makes this a new-hire, full-time position that is separate from the security officer. Whoever takes on the role must be enthusiastic and motivated about building the continuity plan. It is no small task; there will be many hurdles to overcome.

The project manager sets up the initial meeting of continuity team members and provides an overview of the business continuity process and all that it entails. Additionally, the project manager does the following:

- Constructs a project budget that delineates costs to the company for creating the plan, including manpower costs, planning tools, reference materials, outside consultants, training, and equipment.
- Provides monthly update reports detailing activities, any difficulties that were encountered, subsequent resolution, and progress against project timeline.

Establish Executive Support

- Provides critical resources
- Helps define and agree on the scope of the project
- Final approval of the business continuity plan and its contents

At this point, establishing executive support should be a no-brainer because it ensures money, resources, and people. Most importantly, however, is that a business continuity plan is not yours; it is the CEO's. Ultimately, the business continuity plan is a statement of commitment from the CEO to employees, customers, and colleagues about the CEO's willingness to provide reliable services and products in a timely and assured manner. It says, "I, as the CEO, will do my absolute best to continue to serve you."

Build the Team

Reflect as much of the company as possible:

- Business unit managers
- IT and security staff
- Human resources
- Payroll
- Physical plant manager
- Office managers

It is important to include as much of the company's hierarchy as realistically possible. There is no telling where a disruption might occur; and it is important to rely on the expertise of each member to add value to the business continuity plan. In reality, each employee has a vested interest in the company's ability to handle disruption because paychecks depend on it. Possible members include business unit managers, IT and security staff, human resources, payroll, the physical plant manager, and office managers.

The temptation is to include too many people on the continuity team or to fail to carefully select and train the team. To fall into such a trap might impede the planning process in particular and the value of the continuity plan as a whole. Include team members based on their positions in the company, the importance of those positions, and the business functions they represent in addition to their ability to work in a collaborative and team-oriented manner. Project managers should be discerning, but not repressive in the selection process. The business continuity plan's success depends on the ability of the team who creates, plans, and then executes the continuity plan.

Your team will eventually have the following categories:

- **Executive team:** Business unit managers, senior managers, and executive managers in the business unit who are responsible for recovering critical functions
- **Management teams:** People in the command center who are responsible for managing, controlling, and guiding the recovery efforts
- **Response teams:** People responsible for executing the recovery procedures and processes. Typically, you assign one team per critical business function.

Scope the Project

- What do you include in the plan?
- How do you collect information?
- What resources are required?
- What is the continuity team's management structure?
- Will you use a top-down or a bottom-up approach?

A little bit of forethought goes a long way. As the size of the company increases, so does the necessity to detail the required work and the resources necessary to build an effective business continuity plan. "Detail" is the name of the game. You are creating a map of the company; therefore, the more detail, the better. You should closely examine the company's operations and describe them in as much detail as possible. Who gets paid when? Who are the vendors? Who are the customers? What is the company's workflow? On whom do you depend for raw material, paper, water, and electricity? How many offices do you have, and where are they located? How many employees do you have? What is your turnover? Who is your insurance provider, and what are you insured against?

In these cases, you are not looking for vulnerabilities or weakness; you are simply trying to build a map of the company so you know your assets. If you do not know what you have, you might not know what needs attention. Of course, detailing the continuity team's needs is just as important. How often do you meet? How do you handle all this information? How do you categorize it? How much work do you have? What resources do you need to make this possible? This step gives the list-happy people in the group an opportunity to contribute to the effort. A final important point is to document the continuity team's management structure. Will it be a flat organization with individuals acting on behalf of their business units, or will you adhere to a strict hierarchy with information flowing up and down the chain in a predefined manner?

A top-down approach is a great way to create a company's first business-continuity plan. Beginning with senior management, the team interviews business unit leaders, middle management, IT management, and end users. In this manner, the continuity team can see the company from many different perspectives and build cross-company relationships that are necessary during the risk-analysis portion of the process. Again, you are not yet looking for vulnerabilities or weaknesses; you are simply getting a feel for the environment. The bottom-up approach is better for maintaining the continuity plan than creating it. After you document all aspects of the organization, the bottom-up approach works better as a sanity check and a measure of the effectiveness of the current continuity plan.

Define Objectives and Deliverables

- Objective: Create a business continuity plan.
- Deliverables:
 - Risk analysis and impact
 - Disaster recovery steps
 - Plan for testing
 - Plan for training
 - Procedure to keep the plan up-to-date

The objective of the business continuity team is fairly self-explanatory: to produce a continuity plan that enables the corporation to recover as quickly as possible from unforeseen disruptions that interrupt the normal flow of information and/or business.

The deliverables can be just as simplistic as the objective statement: a spiral-bound business continuity plan for all involved parties. However, such a statement is a bit too broad. The business continuity plan is actually a number of documents rolled into one. You should list each of those documents as a deliverable. There is no telling how complex the plan will be or how many situations the continuity team might face, so you should account for each section of the plan. Additionally, depending on the sensitivity of the information, you might exclude the risk analysis from the document for purposes of confidentiality.

This sort of documentation is usually required for federal agencies, but it is also beneficial to commercial agencies. Having clearly defined processes, procedures, roles, and responsibilities eliminates confusion, reduces misinterpretation, helps facilitate the training of new personnel, and allows management to understand the environment in which the business operates. The documentation can also serve as justification for additional funding.

Steps to Business Continuity

- Project initiation
- **Risk analysis and reduction**
- Recovery strategies
- Developing the continuity plan
- Exercising and maintaining the plan
- Training and awareness

Risk analysis and reduction is a critical step in the business continuity process because understanding a corporation's threat environment directly affects decisions regarding recovery strategies. This section discusses concepts that relate to risk identification, analysis, and reduction.

Risk Analysis Questions

- What are the specific threats to your organization?
- What would you do to protect your information resources?
- More importantly, what are your critical business systems and processes?

Risk Analysis

Here we focus on risk analysis as a component of contingency planning. For that purpose, risk analysis consists of the following steps:

- Identifying your critical business systems and processes
- Identifying the specific threats to your organization, especially to those critical systems and processes
- Evaluating the vulnerability of an asset and the probability of an attack or disruption to occur
- Determining what you would do to protect your information resources
- Weighing the loss of assets versus the cost of implementing mitigating controls

Risk can be expressed as follows:

$$\text{Risk}(\text{duetoathreat}) = T_{\text{threat}} \times \text{Vulnerability}^{\text{that threat}}$$

Or more completely, as expressed in ISO 1779 and many risk management methodologies :

$$\text{Risk}(\text{duetoathreat}) = T_{\text{threat}} \times \text{Vulnerability}^{\text{that threat}} \times \text{Impact}$$

Consider an example:

Suppose I have a big glass window in the front of my house. The vulnerability is that the glass is breakable. The threat is that someone can throw a brick to break the window. Which one is easier to fix, the vulnerability or the threat?

I can probably eliminate the vulnerability more easily (that is, less expensively) than trying to eliminate the threat. In our example, I can reduce the vulnerability by changing the glass window to something more resistant. This would be less expensive than taking steps to prevent bricks from being thrown at the window (and therefore removing the threat).

Notice the multiplier in these equations. To eliminate the risk, either the threat or the vulnerability must be equal to zero. Of course, if the impact (sometimes termed asset value) is zero, then the risk is also zero. Can we really eliminate the threat or the vulnerability? The question you need to ask yourself is, "How does the cost of the asset compare with the cost of protecting the asset?" By knowing these two costs, you can determine the return on investment (ROI) for protecting the asset and decide a course of action accordingly.

When calculating the cost of a threat, look at two factors: the single loss expectancy (SLE) and the annualized loss expectancy (ALE). SLE is the cost of the event should it occur once. It is calculated by multiplying the asset value by the exposure factor (percentage loss for that threat).

$ALE = SLE * \text{the Annualized rate of occurrence (ARO)}$, where ARO is the possibility of a threat taking place within a one-year period.

Risk Analysis

- Weigh the losses of assets versus the cost of implementing a mitigating control.
- Evaluate the vulnerability of an asset and the probability of a loss.
- Sometimes it is more economical *not* to protect the asset!

After you understand the risk, you can take one of four approaches:

- *Risk avoidance*: In this instance, you decide not to become involved in the risk situation.
- *Risk acceptance* (also termed risk assumption or risk retention): Here you acknowledge and accept that the risk is something that could happen. You intentionally or unintentionally retain or assume the responsibility for loss or the financial burden of loss within the organization.
- *Risk transfer*: You shift the responsibility or burden to someone else. An example would be getting insurance to cover the damage.
- *Risk reduction*: You apply the appropriate controls to mitigate the effects of the disaster, thereby reducing the risk.

Next we look at the impact component of business risk by performing a business impact analysis, or BIA.

Business Impact Analysis (BIA)

- Determine the tolerable Impact levels your system can have.
 - How long can your systems be compromised?
 - What is the maximum allowable or tolerable downtime?
- Evaluate the effect of a disaster over a period of time.

Business Impact Analysis (BIA)

After risk analysis in the BCP-DRP planning process lifecycle comes business impact analysis (BIA), where you determine what levels of impact to your system, such as the duration of system outage, are tolerable.

The process of developing the BIA typically involves interviewing key users of the various computer systems (for example, payroll, accounts payable, and accounting) to get a better understanding of how a disaster could impact the ability to continue operations. Some of the key interview questions might include the following:

How would an information technology failure affect cash flow?

Would the disaster impact the level of service?

How long could the outage last before it began to affect your productivity?

How long could operations continue if data were unavailable?

Would there be irretrievable loss of data?

What key resources are required to continue operating?

At what point would those resources need to be in place?

If we implement a mitigation strategy, will there be additional risks? If so, are we better off by implementing or not?

The answers should come from or be agreed upon by executive management. Executive management understands such cost tradeoffs as mitigation and loss and has individual accountability either way. Lower management might err toward too much (that is, too expensive) risk avoidance, while upper management might prefer to accept certain risks and redirect mitigation resources elsewhere in the business. Not considering the proper balance is a common mistake in BCP/DRP planning.

Maximum Allowable Downtime

- Total amount of time for which a process can be nonfunctioning before causing major financial impact
- Identifies point of no return
- Derived from BIA
- Used to define resource requirements

Maximum allowable downtimes derived from the BIA are the basis for determining recovery resource requirements. The ultimate objective is to define the post-disaster resource requirements upon which a recovery strategy might be based. Ultimately, the need for recovering critical business processes drives the recovery resource requirements (the recovery budget). Often senior managers try to set an arbitrary budget of what the company is willing to spend on recovery and thereby force the business continuity team to work within those parameters. However, the needs of the business should drive the budget, not the other way around.

What is the financial impact you should consider? The following are a few points to consider:

- How much revenue would your company lose if its systems were unable to accept orders?
- What is the cost of lost productivity?
- How much inventory would be lost or spoiled; and how much would it cost to recover the inventory?
- What is the value of IT professionals' productivity while trying to resolve the problem?
- What fines and fees would the company have to pay?
- How much would a public relations campaign cost to regain your company's image?
- Will the company face any legal, health, safety, or liability exposure?
- Can you really afford the cost of implementing 24X7 operation without any downtime? Do you have the personnel and technical resources to do this? If not, how do you prioritize?

Many companies make a critical mistake by assuming that they should conduct BIAs only once before writing the initial business continuity plan. One BIA is usually never enough; you should conduct BIAs over the lifetime of a corporation, especially if you undertake any major technology upgrades or add, modify, or delete processes. Any alterations to the business affect the recovery-resource requirements. These resource requirements drive your recovery strategies, so it is important to ensure that the business needs are properly reflected.

Risk Analysis and Reduction

Vulnerability assessment:

- It is smaller than a full risk assessment.
- Identify critical business functions.
- Use results as input to recovery strategy.

The vulnerability assessment is typically part of the business impact assessment (BIA) and is smaller in size and scope than a full risk assessment.

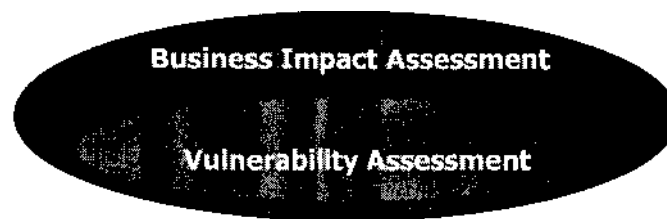
The focus of the vulnerability assessment is to provide data that is used solely as input into the recovery strategies and determine the impact of losing a critical business function. You identify and target critical business functions. Any business function that must be present to sustain the continuity of the business or could in any way threaten human life during a failure is a critical business function. Additionally, if a business function's failure brings discredit or public embarrassment to a corporation, it is also considered critical. Such a determination is usually up to the corporation, however, because only the business can determine what it deems embarrassing.

Vulnerability assessments provide the bulk of the financial and operational costs of a disruptive event. If anyone in your company is looking for hard numbers, this is the place to find them. You can establish quantitative and qualitative criteria to determine financial and operational costs.

Business Impact Assessment

Business Impact Assessment (BIA):

- Business function priorities
- Timeframe for recovery
- Resource requirements



The business impact assessment (BIA) documents the impact a disruptive event might have on a corporation. The BIA uses the information in the vulnerability assessment to prioritize business functions and calculate business impact.

Obviously, the greater the impact of a business process failing, the higher its priority in terms of criticality. A direct relationship might exist between the criticality of a business function and the timeframe for which it must recover. Some business functions, if down for only a few seconds, might dramatically and detrimentally impact the business. Other business functions might be interrupted for days or weeks and have no negative affect on the corporation.

The primary goal of the BIA is to determine the maximum allowable downtime for any given system. A rough guide for timeframes follows:

- **Immediate recovery:** No downtime allowed. Implement a fully-staffed, fully-equipped alternate site (more on alternate sites later).
- **Quick recovery:** Up to four hours of downtime allowed. Pre-equipped alternate site should be available. Staff can arrive at the site within four hours.
- **Same-day recovery:** You can move equipment to another location and set it up in an eight-hour period. Same-day recovery can also mean same *business-day* recovery. The alternate site can be anything that affords appropriate power and protection (another office, hotel room, home, and so on).
- **24-hour recovery:** This is self-explanatory.
- **72-hour recovery:** This is self-explanatory.
- **Greater than 72-hour recovery:** This is self-explanatory.

Steps to Business Continuity

- Project initiation
- Risk analysis and reduction
- **Recovery strategies**
- Developing the continuity plan
- Exercising and maintaining the plan
- Training and awareness

Based on the risk analysis and mitigation strategies developed in previous steps, we must now look at what to do in the event that a disruptive event should actually occur. Because we know that there is no such thing as a 100% secure operation, we know that recovery strategies will be required— the only questions are: When? And will we be prepared?

Recovery Strategies

- Outside help might be necessary
- Respond, and then recover
- Disaster recovery planning
 - Procedure for handling the disaster

After the BIA is complete and the corporation knows what the impact of a loss might be, it can start planning an appropriate response. The fun — and frustrating — part of recovery strategies is that you are solving problems that do not yet exist. Essential to any top-notch recovery plan are multiple strategies to cover most, if not all, business disruptions. However, actually accomplishing such a feat can be challenging and, in some cases, unrealistic. Most often, companies must look to consultants, vendors, and similar companies for advice and recovery strategy trends. Developing recovery strategies can also be the most frustrating part of the continuity planning process because this is where the rubber hits the road. Costs might loom large. The complexity of replicating, backing up, or mirroring critical business processes all of the sudden seems cost-prohibitive, and executive and senior management begin to waiver in the face of the beast that is their own business.

The sanity check for the growing hysteria of your senior management comes from the BIA that you, as the team lead, so diligently conducted. Compare the options for attaining recovery, once investigated and priced, against the potential cost of failing to recover. Contrasting these numbers might make senior management wholeheartedly continue with the continuity process. Suppose it costs \$1 million to recover a business function, but the company would lose \$1 million per day if it were unable to recover in a timely manner. Of course, the numbers are not always that simple, but that is why the BIA is so important: It gives the company some type of objective measurement to consider.

Recovery Strategies (2)

- Use your BIA.
- Minimum requirements:
 - Determine space needs.
 - Determine equipment needs.
- Start planning for continuity.
- No backup, no recovery.

All recovery strategies are driven by the maximum allowable downtime of a given business function and the resources required to continue to perform that function. At a minimum, planners should determine the necessary space and equipment needs for continuing the critical business process and their availability. It might be necessary to put agreements in place with vendors and suppliers to provide equipment, office supplies, services, and even personnel in the event of a disruption.

The disaster recovery plan enumerates all necessary information in the event of disruption, including (but not limited to) the location of the emergency operations center (EOC), directions to the EOC, the location of alternate recovery sites (also with driving directions), team members and all contact information, the procedure for handling the disruption, and the declaration and notification procedures.

In all cases, no matter what the recovery strategy is, you must have arrangements in place for the recovery of vital records—whether they exist in hard or soft copy. No backup, no recovery: the mantra of business continuity. Without backups, the business has no way of picking up where it left off.

Recovery Strategies (3)

- No strategy
- Self-service
- Reciprocal agreements
- Alternate sites:
 - Hot, warm, cold, hybrid, and mobile

Understandably, for certain business functions the cost of recovery might not be justified. A business function of this type is most likely low priority because it is not truly critical to the survivability of the corporation. You must use sound judgment, but do not be surprised if you find it reasonable to put no formal response in place.

A self-service strategy uses the corporation's offices to transfer or host disrupted business functions. Conference rooms, cafeterias, satellite offices, training rooms, even employees' homes might be equipped to temporarily support business functions. Given the scope of the disruption, this might or might not be a plausible strategy.

Reciprocal agreements involve making arrangements with other (possibly competing) companies that have similar needs to your own. Depending on your industry's specialization, there might only be a handful of businesses with unique operating needs. These needs might make it too cost-prohibitive to replicate business functions; therefore, by forming a reciprocal agreement, each company agrees to help the other in the event of a disruption.

We'll cover alternative sites next.

Alternate Sites

- Hot
- Warm
- Cold
- Hybrid
- Mobile
- Mirror
- Reciprocal (Mutual Aid Agreement)

Third-party continuity service providers offer many types of alternate sites, ranging from empty shells to full-fledged operation centers:

- **Hot sites:** Fully equipped and staffed facilities running 24/7 that intend to serve an organization that has sustained total disruption either through catastrophic failure or total physical destruction. A hot site is feasible for critical business functions that cannot tolerate any downtime.
- **Warm sites:** Descriptions vary for a warm site, but it is primarily a facility that is pre-equipped, but not necessarily ready to go. Business processes that can tolerate a few hours of downtime might be ideal candidates for a warm site; however, companies should fully investigate what they are paying for and what they are getting.
- **Cold sites:** The simplest and least responsive of the alternate sites, the cold site is simply an empty facility the company must equip in the event of disruption. Given that the response time of a cold site is in the order of several hours, if not days, it is debatable whether a cold site will meet the recovery requirements of a business.
- **Hybrid sites:** Hybrids combine multiple sites to afford maximum flexibility. For instance, although the average disaster recovery takes seven to ten days, recovering from truly catastrophic disaster might take six months or more. Buffering a hot site with a cold site allows you to gradually move to the cold site after your contracted time at the hot site expires.
- **Mobile sites:** Mobile sites are routinely identified as the up-and-coming alternate site because they provide almost the same capabilities as a hot site—but not quite. Depending on the type of disruption, a mobile site is akin to an "office on wheels" that you can locate conveniently near the company, thereby precluding extensive employee travel and personal issues such as daycare and special needs. Unfortunately, mobile sites can only realistically meet a 12- to 72-hour response time, depending on the proximity of the service provider who will deliver the mobile facility. Obviously, the closer the service provider, the quicker the response. Depending on the business functions' maximum allowable downtime, a mobile site might or might not be a viable option.

Temporary Help

- General office help
- Security and patrols

Unfortunately, some of the staff might be unavailable to help with the business recovery. Many of the staff will be working on recovery operations either at the original site or at the temporary location. Because they cannot be in both locations at the same time, extra staff might be required.

IT work is being outsourced, leaving a rich talent pool available in case of a disaster. Many temporary agencies can offer help. Your current staff must be able to work well with this group. It is best to interview these companies and their talent pool ahead of time, looking for the same business philosophy and then the same skill sets. Define the contract before the plan needs to be enacted, keeping an eye on level of service and the agency's ability to replace personnel instantaneously.

A temporary security force to protect a damaged site will protect the assets from theft and unwanted intrusions by such groups as the press. Security as a presence in the face of media attention will provide a sense of control where there might otherwise be none.

Loans versus Insurance

- Loans
 - Short term relief
- Insurance
 - Long term relief

In larger insurance settlements, two major issues occur that cause proper planning to fall apart: insurance payment negotiations and legal negotiations. Like all businesses, insurance companies try to maximize income and reduce expenses. Their major expense is paying settlements. If you have ever tried to place a claim against your personal insurance and have been rejected, you know the tactic of "deny the claim until legal action is imminent." When millions of dollars are at stake, insurance companies have it in their best interest to first deny, then litigate, and then finally settle. When they do settle, the first offer is typically much less than provided in the terms of the policy.

If your company is in a disaster situation, there might be great pressure on your organization to settle for less cash now.

What can be done?

1. Find an insurance expert who is not affiliated with your current insurance company.
2. Find an attorney who specializes in insurance contract law.
3. Look for loopholes in current insurance plans.
4. Negotiate with banks for disaster relief funds.

This last point is new for most banks. If your organization is in good standing with the bank, a short-term loan earmarked for "disaster only" can be negotiated. Expect the bank to wait up to 180 days for the payment schedule to begin. When a disaster happens, your institution needs cash to solve problems. When the insurance company offers less than the agreed-upon amount, you have the time to litigate and wait.

This is out of the BCP/DRP officer's realm, but by asking the questions of the business unit, you make great strides toward buy-in for your entire BCP/DRP plan.

Disaster Recovery Plan

- Steps and procedures
- Lists primary and alternate team members
- Current call tree
- Easily accessible, well-written, and logically organized

The disaster recovery plan is the corporation's immediate response to disruption. As such, it is a primary recovery strategy and is, itself, a critical business function because it ensures the company's ability to recover. The plan should include a list of all primary and alternate team members who are responsible for handling the crisis, specific and detailed steps that members should execute, and a current contact list (call tree) of all personnel and the functions they are qualified to perform.

Most notably, because the disaster recovery plan will be used by people under duress, the plan should be well-structured, clear, concise, and complete. The first draft of a plan might be none of these, which is why testing is so important in business continuity planning. As a purely academic process, business continuity planning is of limited use. Where the plan is worth its weight in platinum is how it is revised during the testing phase.

The structure of a disaster recovery plan might include the following elements:

- **Introduction:** The organization's goals and, in general terms, what it considers an emergency and the potential risk.
- **Emergency management team:** Who is on the emergency response team, contact numbers, roles and responsibilities, and alternate team members.
- **Emergency operations center:** Operational concept, location, driving directions to primary and alternate sites, availability of communications, communications protocols, and physical and logical layout.
- **Emergency notification procedure:** How the organization will be alerted to an event and the communications protocols for notifying internal and external entities, particularly relating to the news media. List contact information for all pertinent personnel and the conditions under which they will be contacted.

No Backup, No Recovery

- Frequency
- Availability
- Location
- Backups
 - Not real time
- Mirroring
 - Electronic vaulting
 - Real-time backup of data

Without backups, a company cannot recover... at least, not quickly. You must back up all vital records relating to a corporation and duplicate any hard copy. The archival process of backups allows a company to return to some specific time in the past and rebuild its business functions. The more backups are time synchronized with data as it is created, the quicker a corporation can recover from a disruption. The pinnacle of time-synchronized backups is called *mirroring*, otherwise known as *electronic vaulting*. Electronic vaulting provides real-time, or near real-time, backup of data through a network connection to an off-site facility. Not all business processes require electronic vaulting, but more companies are using it for even less time-critical data, primarily because of the simplified process of creating the backup.

As important as time is to backups, location is equally important. If a system's backups are destroyed, so too is the company's ability to recover. Storing backups off site increases the likelihood that backups will survive most types of disasters or emergencies. Storing backups within the same physical facilities as the company defeats the purpose of trying to protect your data.

The next consideration is the availability of backups when the time comes to recover a system. Will the backups be delivered to the company's primary or alternate site? How long will it take? Is delivery time guaranteed? Will a corporate representative pick up the backups? How long will it take to complete the backup process? Is that time within the maximum allowable downtime timeframe? Who will restore the system?

Steps to Business Continuity

- Project initiation
- Risk analysis and reduction
- Recovery strategies
- **Developing the continuity plan**
- Exercising and maintaining the plan
- Training and awareness

At this point, all the pieces of the puzzle are assembled, but what is the picture? That is entirely up to you. This section discusses the first draft of a business continuity plan, its contents, and format. Later revisions must include more information, such as plan maintenance and training goals.

Developing the Plan

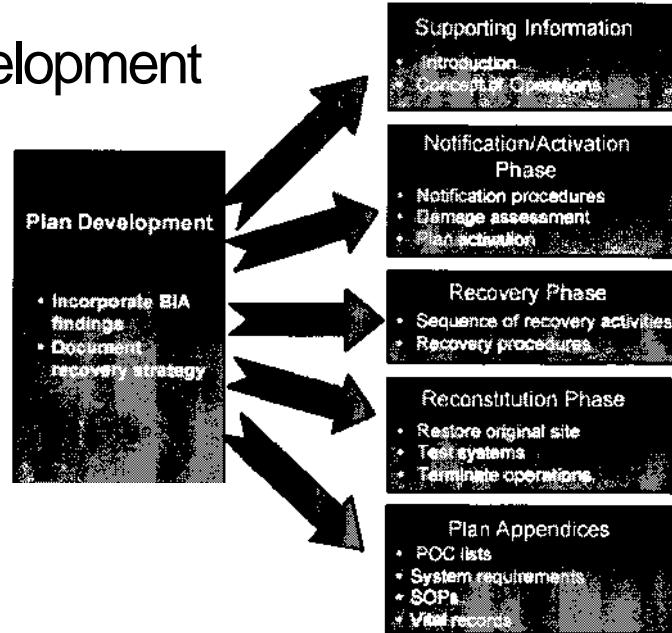
- Document your plans, strategies, and findings.
- Make the language terse, clear, and direct.
- Plan approval is a must.

Business continuity plan documentation is the end product of the process and is therefore terse and direct. Business continuity plans take on many forms and many different formats, but you can organize one as follows:

- **Introduction:** Explain why the plan is necessary and detail the scope of the plan, including who is part of the response and recovery process and the range of events addressed.
- **Crisis-management structure:** Include details about the roles and responsibilities of everybody involved.
- **Locations:** Document the location of the command center and the procedure for activating the center. Include the location of alternate and backup sites.
- **Procedures:** This section includes the alert procedure when an incident is first discovered, damage assessment, declaration procedures, notification procedures, and team procedures.
- **Exercise log:** Document the calendar date on which you tested the continuity plan, what type of test you conducted, and any shortfalls you encountered during the test (phone numbers that were out of date, a team member who no longer works at the company, and so on).
- **Revision history:** Document the date changes that were made to the document, the person who made the changes, which executive approved the changes, and the details of the change (for example: page 24, updated phone number for the IT manager).

The executive management team should sign off on the finalized plan. Although the business continuity plan is finished when the executive(s) signs it, it is far from complete. You must now flesh out the document's usefulness, removing any theoretical remnants and leaving only tested, certified, and accurate procedures for recovery.

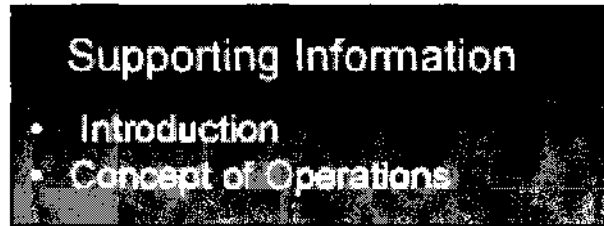
Plan Development



From SP 800-34, "IT contingency plan development is a critical step in the process of implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually the more detailed the plan is, the less scalable and versatile the approach. The information presented here is meant to be a guide; however, the plan format in this document may be modified as needed to better meet the user's specific system, operational, and organization requirements...

"Plans should be formatted to provide quick and clear direction in the event that personnel unfamiliar with the plan or the systems are called on to perform recovery operations. Plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used. A concise and well-formatted plan reduces the likelihood of creating an overly complex or confusing plan."

Plan Development Supporting Information

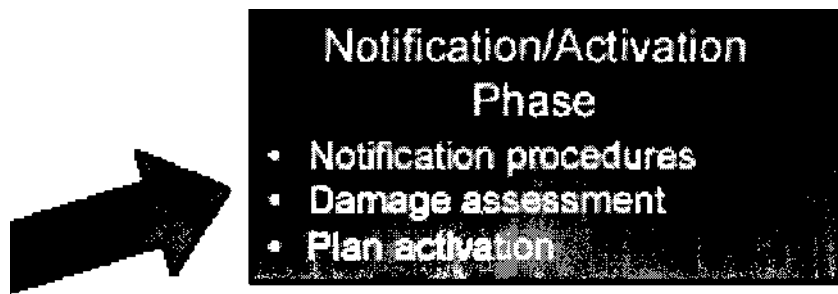


The planning and development stage includes the purpose, applicability, scope, references and requirements, and record of changes:

- **Purpose:** Establishes the reason for developing the contingency plan and defines the plan objectives.
- **Applicability:** Defines the parties affected by this plan. Any related documents are detailed here.
- **Scope:** Details the assumptions, issues, situations, and conditions discussed in the plan. It also defines the systems that are managed by this plan.
- **References/Requirements:** Identifies the legal requirements and governing institutions that impose conditions on the plan.
- **Record of Changes:** Contains issues of how change control is managed.
- **Concept of Operations:** Provides additional details about the IT system; the contingency planning framework; and response, recovery, and resumption activities.
- **System Description:** A general overview of the hardware and software systems.
- **Line of Succession:** Identifies personnel to assume authority in the event others are not available.
- **Responsibilities:** Details the teams' functions.

Plan Development

Notification/Activation



Notification/Activation Phase

The Notification/Activation Phase defines what triggers a declaration of action.

Notification Procedures:

Because we cannot determine the type of notice we will be given for an event, we assume that no notice will be given. At this point, documentation starts with damage assessment. Because some events cause us to use different communication channels, a checklist is appropriate. Each communication channel should be monitored regularly. A phone tree is one of the best tools for little cost. A global organization should consider an automated third-party phone tree. Whatever the technique for notification, it must be clear who to call. That information must be in the plan. The documentation should list team members, any other organizations, and the various points of contact.

Notification information should include the following:

- Nature of the emergency
- Loss of life or injuries

Damage estimates

- Response and recovery details
- Where and when to convene for briefing
- Relocation estimated time period
- Instructions to complete notifications using the call tree

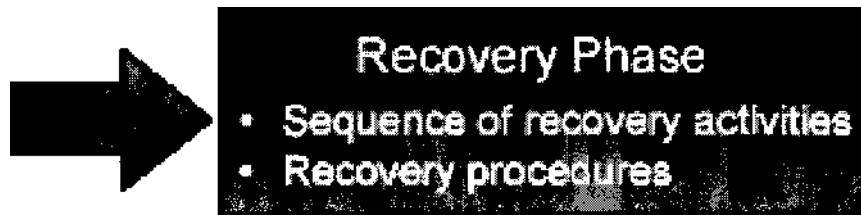
Damage Assessment:

This step might be unreliable, depending on the team member's experience. Quick, efficient, and safe are the major concerns in damage assessment. The damage assessment team is the first team that is notified of the incident. Documentation should include: the cause of the emergency or disruption, the potential for additional disruptions or damage, the area affected by the emergency, the status of physical infrastructure, the inventory and functional status of equipment, the type of damage to equipment or data, the items to be replaced, and estimated time to restore normal services.

Plan Activation:

The contingency plan should be activated when the damage assessment triggers have been achieved based upon some or all of the following: the safety of personnel, the extent of damage to system, the criticality of the system to the business objective, and the estimated duration of disruption.

Plan Development Recovery



Recovery Phase

The recovery phase has three categories of activities:

1. Execute temporary processing capabilities
2. Repair or replace
3. Return to original operational capabilities

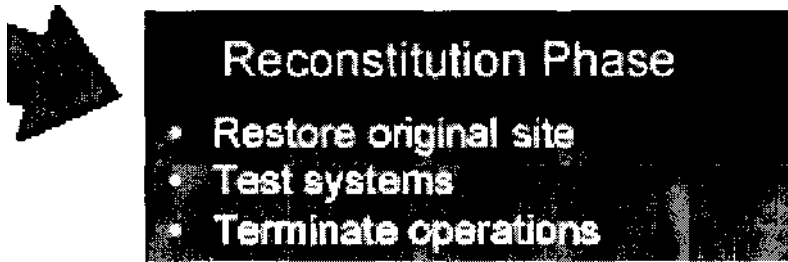
Sequence of Recovery Activities:

This order of activities follows business requirements of critical systems to return to production. Any critical, prerequisite supplies should be on hand to achieve the goal. For example, if you were to choose to use a manual system at an alternate location, you would need the supplies to be delivered first and the personnel transported second. It would do you no good to have staff without supplies.

Recovery Procedures:

Recovery procedures are the most time-consuming part of the plan to maintain. This section should be tested heavily. Recovery procedures are the step-by-step of how to return to an operational state. If you were a help desk support person, what kind of instructions does the help desk need to support 100 servers in running order with the proper software configured for the business? What would be the order of restoration from backup? What configurations would your telephone operator need for the phones? How do you test that the system is working properly? Checklists work well in this area.

Plan Development Reconstitution



Reconstitution Phase

The reconstitution phase consist of the return to the permanent facility, testing systems, and shutting down the temporary facility:

- **Return to permanent facility:**
If the original facility was destroyed, you might be resuming operations at a new location. Hopefully you can resume operations at the original site.
- **Test systems:**
Resuming at the permanent facility requires that you are able to cease BCP and go to "business as usual" mode. All systems must be verified, certified, or accredited depending on the regulatory bodies.
- **Shutdown temporary facility:**
It might seem simple, but the infrastructure set in place might be very costly to maintain. It will take time to break down the systems. You must also make assurances that the residual data at that site is disposed of properly.

If possible, each section of the reconstitution phase should have a team at each location.

Plan Development Appendices



Plan Appendices

Each section of the plan should be complete by itself, but it might not contain the step-by-steps of server restores or the phone list of every customer to call. This is the realm of the appendices. Follow the BIA to guide you regarding the requirements for your organization. Here is a list of common items that appear in the appendices:

- Contact information
- Vendor contact information
- Standard operating procedures
- Checklists for system recovery or processes
- Detailed equipment and system requirements lists of resources
- Vendor service level agreements
- Reciprocal agreements
- Alternate site information

Steps to Business Continuity

- Project initiation
- Risk analysis and reduction
- Recovery strategies
- Developing the continuity plan
- **Exercising and maintaining the plan**
- Training and awareness

There is a saying among scuba divers: "Plan the dive. Dive the plan." This refers to the necessity of forethought before conducting a diving expedition, and then sticking to the plan after it is implemented. Of course, mindless adherence to a plan is hardly a good characteristic, but this SCUBA saying is not referring to mindlessness. Executing a plan in a disciplined manner is far different than having no plan to execute. Discipline manifests itself by controlling the panic-prone mind in as appropriate a manner as possible, without unduly constraining team activities.

Without a plan, diving expeditions frequently fail — or worse, result in the loss of human life. Likewise, exercising and maintaining a business continuity plan controls the panic-prone mind when the organization is confronted with a disruption. In this section, we discuss the "freshness" of business continuity plans and how "freshness" relates to the company's survivability.

Exercising and Maintaining the Plan

- Validate the plan.
 - Pass or fail?
 - It either allows complete recovery or it doesn't.
- Work out the kinks now, not during an emergency.
- Make periodic or ad hoc reviews.

Confidence in the company's continuity plan can only be achieved through testing. Leaving the business continuity plan on a shelf somewhere, forlorn and forgotten, immediately vaporizes any value the plan might have initially possessed.

Testing verifies the accuracy of the recovery procedures and highlights any discrepancies or areas that were unintentionally overlooked during the plan's creation. Also, testing familiarizes personnel with the plan's objectives and provides the necessary preparation for quick, decisive response to disruption. Remember, "Plan the dive. Dive the plan."

In short, testing the business continuity plan provides the following:

- **Consistency:**
Testing ensures that there are few, if any, gaps between the plan and the organization's current characteristics. The organization's hierarchy, infrastructure (network), business processes (and maximum allowable downtimes), staffing levels, and vendor and outsourcing relationships should all be current and accurate within the document.
- **Validity:**
Testing ensures that the plan is still valid and that the assumptions contained therein are logical and practical. The question to be answered is, "Does the plan truly enable recovery?"

Testing and maintenance of the plan can happen periodically or on an as-needed basis. Periodic review consists of testing and reviewing the plan at specific times within the calendar year, either quarterly, bi-annually, or annually. Ad hoc review consists of testing the plan as needed or as warranted by executive decision-makers. Opinions differ about which method is better, but it is incumbent upon the company to make the investment in the business continuity plan worthwhile. The company is free to combine the two methods for optimum coverage.

In all cases, any time the company adds new business processes or upgrades/alters the infrastructure or makes any other modifications, you should review and update the business continuity plan. Preferably, test the plan within a reasonable amount of time to ensure that you can recover the new business processes or infrastructure. Remember that you should conduct BIAs to ensure that the company is responding to the right weaknesses.

Types of Testing

- Checklist
 - Consistency testing
- Structured walk-through
 - Validity testing
- Simulation
- Parallel
- Active simulation
- Full interruption

Checklist testing, also known as *consistency testing*, simply involves reviewing the business continuity plan to ensure that it addresses all critical areas of the enterprise and that the procedures to recover those areas are accurate and consistent. Checklist testing is the least expensive of all the testing methods; however, it is also the least valuable because it does not depict the company's responsiveness to disruption. Checklist testing is for sanity checking and should not be considered a viable testing method in and of itself.

Structured walk-through testing, also known as *validity testing*, ensures that the plan contains no errors, erroneous assumptions, or blind spots, and that it accurately reflects the company's ability to recover from disruption. Team members and other individuals who are responsible for recovery meet and walk through the plan step-by-step.

Simulation testing involves a mock emergency where team members respond as if an emergency is occurring. This test is really a structured walk-through test on steroids or at least some type of amphetamine. You may recover locations (including the emergency operations center and the alternate sites) and enable communications links while team members execute the recovery steps in a walk-through manner. You do not actually perform recovery actions (restore backups). This testing method can be expensive for a company, but in comparison to the following two testing methods, it can prove invaluable, and provide great service for the dollars spent. A simulation test is a satisfactory testing method because it gives the enterprise fairly good insight into its recovery responsiveness.

Steps to Business Continuity

- Project initiation
- Risk analysis and reduction
- Recovery strategies
- Developing the continuity plan
- Exercising and maintaining the plan
- **Training and awareness**

Finally, we address corporate training and awareness. Sometimes a corporation's first (and last) line of defense are the eyes and ears of its employees, yet nothing is done to train the eyes and ears to know what to look for (at least with any reliability).

Additionally, good training helps reduce panic that is commonly associated with crisis situations. This section discusses training and awareness and expands on "diving the plan."

Training and Awareness

- "Plan the dive. Dive the plan."
- Training promotes success.
- It is easy to become complacent.
- Key areas of training:
 - How to operate the alternate site
 - How to start emergency power
 - How to perform an restorative backup

A crucial aspect of the business continuity plan, training is often minimized because it takes employees away from their primary responsibilities.

An organization should and must train all staff in the recovery process. Recovery procedures might be significantly different from those pertaining to normal operations, and team members should feel confident in their ability to recover the company. Confidence is the driving factor in the plan's success, especially when employees are under duress. Training might include the following:

- How to operate the alternate site
- How to start emergency power
- How to perform an restorative backup

"Plan the dive. Dive the plan," is a SCUBA diver's saying about conducting a safe dive. A lot of effort and attention goes into a safe dive, but above all, the diver must execute the agreed-upon plan. It requires expertise with equipment, environment, and the diver's own personal limitations.

As a company, you are giving your team members the same expertise by providing training. Training also gives the team valuable feedback on the readiness and preparation of emergency response and recovery team members and the overall recovery process itself.

Most importantly however, a corporation cannot assume that all members of the response and recovery teams will be available or even alive. Training all employees (or a large subsection) increases the likelihood that individuals will be available when loss of life has drastically reduced the number of experienced individuals.

Top BCP/DRP Planning Mistakes

- Lack of BCP testing
- Limit scope
- Lack of prioritization
- Lack of plan updates
- Lack of plan ownership

Top BCP/DRP Planning Mistakes

A number of other mistakes are commonly, almost predictably, made in contingency planning:

- **Lack of BCP testing/over-reliance on BCP:**

Many companies believe that just having the BCP is enough. Without adequate updating and testing, the document is just a lifeless draft. Organizations that test their BCP consistently find areas that need improvement, and they often find critical flaws. The time to discover these is before a real disruption. "Practice makes perfect." If you need less expensive testing and do not want to perform it in-house, you can use off-site test facilities. Try simulating a disaster, as in a business simulation game. Pretend that something has happened and that certain resources are no longer available, and have your personnel (who are assumed available) walk through the plan.

- **Too limited in scope:**

An incomplete BCP does not address all of an organization's needs for recovery. The BCP plan should cover organizational processes and process dependencies, systems recovery, and the replacement of key personnel, if needed. The organization should continue to function throughout a disruption and beyond.

- **Lack of clear authority and process:**

In times of disaster, only partial staff might be available, and their level of empowerment might need to be significantly higher than normal. Definitions for when and under what circumstances a change in empowerment and processes should begin and end needs to be clear and unambiguous.

- **Lack of prioritization:**

There is a need to prioritize the key business processes. The risk is to prioritize less-than-critical processes rather than those that are crucial for business survival. This is a time for thoughtful evaluation and decisions.

- **Lack of plan updates:**

The BCP should be updated periodically, especially when there are significant system, business process, or personnel changes.

- **Lack of plan ownership:**

Someone with the power to lead, influence, prioritize, and organize the BCP is instrumental to the success of the program. This is true during planning and during the plan's execution.

Top BCP/DRP Planning Mistakes (2)

- Lack of communication
- Lack of public relations planning
- Lack of security controls
- Inadequate insurance
- Inadequate evaluation of vendor suppliers

- **Lack of communications:**

There is a need for clear and precise communication with all affected stakeholders of the organization: potentially employees, contract employees, vendors, business partners, customers, and shareholders. (This relates to public relations planning, which follows.)

- **Lack of public relations planning:**

Organizations often fail to consider public and investor relations to limit the perceived disaster impact. This can literally make or break the organization. Remember the Tylenol tampering scare several years ago and how the strong PR from that company turned a disaster into a marketing opportunity?

- **Lack of security controls:**

During the recovery process, security controls are sometimes disregarded; this results in a greater risk of exposure. Security controls might need to be altered and loosened during recovery. However, this should be a matter of conscious decision and empowerment that is built into the plan. Strict adherence to the security controls incorporated into the plan is vital during plan execution.

- **Inadequate insurance:**

Some organizations lack adequate insurance coverage and fail to support the filing of insurance claims. These inadequacies result in delayed or reduced settlements. The plan might lack appropriate processes for capturing losses and recovery costs, without which the organization might realize a loss greater than otherwise necessary.

- **Inadequate evaluation of vendor suppliers:**

Many companies poorly evaluate recovery products (hot site, cold site, and planning software), relying on vendor-supplied information. This often leads to a solution that might not adequately address a company's needs.

Use these examples of common mistakes as a checklist to review your organization's contingency planning: the documentation, testing, integration with organizational processes and personnel, and so on. There are companies and consultants that specialize in designing and implementing business continuity plans. As appropriate for your organization, you may wish to consider their services.

Configurations to Protect and Document

- Desktops
- Server
- Web sites
- LAN/WAN
- Remote access
- Distributed systems

Documentation is often overlooked or simply not done because it's "too time consuming" or technicians and managers "... have other things to do." Some senior engineers have even said that documentation was unnecessary because they "know the system inside and out." Unfortunately, if the person who is most familiar with the system is unavailable due to death, illness, weather, or even just a job transfer, other engineers might have to resort to building the system from scratch if no documentation exists. For example, an organization recently undergoing a vulnerability assessment was proud to have eliminated single points of failure from their network. They had their Microsoft engineers cross trained to ensure that their vital applications would remain functional. Unfortunately, they neglected to cross-train anyone on the routers or the Unix systems. When their Unix engineer left unexpectedly, they suddenly realized that they were left with little information about several vital components. Luckily, they were able to document the configurations before an outage occurred. This example provides a strong case for a proactive change management system. Fully testing and documenting changes to systems allows engineers to easily and quickly recover or rebuild systems when they fail.

Each level of the network must be protected and the configuration documented to provide "defense-in-depth." Many small to mid-sized companies believe that they are secure if they implement a firewall and antivirus software on their desktops, but they have not considered the full range of threats that could affect their operations. All network components must have some measure of security commensurate with the threats against those assets.

Desktops and Portable Systems

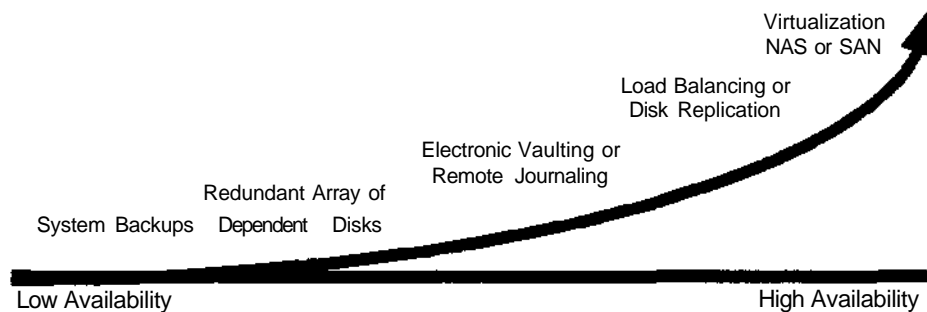
- Backups.
- Standardize hardware, software, and peripherals.
- Coordinate with security policies and system security controls.

Desktops and Portable Systems

In today's world of sub \$400 systems, imaging software, and 8:00 AM overnight delivery, you can push the damaged PC off the desk and start over. Here are a few considerations, assuming that you have systems that need to be restored:

- **Store backups offsite:**
Well-documented system configurations ease recovery. Backup media should be stored offsite in a secure, environmentally controlled facility. Balance media cost with the cost of systems data and duplication of work, not with duplication of parts. Backup procedures must also contain vendor contacts and agreements, software licenses, and system information.
- **Encourage individuals to back up data:**
Realizing that this is not a reality in most operations, education might help for critical data on laptops. Give personnel simple procedures with step-by-step instructions.
- **Standardize hardware, software, and peripherals:**
Repeatable builds on both hardware and software speeds resumption of service to the end user.
- **Coordinate with security policies and system security controls:**
All systems must incorporate issues of the data's confidentiality into the backup and restore plan. For example, if backups of laptops are not stored securely, could this compromise the entire enterprise?
- **Equipment interoperability:**
All backup devices and tapes should work if they are installed on similar hardware.
- **Media life:**
Certain backup media are only good for a limited number of uses; take this into account when choosing a systems strategy.

Server Availability



Server Availability

Servers and the services they provide have some of the same contingencies. When adopting a contingency plan, think of how many people are affected by the loss of the service and the cost of lost productivity. Server contingency planning must emphasize the availability of the network services provided by the server.

The following are key issues to address when securing servers:

- Store backup media and software offsite.
- Standardize hardware, software, and peripherals.
- Document system configurations and vendors..
- Coordinate with security policies and system security controls.
- Consider RAID systems for fault tolerance.
- Consider electronic vaulting and remote journaling.
- Balance server loads.
- Consider network-attached storage (NAS).
- Consider a storage area network (SAN).

Transaction Redundancy Implementations

- Electronic vaulting
 - Batch process
 - Transmitting data through communication lines to storage on a remote server
 - Example: performed every evening at a specific time
- Remote journaling
 - Transmitting data in real-time or near real-time to back-up storage at a remote location
- Database shadowing
 - Similar to remote journaling
 - Provides additional robust backup by storing duplicate data on multiple remote storage devices
- Disk duplexing
 - Disk controller duplicated
 - If one controller fails, other controller operates

There are many approaches that are used to backup databases. One is done in near real time (journaling) and one is done in batch mode (vaulting), usually at the end of the day.

In remote journaling, data is available at the backup at any time and provides a high degree of fault tolerance in the event of a disaster.

Note that disk duplexing does not denote multiple disks as backups, but multiple disk controllers.

Web Sites

- | | |
|---|---------------------|
| • Store backup media and software offsite | RAID |
| • Standardize | Electronic vaulting |
| • Document configurations | Load balancing |
| • Coordinate security policies and system security controls | NAS |
| | SAN |

Web Sites

Web sites present information to the public or internal personnel. In some cases, the Web site might be the main focus of the business, as for Amazon or eBay. In other cases, the Web site projects a company's image to the public. Damage to the reputation can cause just as much damage as a physical disaster. Therefore, in addition to all the items listed on the server, you must take the following actions:

- **Document the Web site:**
Document the hardware, software, and their configurations.
- **Review Web site programming and coding:**
The code review process should examine the Web site for static information such as "hard-coded IP addressing." Removal of any static information increases the speed of restoration to new systems.
- **Provide for load balancing via DNS:**
One common DNS approach is the "round robin" method for redundancy. In this case, the DNS server can point to another Web server if the primary server goes down.

Local Area Networks

- LAN
- PSTN
- Leased lines
- Documentation

Local Area Networks

Public switched telephone networks, leased lines, and the local media and connection devices are included in LAN technologies. The following practices should be considered:

LAN Documentation:

The physical and logical LAN diagram should be up-to-date. The greater the detail, the easier the restoration process.

System configuration and vendor information documentation:

Document configurations of network connective devices such as routers, switches, bridges, and hubs. These configurations should be a part of the normal backup procedure and should be stored as such.

Coordinate with security policies and security controls:

LAN contingency solutions must include re-implementation of security measures such as firewalls and intrusion detection systems.

Wide Area Networks

- Dialup
- T1
- Frame relay
- ATM
- SONET
- ISDN
- Wireless
- Documentation
- Systems configuration
- Redundancy

Wide Area Networks

Each of the above services for communication must be part of the contingency policy.

Document the WAN:

The WAN architecture diagram should be kept up-to-date and should identify network connecting devices, IP addresses, and types of communication links and vendors. This "Network Map" must be kept under tight security at all times. Do not post it in plain sight.

The following are critical things to do to protect your network:

- Document systems configurations and vendors
- Create redundant communications links
- Have redundant network service providers
- Use redundant network connecting devices
- Expect redundancy from Internet service provider

Distributed Systems

- Standardize hardware, software, and peripherals.
- Document systems configurations and vendors.
- Coordinate with security policies and security controls.

Distributed Systems

Today, distributed systems are more widely used in large companies. Most examples are in databases and e-commerce solutions. Because the distributed system relies extensively on local and wide area network connectivity, distributed system contingency measures are similar to those discussed for LANs and WANs.

The following are key things to address when securing distributed systems.

- Standardize hardware, software, and peripherals.
- Document systems configurations and vendors.
- Coordinate with security policies and security controls.

Threats to BCP/DRP

- Lack of management support
- Lack of business unit support
- Lack of change control
- Lack of funds
- Poor updates

This slide shows internal threats to implementing a quality BCP/DRP.

IT managers and engineers cannot implement a successful BCP/DRP without upper management's support. They need proper funding and often a high-level champion to facilitate participation, planning, and training by other departments within the organization. BCP/DRP must be a priority of the IT department and the organization as a whole; and it must be adequately funded.

Previously we discussed the importance of change control and how lack of documentation can adversely impact a network. In addition, lack of control over the changes can cause problems. You are probably aware of the debate surrounding wireless networks. Imagine the frustration of a security manager who finds out that all the work he has done to secure proprietary information on the corporate network is negated because several departments have independently installed wireless access nodes on their floors and the configuration does not use even the basic encryption settings. The entire network is now vulnerable.

Poor updates can refer to plan or security measure updates. Changes to the threat profile might require changes to configurations to maintain the current security level. How many times have you seen articles about a company that failed to implement new security patches or antivirus updates that had been released weeks before the incident? Just as virus lists and software patches must be updated, a BCP and DRP must be examined and routinely updated to be successful.

BCP/DRP Summary

- BCP should be mapped to critical assets and actions to reduce risk.
- All critical assets and corresponding servers should be prioritized.
- Plan for the worse and hope for the best.

You should now understand how critical contingency planning is to your organization's security policy and how you can go about doing it. We identified components of business continuity plans and disaster recovery plans, and then walked through the BCP/DRP planning process lifecycle, which is an ongoing process. Fortunately, considerable information is available on the World Wide Web and from vendors on this subject if you would like to read further.

This page intentionally left blank.

9. Regulations and Compliance

10 Domains of Knowledge

This section covers Domain 9, the Law, Investigation, and Ethics domain.

9. Regulations and Compliance

- Code of ethics
- Regulatory
- Criminal law
- Civil law

It is important to note that incident handling plans, policies, and procedures must comply with the applicable laws of your state or province and country. Globally, there are many different legal systems, but the two most common are Common Law and Civil Law. Common Law was developed in England hundreds of years ago and is also practiced in the United States, Australia, and parts of Canada. Civil Law, on the other hand, was developed in France and is practiced in Canada, primarily Quebec. Both legal traditions are quite similar with the primary difference being the terminology associated with each. Generally speaking, any concept found in Common Law is usually present in Civil Law, but the wording may be slightly different. As is the case with most things, laws constantly change and evolve over time. For example, in the United States, common laws were modified when the Federal Rules of Evidence were first enacted in 1975 and again in 2001.

Ethics

- Ethics bodies
- Ethical dilemma
- Ethics as a process

Ethics is defined as:

1 the discipline dealing with what is good and bad and with moral duty and obligation
2 a: a set of moral principles or values b: a theory or system of moral values <the present-day materialistic *ethic*> c *plural but singular or plural in construction*: the principles of conduct governing an individual or a group professional *ethics*> d: a guiding philosophy

Ethics is the field of study that is concerned with questions of value—judgments about what human behavior is "good" or "bad" in any given situation. Ethics are the standards, values, morals, principles, and so on, that are used to guide one's decisions or actions; often there is no clear "right" or "wrong" answer.

Source: <http://www.m-w.com/cgi-bin/dictionarv?book=Dictionary&va=ethics>

Ethics Bodies

- Internet Activities Board (IAB)
- Computer Ethics Institute
- Association for Computing Machinery (ACM)
- Australian Computer Society
- The Institute of Electrical and Electronics Engineers, Inc.(IEEE)
- Information Systems Audit and Control Association (ISACA)
- International Information Systems Security Certification Consortium, Inc. (ISC)²

This list is by no means exhaustive. The list in the slide represents national and international organizations. Each group provides a guiding philosophy (a set of canons) to follow when a member does not know how to act. Most organizations have a process to review actions taken by its membership. Some have an ethics officer, who can be approached about "gray" area issues. Other organizations have peer review boards. CISSPs can post to their private forum and get feedback on current dilemmas. Peer review boards can be harsh critics, so be prepared to clearly state: the section of the ethics code you are interpreting, the situation sanitized for the group's review, and your current view. It is good to have your peers judge or criticize your actions and interpretations; but it takes a thick skin. Most people are not willing to place themselves under this level of scrutiny. If you are not, then ask yourself, do I feel guilty or dishonest? Maybe you have answered your own ethical question...

This is a list of the URLs where individual codes of ethics can be found as of 2003-10-01:

- <ftp://ftp.rfc-editor.org/in-notes/rfc1087.txt>
- <http://www.cpsr.org/program/ethics/cei.html>
- <http://www.acm.org/constitution/code.html>
- <http://www.acs.org.au/national/pospaper/acs131.htm>
- http://www.ieeeusa.org/DOCUMENTS/CAREER/CAREER_LIBRARY/ethics.html
- http://legacy.eos.ncsu.edu/eos/info/computer_ethics/basics/principles/
- http://www.isaca.org/Content/ContentGroups/Standards2/Standards_for_Information_Systems_Control_Professionals/4927standards-booklet.doc
- <https://www.isc2.org/cgi/content.cgi?page=31>

Ethics: ISC²'s "Code of Ethics"

Protect society, the commonwealth, and the infrastructure.

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

This code of ethics is fairly straightforward. It should not be taken lightly. Even though at first glance it seems very straightforward, there are still several terms that are open to interpretation. For example, depending on background and perspective, different people can argue what a high standard of moral or ethical behavior is. People do things all of the time that I do not think are ethical and when I question them, they strongly disagree.

The first section of the code of ethics is:

- **Protect society, the commonwealth, and the infrastructure.**
- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Ethics: ISC²'s "Code of Ethics" (2)

Act honorably, honestly, justly, responsibly, and legally.

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

The second section of the code of ethics is:

- **Act honorably, honestly, justly, responsibly, and legally.**
- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Ethics: ISC²'s "Code of Ethics" (3)

Provide diligent and competent service to principals.

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

The third section of the code of ethics is:

- **Provide diligent and competent service to**
- **principals.**
- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Ethics: ISC²'s "Code of Ethics" (4)

Advance and protect the profession.

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

<https://www.isc2.org>

The fourth section of the code of ethics is:

- **Advance and protect the profession.**
- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.
- <https://www.isc2.org>

Ethics: Internet Activities Board (IAB)

What not to do:

1. Seek to gain unauthorized access to the resources of the Internet.
2. Disrupt the intended use of the Internet.
3. Waste resources (people, computer, and capacity) through such actions.
4. Destroy the integrity of computer-based information, and/or compromise the privacy of users.

As security professionals, we are entrusted with protecting our information infrastructure. We have a fiduciary responsibility to the public to allocate government resources wisely and effectively. These tend to be strong statements, but they do not speak to intention. Intention is important because people tend to justify their own actions in their minds. For example, if someone breaks into a site and you take matters into your own hands and attack that person, gain access to their system, and crash their boxes, is there anything wrong with that? The short answer is yes. Read 1 and 4 again. It is not your job to enforce the rules of the Internet, and in doing so, you might actually attack the wrong systems and cause damage to an innocent bystander. If that occurs, then you definitely have crossed the ethical line.

Ethics:

Computer Ethics Institute

Ten commandments:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.

In addition, there might be legal guidance about what you can and cannot look at in an individual's computer system. Some people believe AOL's Instant Messenger is unethical (it uses company resources). Again, intent is at the core of the ethical issue.

Most of these items are fairly straight forward and map to other ethical items we discuss.

Ethics: Computer Ethics Institute (2)

6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources.
8. Thou shalt not appropriate other people's intellectual output.
9. Think about the social consequences of the program or system you design.
10. Use a computer in ways that ensure consideration and respect for your fellow humans.

Here are some ethical dilemmas for you to consider:

If I intend my program for good and you use it in an unethical manner, am I at fault? What if you copy software that you think your company has a license for. Would you use the software? If you did not ask whether you had a legal copy and made that assumption, are you operating outside the ethical boundary? What if someone told you that you did have a license, but they were not telling the truth? How far do you have to research something to make sure you are covered from an ethical standpoint?

Ethics: Standards

The information systems security manager needs to understand what *motivates* people to behave in an unethical manner in the information age and the environment conducive to computer crime, misuse, and fraud. A good manager can create an environment that will discourage computer abuse and promote ethical behavior.

Any company and manager needs to minimize ethical dilemmas for their employees. A company must avoid potential conflict-of-interest scenarios because these scenarios can lead to ethical issues at a later point. As an example, if I currently work onsite at another company and the company I work for just won a penetration test against that same company, not only should I not be allowed to work on that contract, but I should not be allowed to talk to anyone on the penetration test team. Otherwise, I might be put in an ethical dilemma whereby I want to help my company, but I might reveal information that I should not reveal.

Ethics: Standards (2)

Computer hardware and software vendors, service contractors, systems developers and maintainers, system managers, and system users all have an **EQUAL ROLE** in sharing ethical responsibilities.

If a software or hardware vendor produces a piece of software or equipment, they put it through testing and release it, and there is a vulnerability in the design that allows it to be exploited, is the vendor operating in an unethical manner? Most people would say that if the company released a patch in a timely manner, they were acting in an ethical fashion. However, you can see that there are several shades of gray when handling ethics.

Ethics: Standards (3)

The key issues involved in information ethics are:

- Software piracy
- Data security and individual privacy
- Data integrity
- Human/product safety
- Fairness, honesty, and loyalty

Because ethics are not always black and white, there are certain standards or tests you can use to make sure that what you do is ethical. The following are some of the areas you should be prepared to confront:

- **Software piracy:** Taking someone else's software without paying for it or asking for permission.
- **Data security and individual privacy:** Doing anything that violates someone else's personal privacy.
- **Data integrity:** Modifying information in a way that deliberately gives someone false information.
- **Human/product safety:** Causing harm to someone directly or indirectly through the use of a product.
- **Fairness, honesty, and loyalty:** Making sure you treat everyone in a fair and honest manner

Two key things come into play. First, there are situations in which unethical behavior is illegal. Second, there is a fine line delineating good business decisions and negotiation techniques and ethical behavior.

Ethical Dilemma

- If you have ethics, do you need a governing body?
- If you do not have ethics, does a governing body do any good?
- If you had ethics when you joined the governing body, and your ethics have eroded over time, would you resign?

Are the following okay? Would you do any of the following?

- Go to a fake interview to collect competitive information?
- Hire someone away from a competitor?
- Overhear the conversation of a competitor?
- Pick plans from a competitor's trashcan?
- Pick up plans that fell out of a competitor's briefcase?
- Look at plans on a competitor's desktop?
- Take a customer list from a competitor's file cabinet?
- Blackmail someone to get a competitor's information?

Where do you draw the line between good business practice and ethical behavior?

Laws

Laws, directives, and regulations do not normally provide detailed instructions for protecting computer-related assets. Instead, they specify requirements, such as restricting the availability of personal data to authorized users.

Laws, directives, and regulations do not normally provide detailed instructions for protecting computer related assets. Instead, they specify requirements, such as restricting the availability of personal data to authorized users.

The following is an article that highlights these critical points.

http://news.com.com/2010-1022_3-5129350.html

December 19, 2003

By Charles Cooper

After a run of corporate scandals at companies such as Enron, WorldCom, Arthur Andersen, Tyco, and others, Congress enacted the so-called Sarbanes-Oxley bill in 2002.

The intent was to remedy the U.S. accounting system, which had allowed corrupt managers to take advantage of gaping holes. The new law now holds senior executives and directors of public companies responsible for the preparation and approval of their business's financial statements.

Although the final verdict on the law won't be in for several years, this much is clear: If a CEO gets caught with his or her hand in the till, Sarbanes-Oxley makes sure that there's a comfy jail cell waiting in a federal penitentiary somewhere.

There's a lesson here for the debate over how best to proceed on cyber security: Whatever its imperfections, the lesson of Sarbanes-Oxley is that if you want results, scare the hell out of 'em.

Computer Fraud and Abuse Act

- Amended in 1996
 - FIC (federal interest computers)
 - Covers altering, damaging, or destroying information
 - Computer passwords
- Original Law
 - Classified information
 - Financial information
 - Government computers
 - Unauthorized access

The Computer Fraud and Abuse Act is the base law from which most other computer crime laws have been derived. There was the original law and then an amended version in 1996.

U.S. Privacy Act of 1974

- Protects personal information
- Allows for the updating of inaccurate information
- Establishes criteria for classification

The U.S. Privacy Act of 1974 provides for the protection of personal information maintained in federal information systems and grants access to such information by the individual. The law establishes criteria for maintaining the confidentiality of sensitive data and guidelines for determining which data is covered.

U.S. Computer Security Act of 1987

Requires federal agencies to identify sensitive systems, conduct computer security training, and develop computer security plans.

The U.S. Computer Security Act of 1987 is a broad effort to get federal agencies to better protect the information that resides on federal computers. The first step is that an agency has to develop criteria that they can use to identify sensitive information that resides on their computer system. It is important to note that they are dealing with sensitive information—not just classified information. After the critical information has been determined, the agency then needs to build a plan around how that information will be protected through security training and reviews.

FOIA

Freedom of Information Act:

This law makes federal information readily available to the public. It also establishes the conditions under which information can be withheld from the public to ensure that certain information, such as trade secrets, is protected.

The Freedom of Information Act (FOIA) makes information that is kept on federal computers available to the public. Access to this information is given based on a determined set of criteria. For example, classified information cannot be given away to the public. This would defeat the reason why there is classified information. FOIA is the law that determines the rules and criteria for what information can be withheld from the public. Anything that is not withheld is made available. Notice the stance taken here. Instead of saying nothing is given except what we allow, it states that everything is given to the public except what we prohibit based on a set criteria.

SAFE

Security and Freedom Through Encryption (SAFE) Act:

- Guarantees the rights of all U.S. citizens and residents to use or sell any encryption technology
- Note that the bill specifies legal, not illegal use of encryption

Especially when we get into laws, the government loves acronyms. SAFE stands for the Security and Freedom Through Encryption Act. This law deals with the use of encryption. When dealing with encryption, there are three general types of laws that apply. The use of encryption within a country, the importing of encryption, and the exporting of encryption. This law deals with the internal use of encryption in the U.S. The law allows every citizen to use encryption technology to protect their information. The other important point is that it says everyone has the right to use encryption, but it does not mention whether the government has a right to escrow keys and read the encryption.

HIPAA

Health Insurance Portability and Accountability Act (HIPAA) of 1996:

- Originally called Kennedy-Kassenbaum Act
- Five topics of focus:
 - Consumer control of medical information
 - Limitations on use of PHI by healthcare industry
 - Fines for breach of confidentiality
 - Control of health-care fraud and abuse
 - Security against deliberate or inadvertent misuse or disclosure

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 says its goal is "to improve portability and continuity of health insurance coverage in the group and individual markets; to combat waste, fraud, and abuse in health insurance and health care delivery; to promote the use of medical savings accounts; to improve access to long-term care services and coverage; to simplify the administration of health insurance..." Aug. 21, 1996 [H.R. 3103]

In the past, the healthcare industry has focused on availability and integrity, leaving confidentiality a very distant third. To reduce competition, healthcare insurance companies have created a complex, costly system that makes translation from one company to another very difficult. HIPAA seeks to fix both of these issues in a continual improvement process. The part that CISSPs tend to ignore is the "P" for portability. It is often mislabeled as "P" for privacy. That privacy is extended to all PHI (Patient Healthcare Information) or data. The key "P" is that HIPAA requires all healthcare providers to adopt a common set of codes (making the information more portable) for describing medical technologies, drugs, procedures, and all other aspects related to the medical profession. The part of HIPAA that CISSPs tend to focus on is the "A," or accountability.

Summary of the Law

There are five topics of focus:

- Consumer control of medical information
- Limitations on use of PHI by healthcare industry
- Fines for breach of confidentiality
- Control of health-care fraud and abuse
- Security against deliberate or inadvertent misuse or disclosure

USA Patriot Act

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT):

-Changed the following laws

- . Wiretap Statute (Title III):
- Electronic Communications Privacy Act
- Computer Fraud and Abuse Act
- Foreign Intelligence Surveillance Act
- Family Education Rights and Privacy Act
- Pen Register and Trap and Trace Statute
- Money Laundering Act
- Immigration and Nationality Act
- Money Laundering Control Act
- Bank Secrecy Act
- Right to Financial Privacy Act
- Fair Credit Reporting Act

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism is also known as USA PATRIOT Act. According to the U.S. Congress, "The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. It vests the Secretary of the Treasury with regulatory powers to combat corruption of U.S. financial institutions for foreign money laundering purposes. It seeks to further close our borders to foreign terrorists and to detain and remove those within our borders. It creates new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists."

The bad news is that Congress gave broader power to law enforcement at the expense of 12 major pieces of legislation. Further, they gave the budget to law enforcement to help seek out terrorists. The good news is, this power has a time limit.

Source:

<http://fpc.state.gov/documents/organization/10092.pdf>

The USA PATRIOT Act introduced sweeping changes to 12 U.S. laws. This loss of privacy has some people worried. Section 224 is the Sunset Provision. It states that sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, will expire on December 31, 2005. Therefore, if Congress feels that these powers need to be rescinded, they do nothing. Some of these sections are being extended in the current 108th Congress.

Source:

<http://www.epic.org/privacy/terrorism/usapatriot/>

GLBA

- Gramm-Leach-Bliley Act
- Financial Modernization Act of 1999
- Enhanced Glass-Steagall Act
 - Hard dollar limits for small banks
- Increases privacy and security

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act," is a law to change the way the banking industry is regulated and updates certain capabilities. Smaller banks were limited by hard dollar limits from the Glass-Steagall Act. The key element for security professionals is the reporting and protection sections that help protect individual information. Simply, GLBA increases privacy and security of banking customers.

DMCA

- The original intent of the Digital Millennium Copyright Act (DMCA) was to fall in line with Article 20 of the Berne Convention for the Protection of Literary and Artistic Works.
- Title V, the "Vessel Hull Design Protection Act"

The Digital Millennium Copyright Act (DMCA) covers a broad range of copyright rules and regulations relating to almost every conceivable incarnation of literary and artistic works that come in contact with the digital medium. The original intent of the DMCA was to fall in line with Article 20 of the Berne Convention for the Protection of Literary and Artistic Works. The Berne Convention was managed by the World Intellectual Property Organization (WIPO). The idea is to protect intellectual property rights equally throughout the world. As in any endeavor encompassing such a large diverse group, compromises were made. Many people complain that the DMCA is unfair to scientists and academic types.

Source:

- [http://www.gseis.ucla.edu/iclp/dmcal .htm](http://www.gseis.ucla.edu/iclp/dmcal.htm)
- <http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281> .ENR:

Economic Espionage and Protection of Proprietary Economic Information Act of 1996

The Act addresses the problem of industrial and corporate espionage work. It allows the FBI to investigate cases in which a foreign intelligence service attacks American firms.

With the end of the Cold War, a lot of foreign countries are changing their focus. Money that was once spent spying on other countries is now spent spying on foreign companies that compete with local companies. Several countries have publicly acknowledged that this is occurs. In response to an increase in corporate espionage attacks against U.S. companies, the Economic Espionage and Protection of Proprietary Economic Information Act of 1996 was created. It essentially gives the FBI jurisdiction and responsibility to investigate corporate espionage attacks involving a foreign intelligence service.

International Laws

- Lack of universal cooperation
- Differences in interpretations of laws
- Outdated laws against fraud
- Problems with evidence admissibility
- Extradition
- Low priority

Cases are easier to deal with when the crime took place in the U.S. and the person who committed the crime and the victim are in the U.S. The reason for this is that there is a central body of law and law enforcement that is involved in prosecuting the case. When either the person who committed the crime, the victim, or the actual crime is not in the U.S., the case is more difficult. Based on many laws, the actual legal action could take place in another country and be bound by the local laws of that country. These laws can be quite different than U.S. laws. Even more interesting is that what is illegal in the U.S. might actually be legal in another country.

International Computer Crime

Key international efforts dealing with computer crime:

- United Nations (UN)
- The G8 Nations
- Mutual Legal Assistance Treaties (MLAT)
- European Union Border Controls (Interpol)

The following are key international efforts dealing with computer crime

- United Nations (UN)
- The G8 Nations
- Mutual Legal Assistance Treaties (MLAT)
- European Union Border Controls (Interpol)

Laws:

International Differences

- The Pacific Rim
 - Patent Law: Japan, Taiwan, Korea, and Thailand are all silent on the issue of patentability of computer programs.
 - Copyright Law: Under Japanese law, both source code and object code are copyrightable.
 - Trade Secret Law: Japan is the only Pacific Rim nation whose law provides for trade secret protection.

One of the big differentiators among countries is the law. Every country has different laws, different interpretation of the laws, and different ways to enforce them. In some extreme cases, there are some laws that are the same in all countries. For example killing another individual is illegal and against the law basically around the world. However, issues around computer-related crime are more vague and less defined. Some countries do not have special laws on computer crimes and use their traditional laws. Other countries are just silent, which means they allow the behavior to occur. This slide shows some of the differences for Pacific Rim countries.

Laws: International Differences (2)

- Western Europe
 - Computer software might be protected under patent law in addition to copyright law.
 - Trade Secret Law: Computer software is protected by trade secrets in European community member nations.

Although not always true, the countries that seem to have laws that are the closest to the United State are in Western Europe. Their laws on intellectual property are similar to ours with regard to patent and copyright protection. In Western Europe, computer software can be protected by both a patent and a copyright. There are also some limited laws on the protection of trade secrets.

Laws: International Differences (3)

- Latin America
 - Patent Law: In Argentina, software was not known or considered. Brazilian law, hardware is known, software is not.
 - Copyright Law: Mexican law now includes computer programs as a category of protected work.
 - Trade Secret Law: Brazil and Argentina have no specific protection. Mexican law generally protects industrial secrets.

In Latin America there are very few laws protecting software. In most of these countries, hardware has more protection than software does. This is slowly changing, but currently the software laws in Latin American countries lag behind the U.S.

Laws: International Differences (4)

Bottom line:

Not all countries play by the same rules.

At the end of the day, if you deal with protecting intellectual property outside of the U.S., get a lawyer. Even within the United States these laws can be very confusing, so consult an expert before you make critical business decisions. The bottom line is that when you deal with entities outside of this country, make sure you remember that they are probably not playing by the same rules that you

Privacy and Other Personal Rights

- The Federal Privacy Act
 - Government files open to public unless specified
 - Act applies to executive branch only
 - "Record" = information about an individual
 - Must be a need to maintain records
 - Disclosure prohibited without consent
 - Requirements on government agencies
 - Record disclosures
 - Public notice of existence of records
 - Ensure security and confidentiality of records

For the government to function, it must maintain records on individuals. The Federal Privacy Act is meant to keep information on individuals private and protected. Any information that is kept on a person cannot be revealed or disclosed without their consent. This is why if you apply for a loan or get hired at a company, you have to sign a waiver that says the company is allowed to obtain personal information about you. In addition to controlling the access, you as an individual also have a right to know what information is kept on you. You can fix errors that might exist in that information.

Privacy and Other Personal Rights (2)

- State Acts and Regulations
 - Fair Information Practices Acts: Define information that can be collected
 - Uniform Information Practices Code: National Conference of Commissioners on Uniform State Laws: recommended model
 - Statutes regulating information maintained by private organizations: Healthcare, insurance, and so on

There is a fine line between public and private information. To put it another way, there is a fine line between what can be collected and used by outsiders and what is not allowed. In an effort to clarify this, various laws have been passed to address the issues. The Fair Information Practices Acts define what type of information can be collected. It is always important to carefully read them. It does not state what information cannot be collected; it just says what information can be collected. There is a lot of debate about whether or not something that is not listed can still be collected. This is the most general law, but there are also specific laws for certain industries or companies doing working in specific areas.

Privacy and Other Personal Rights (3)

- Other Employee Rights
 - Electronic Mail: Expectations of privacy
 - Drug Testing: Limited to sensitive positions only
 - Freedom from hostile work environment
- International Privacy
 - European statutes cover both government and private corporate records
 - Application primarily to computerized data banks
 - Strict rules on disclosure
 - Prohibitions of transfer of information across national boundaries

Another principle that is important to understand when talking about law is expectation of privacy. Expectation of privacy states that with a certain piece of information there is an assumed expectation that this information is private. If there is, then if a company is not going to make it private they must put measures in place to inform the employee that the information is not private. If there is not an assumed expectation of privacy then it is assumed the information is public information or in the public domain and can be used without notification.

International policies on this can be quite different; so if you have remote offices in other countries, you should validate the law in those areas of interest.

Privacy and Other Personal Rights (4)

- Management Responsibilities
 - Regular review with legal department
 - Consider all jurisdictions
 - Prepare policies for compliance
 - Enforce policies
 - Document enforcement

When you look at an organizational chart, you have to remember who has what responsibility. Although an employee should have a basic understanding of the law, it is the responsibility of management to find out the specifics. The best way to do this is to meet with the legal department on a regular basis and keep that department informed of what to do. This way, if new laws come out, they can be proactive in keeping you informed.

Privacy Codes

- The Canadian Independent Computer Services Association
- The European Organization for Economic Cooperation and Development (OECD)
- The European Council of Ministers
- Policies for Secure Personal Data

The following are privacy codes that will be reviewed:

- The Canadian Independent Computer Services Association
- The European Organization for Economic Cooperation and Development (OECD)
- The European Council of Ministers
- Policies for Secure Personal Data

We'll cover each in subsequent slides.

The Canadian Independent Computer Services Association

- Privacy principles for data processors
- Guidelines for handling client information
 - Information remains the property of the client.
 - Information may be retained for a limited time.
 - Receive permission from client prior to destroying or dispensing information.
 - Information should only be used for the purpose for which it was intended

The Canadian Independent Computer Services Association provides privacy principles for data processors.

The following are guidelines for handling client information:

- Information remains the property of the client.
- Information may be retained for a limited time.
- Receive permission from a client prior to destroying or dispensing information.
- Information should only be used for the purpose for which it was intended.

The OECD Guidelines

- The European Organization for Economic Cooperation and Development (OECD)
- Privacy and trans-border personal data flow
- Key provisions
 - Limitations on collection
 - Lawful collection
 - Accuracy of data ensured
 - Collected for legitimate purposes
 - No data disclosure, except with consent
 - Provide safeguards for data
 - Accountable for data controller
- Additional provisions
 - Notification of holding information
 - Ability to correct inaccuracies
 - Ability to examine data

The European Organization for Economic Cooperation and Development (OECD) provides for privacy and trans-border personal data flow. The following are the key and supplemental provisions.

Key provisions

- Limitations on collection
- Lawful collection
- Accuracy of data ensured
- Collected for legitimate purposes
- No data disclosure, except with consent
- Provide safeguards for data
- Accountable for data controller

Additional provisions

- Notification of holding information
- Ability to correct inaccuracies
- Ability to examine data

The European Council of Ministers

The Council of Ministers of the Committee of Experts on Human Rights of the Council of Europe:

- All information accurate and up-to-date
- Private data not stored
- Appropriate and relevant data
- Information obtained through fair methods
- Time periods established for how long data is kept
- Only use information for purpose for which it was obtained
- Knowledge of information stored
- Correct inaccuracies
- No abuse or misuse of information
- Enforce need to know
- No specific information released

The Council of Ministers of the Committee of Experts on Human Rights of the Council of Europe provides the following guidance:

- All information accurate and up-to-date
- Private data should not be stored
- Appropriate and relevant data
- Information obtained through fair methods
- Time periods established for how long data is kept
- Only use information for purpose for which it was obtained
- Knowledge of information stored
- Correct inaccuracies
- No abuse or misuse of information
- Enforce need to know
- No specific information released

Policies for Secure Personal Data

Two key elements:

- Commitment to internal privacy code principles
- Commitment to meaningful data security

The following are two key elements for securing personal data:

- Commitment to internal privacy code principles
- Commitment to meaningful data security

Intellectual Property

- Patent
- Copyright
- Trademark
- Trade secret

Because the United States is a service providing nation rather than a manufacturing nation, intellectual property is the main asset of the nation. It is in the best interest of the U.S. to protect intellectual property. The United States government has worked hard in this area.

Patent

- Protects inventions for 20 years from date of filing
- Invention must:
 - Have utility
 - Novelty
 - Be non-obvious
- Must reduce the invention to practice and cover a single idea

What Is a Patent?

A patent for an invention is the grant of a property right to the inventor, issued by the Patent and Trademark Office. The term of a new patent is (20) years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. U.S. patent grants are effective only within the U.S., U.S. territories, and U.S. possessions.

What is granted is not the right to make, use, offer for sale, sell, or import, but the right to exclude others from making, using, offering for sale, selling, or importing the invention.

Source:

<http://www.uspto.gov/web/offices/pac/doc/general/whatis.htm>

Copyright

- Form of expression
- Recorded thought on:
 - Paper
 - Vinyl
 - Plastic
 - Magnetic media
 - Or other media

What Is a Copyright?

"Copyright is a form of protection provided to the authors of 'original works of authorship' including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished. The 1976 Copyright Act generally gives the owner of copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly. The copyright protects the form of expression rather than the subject matter of the writing."

Source:

<http://www.uspto.gov/web/offices/pac/doc/general/whatis.htm>

Trademark

- A trademark is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.
- Sum of marketing efforts
- Sum of good-will efforts

What Is a Trademark or Servicemark?

A trademark is a word, name, symbol or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others. A servicemark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. The terms trademark and mark are commonly used to refer to both trademarks and servicemarks.

Source:

- <http://www.uspto.gov/web/offices/pac/doc/general/whatis.htm>
- <http://www.uspto.gov/web/offices/ac/ahrpa/opa/kids/kidprimer.html>

Trade Secret

- Protects critical intellectual property that is not publicly available
- Must provide "due care" protection to claim a trade secret
- Usually covered by an NDA

Trade Secrets

Trade secrets are information that companies keep secret to give them an advantage over their competitors. The formula for Coca-Cola is the most famous trade secret.

Source:

- <http://www.uspto.gov/web/offices/pac/doc/general/whatis.htm>
- <http://www.uspto.gov/web/offices/ac/ahrpa/opa/kids/kidprimer.html>

Trade secrets protect critical IP that is not publicly available. In order to claim an item as a trade secret, due care must be illustrated in keeping the assets protected and secret. Usually the disclosure of a trade secret is covered by an NDA.

Proprietary Rights and Obligations

- Security techniques to protect trade secrets
 - Numbering copies
 - Logging document issuance
 - Checking files and workstations
 - Secure storage
 - Controlled distribution
 - Limitations on copying
- Contractual commitments to protect proprietary rights
 - Licensing agreements with vendors
 - Liability for compliance

Both patents and trademarks are formal legal means of protection. To obtain either of these, you have to file paperwork and receive approval. A trade secret is less formal in that there is no external paperwork to fill out. The protection is obtained by the measures that you take and put in place to protect your information from outsiders. If a company wants to claim a trade secret at a later point in time, they must prove that they took effective measures to protect their information. For example, limiting and controlling the number of copies of a piece of information are critical. If you publish a piece of information on your Web server, it is hard to claim that you took measures to protect that information. Secure storage and controlled access are also critical measures that must be taken.

Proprietary Rights and Obligations (2)

- Enforcement efforts
 - Software Protection Association (SPA)
 - Federation Against Software Theft (FAST)
 - Business Software Alliance (BSA)
- Personal computers
 - Establish user accountability
 - Policy development and circulation
 - Purging of proprietary software

Protection of intellectual property has gotten out of hand—not only in this country, but around the world. Protecting it internationally is much harder, so efforts are first focused on getting the problem under control in the U.S.

The Software Protection Association (SPA) has been formed to take action to help protect the rights associated with the creator of a piece of software. If you create a piece of software, no one has the right to steal it from you. Federation Against Software Theft (FAST) deals with organizations that believe software has been stolen.

From a personal computer standpoint, a company must be capable of proving accountability. This is a big problem because everyone shares a password at some time. If two people log onto a system with the same user ID and password, how do you determine who gained access or stole a given piece of software?

Software Licensing Issues

- Software licensing
 - Site license
 - Per-server license
 - Per-personal computer license
 - Number-of-users license
- Software distribution
 - Crippleware
 - Shareware

If a company develops a piece of software, one way to protect it is to lock it up and not tell anyone about it. However, in most cases, the reason you develop software is to sell it to others. The question then becomes how do you sell it while maintaining control of the software. In most cases, a software vendor will not sell the source code or unlimited rights to the software (unless you pay them a large amount of money). In most cases, they will give you a limited license to the software. This seems simple, but it is confusing if you are not careful. Two common ways of doing this are per-seat or per-person. An individual with a license associated with him is per-person. If the person works on four different systems, he needs only one license. Per-seat means that each computer has a license. If four people work at the same computer, you need only one license, however, if one person works at three computers, you need 3 licenses. A site license is where you pay a set amount regardless of the number of people that will be using the software. These are usually more expensive, but cover a company from having to purchase new licenses every time a new employee is hired at the company. If a company does not want to spend the money on a full site license they can buy a number-of-user license based on the number of people that will actually be using the software.

In some cases, a software company wants to let people try out a piece of software, but in order to entice them to buy the software they give them only limited functionality. Software with limited functionality is called crippleware. Typically with crippleware, after you load in a valid license, all of the features are enabled on the system. Shareware is another type of distribution where anyone can download the software, but you only pay for the software if you use it beyond the trial period.

Types of Law

- Criminal
 - Felony
 - Jail
 - More serious
 - Misdemeanor
 - Fine or jail sentence
- Civil (Tort)
 - Compensatory damages
 - No fault of the victim
 - Punitive damages
 - Punish offender
 - Statutory damages
 - Determine by law
- Administrative (Regulatory Law)

Incident Handling and the Legal System

As you might guess, there are several legal aspects of incident handling that you must consider before deciding to pursue criminal or civil action from the result of an incident. An organization must be familiar with the laws of its states or countries of operation to develop incident-handling policies and procedures. Laws, as they pertain to incident handling, generally fall into one of three categories: regulatory, criminal, and civil law.

- **Criminal law:**

Criminal law governs individual conduct as it pertains to laws, both federal and state, that were designed to protect the public. Examples include unauthorized use of a system, denial of service attacks, and Web site defacement. Violation of these laws can result in monetary penalties and/or imprisonment.

- **Civil law:**

Civil law refers to an action against a company that causes damage or financial loss. Examples of incidents that could be tried under civil law include worm attacks, denial of service, or any other attack that affects the availability of a system. Violation of civil law can result in punitive or compensatory damages being rewarded to the organization affected by the incident.

- **Regulatory law:**

Regulatory law, by its very definition, deals with the governing regulations of a particular country and is especially important for government workers or those computer professionals in highly-regulated environments, such as banking, finance, healthcare, and pharmaceuticals. An example of this type of law is the Health Insurance Portability and Accountability Act (HIPAA).

In terms of criminal law, traditional crimes, such as theft, fraud, harassment, and child pornography, are likely to come up in the course of incident handling. A variety of federal and state laws regulate the use of computers, networks, and data that reside in the confines of each. These laws impose civil (monetary) and criminal (incarceration) penalties, which are enforced by various agencies and departments of both federal and state government agencies. Examples of these laws include the DMCA (Digital Millennium Copyright Act), HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), and others as they relate to the use and dissemination of personal information.

Criminal Law

- Victim is society
- Purpose of prosecution: punishment
- Deterrent effect of punishment
- Burden of proof: reasonable doubt
- Felonies: jail > one year
- Misdemeanors: jail < one year
- Federal and state levels
 - Elements of proof vary between and among
 - Specific versus general applicability

There are two main categories of law in the U.S.: criminal and civil. With criminal law, the victim is society and to make criminal charges against someone, law enforcement must be involved. An individual or company cannot take criminal charges against someone. Criminal offenses are the only offenses in which someone can get jail time. With civil laws, you can get monetary restitution, but not jail time.

When dealing with law, there is a criterion that determines whether someone is guilty. With criminal law, the burden of proof says you have to prove beyond a reasonable doubt that someone committed a crime. Depending on the severity of the crime, there are different amounts of jail time one can get for a crime.

Civil Law (Tort Law)

- Damage/loss to an individual or business
- Type of punishment is different: No incarceration
- Primary purpose is financial restitution:
 - Compensatory damages, actual damages, attorney fees, lost profits, and investigation costs
 - Punitive damages: Set by jury to punish offender
 - Statutory damages: Established by law
- Easier to obtain conviction: Preponderance of evidence
- Impoundment orders/writs of possession:
Equivalent to search warrant

We mentioned earlier that there are two types of law: criminal and civil. With civil law, you do not need law enforcement involved to take action against an individual. However, with civil law, a person cannot get jail time. A person can only be ordered to pay monetary damages. Because law enforcement is selective about which "hacker" cases they take, it is common for a company to take civil action against an attacker if the attacker is known and there is proof the attacker caused damages to the company. In civil cases, because there is no jail time, the cases are generally easier to prove and take less time in the court room.

Computer Crime

'The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros—little bits of data—it's all electrons... There's a war out there, old friend, a world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... It's all about the information!'

-Lines from the character "Cosmos," in *Sneakers*, MCA/Universal Pictures, 1992.

Types of Computer Crimes

There are four general types of computer crimes:

- Computer as the target = data on the computer
- Computer as the instrumentality of the crime = tool, knife, gun, computer
- Computer is incidental to other crimes = facilitation of crime, encryption for cocaine trafficking
- Crimes associated with the prevalence of computers = file sharing has risen

Source:

- <http://us.imdb.com/title/tt0105435/quotes>
- <http://nsi.org/Library/Compsec/crimecom.html>

Computer Crime Issue: Definition

Computer crime is hard to define:

- Lack of understanding
- Laws are inadequate: Slow to keep pace with rapidly-changing technology
- Multiple roles for computers:
 - Object of a crime: Target of an attack
 - Subject of a crime: Used to attack (impersonating a network node)
 - Medium of a crime: Used as a means to commit a crime (Trojan horse)

We all use words we all understand and know, but that can be difficult to define. A common phrase is, "I cannot define it, but I know it when I see it." Computer crime is a difficult term to define because a computer can be used in many different aspects of the crime. The following are examples:

- Object of a crime: Target of an attack
- Subject of a crime: Used to attack (impersonating a network node)
- Medium of a crime: Used as a means to commit a crime (Trojan horse)

A computer can also be used to store evidence that is used in a crime.

Computer Crime Issue: Prosecution

Difficulties in Prosecution:

- Understanding: judges, lawyers, police, and jurors
- Evidence: lack of tangible evidence
- Forms of assets: magnetic particles, computer time
- Juveniles:
 - Many perpetrators are juveniles.
 - Adults don't take juvenile crime seriously.

From a pure evidence standpoint, anything residing on a computer is just binary data stored in the form of ones and zeros. The abstraction that occurs to take that binary data and make it meaningful is transparent in every day work, but can confuse things when you are dealing with judges and jurors who are not technical and can be easily confused. The goal of some prosecutors is to make the technology so confusing that a juror cannot decide (within the constraints of reasonable doubt) that an individual committed a crime.

Categories of Computer Crime

- Military intelligence attacks
- Business attacks
- Financial attacks
- Terrorist attacks
- Grudge attacks
- Fun attacks

Criminal elements are turning more to computers to commit crimes. Some of the general categories of crime include:

- Military intelligence attacks
- Business attacks
- Financial attacks
- Terrorist attacks
- Grudge attacks
- Fun attacks

Examples of Computer Crime

- Kevin Mitnick's attacks against telephone systems
- Teenagers in Wisconsin (area code 414) known as the 414 gang who, in 1982, launched attacks into the Sloan-Kettering cancer hospital's medical records systems
- The Morris Internet worm

Mitnick was convicted in 1989 for computer and access device fraud, but eluded police and the FBI for over two years while he was on probation. On Christmas of 1995, he broke into the computers of Tsutomu Shimomura in San Diego, California. Tsutomu tracked down Mitnick after a cross-country electronic pursuit. Mitnick was arrested by the FBI in Raleigh, North Carolina, on February 15th, 1995.

The Morris Worm spread through the Internet in November of 1988 and resulted in a Denial of Service (DoS.) The cause of this disruption was a small program written by Robert Tappan Morris, a 23 year old doctoral student at Cornell University.

Monitoring

- Electronic monitoring
 - Applied consistently and uniformly
 - Should be conducted in a lawful manner
- E-mail monitoring
 - User should be informed
 - Logon banner
 - Other means
 - Banner should state:
 - Individual consents to monitoring by logging on to system.
 - Define the consequences of unlawful activities.
- State that there is no guarantee of e-mail privacy.

Voluntary Disclosures

A hacker's victim might voluntarily disclose the contents of internal e-mails relevant to the attack.

Early Communication with ISPs

Investigators should contact a network service provider as soon as possible to request that the ISP retain records that might be relevant to an investigation.

Electronic Surveillance

Investigators tracking down hackers often want to monitor a hacker as he breaks into a victim's computer system. The two basic statutes governing real-time electronic surveillance in other federal criminal investigations also apply in this context. The first is the wiretap statute, generally known as a Title III order. The second statute relates to pen registers and trap and trace devices. DOJ's manual for obtaining evidence of this type, says, "In general, the Pen/Trap statute regulates the collection of addressing information for wire and electronic communications. Title III regulates the collection of actual content for wire and electronic communications."

The bottom line: It is not easy to obtain the evidence legally. Criminals know this.

Source:

http://www.cybercrime.gov/usamav2001_2.htm

Legal Liability

- **Due care:**
Minimum and customary practice of responsible protection of assets
- **Due diligence:**
The prudent management and execution of due care
- **Programming errors:**
Reasonable precautions for:
 - Loss of a program
 - Unauthorized revisions
 - Availability of backup versions
- **Product liability**
 - Liability for database inaccuracies due to security breaches
 - European Union: No limits on personal liability for personal injury

If a problem occurs when one uses software that someone else created, does the person who wrote the software have a legal liability for the damages that were caused. As with most aspects of the law, it depends. In most cases, what it depends on is due care taken in writing and checking the code. Due care is the base level of protection that a reasonable person takes to check a piece of code. If this is not done, there are potential liability issues. Likewise, if you take software and use it on a sensitive piece of information that gets destroyed, and you fail to make a backup, you as the data custodian did not properly execute due care.

Legal Liability (2)

- Defamation
 - Libel due to inaccuracy of data
 - Unauthorized release of confidential information
 - Alteration of visual images
- Foreign Corrupt Practices Act
 - Mandate for security controls or cost/benefit analysis
 - Potential SEC litigation

According to dictionary.com, defamation is the act of injuring another's reputation by slanderous communication, written or oral; the wrong of maliciously injuring the good name of another; slander; detraction; calumny; aspersion.

Essentially, it involves making a false statement about an individual with the goal of injuring their reputation. This can also be manifested in the form of creating false images of someone. Most of these items fall under the category of civil law.

Legal Liability (3)

- Federal sentencing guidelines
 - Chapter 8 added in 1991
 - Applicable to organizations
 - Violations of federal law
 - Specifies levels of fines
 - Mitigation of fines through implementation of precautions

When there has been a wrongdoing, what is the penalty for the person who committed the wrongdoing? Instead of randomly coming up with a punishment, there are federal sentencing guidelines that dictate what the punishment is based on the infraction. This is why there are certain crimes that do not entail jail time, but just a fine, whereas others do have jail time. The way the court determines this is based on these the Federal Sentencing Guidelines. The federal sentencing guidelines determine the maximum and minimum amounts of fines and jail time you can get based on the crime you committed. This allows people to be treated fairly. Without these guidelines two people could commit the same crime but be given unequal sentencing. The guidelines limit the sentences a judge can hand out so everyone pays the same amount of time for doing the same crime.

Investigation Steps

- Detection and containment
 - Accidental discovery
 - Audit trail review
 - Real-time intrusion monitoring
 - Limit further loss
 - Reduction in liability
- Report to management
 - Immediate notification
 - Limit knowledge of investigation
 - Use out-of-band communications

For there to be an investigation, there has to be a wrongdoing or the threat of a wrongdoing. Therefore, identification of an incident is critical. An incident can be identified accidentally by seeing a problem or because someone reported a problem and you formally investigated it. After you know there is an incident, the immediate goal is to contain the problem and make sure it does not get worse.

You should also keep key management involved regarding what occurs, but always keep in mind the need to know principle. Only the minimum number of people should know about an incident and be kept informed, not the entire company.

Investigation Steps (2)

- Preliminary investigation
 - Determine if a crime has occurred.
 - Review the complaint.
 - Inspect the damage.
 - Interview witnesses.
 - Examine logs.
 - Identify investigation requirements.

During the preliminary steps of an investigation, the first thing you need to determine is whether there is, in fact, an incident. Normally you have a good idea that an incident occurred; otherwise, do not waste a lot of time with an investigation. However, even if there is an incident, you have to determine early in the process whether a crime has been committed. Depending on the extent of the crime, you might be required by law to immediately notify law enforcement.

After the investigation has started, determine the extent of the damage so you can figure out which systems were involved. Those systems should first have a binary backup made to preserve the data and then be contained so the damage does not spread to other systems. In addition any key witnesses should be interviewed and written statements should be taken and signed by the witnesses. Any additional details like log files should be reviewed.

Investigation Steps (3)

- Disclosure determination
 - Determine if disclosure is required by law.
 - Determine if disclosure is desired.
 - Take caution in dealing with the media.
- Courses of action
 - Do nothing.
 - Surveillance?
 - Eliminate security holes?
 - Is a police report required?
 - Is prosecution a goal?

A company never wants to publicize that they have had an incident. The main reason is the company might end up losing money due to bad press. However, there are some situations when you must report an incident to law enforcement; otherwise, you might break the law. In addition, from an ethical standpoint, it is usually considered good form to contact a company so they can contain the damage on their end.

During an investigation, there are several approaches you can take. If you do not think the damage is great, you might choose to do nothing about it or just watch and learn to see if the problem gets any worse.

Investigation Steps (4)

- Conducting the investigation
 - Investigative responsibility
 - Internal investigation
 - External private consultant investigation
 - Local, state, and federal investigation
 - Factors
 - Cost
 - Legal issues (privacy, evidence, search, and seizure)
 - Information dissemination
 - Investigative control

During the investigation, you will probably need a whole team involved, but there should also be one person who is in charge. The person in charge is the main point of contact and interfaces with law enforcement, external parties, and management. A company must also decide how much money and resources they will put into the investigation.

Investigative Process

- Identify potential suspects.
 - Insiders
 - Outsiders
 - Collaboration
- Identify potential witnesses.
 - Who to interview
 - Who to conduct interview

Information that leads to evidence is key during an investigation. The more evidence you obtain, the better chance you have of determining who is involved and the better chance there is to prosecute them. If the case goes to court, the more relevant evidence that you can gather and preserve, the greater the chance you can prove your case and win.

There is an old saying that if it is not in writing, it never happened. You can have a star witness who four months from now changes his story and forgets what happened. With a key witness, you should work to put together a written statement and have the witness sign it, thus preserving the evidence.

The witnesses represent a key source of evidence so it is critical that they are identified and appropriate information is gathered from them.

Computer Forensics

- **Conduct a disk image backup of suspect system:**
Bit-level copy of the disk, sector-by-sector
- **Authenticate the file system:**
Create message digest for all directories, files, and disk sectors
- **Analyze restored data:**
Conduct forensic analysis in a controlled environment
 - Search tools: Quick View Plus, Expert Witness, Super Sleuth
 - Searching for obscure data: Hidden files/directories, erased or deleted files, encrypted data, overwritten files
 - Steganography: Hiding a piece of information within another
 - Review communications programs: Links to others

Before any changes are made to the systems under investigation, make a binary backup. A binary backup is different than a file-level backup. A file-level backup backs up only known files on the system. However, deleted files can still remain on the hard drive. A binary backup also captures this information and with a binary backup, you can recover deleted files that can be used as valuable evidence.

After a backup is done, it should be digitally signed so that, at a later point in time, you can prove that it was not modified. After a backup is done, you can analyze the information to look for evidence. The following lists some of the tools available to you and some of the items to look for:

- Search tools: Quick View Plus, Expert Witness, Super Sleuth
- Searching for obscure data: Hidden files/directories, erased or deleted files, encrypted data, overwritten files
- Steganography: Hiding a piece of information within another
- Review communications programs: Links to others

Banner Design

- Creating your own banner properly
- Consider the key functions:
 - Consent for monitoring
 - Examination of stored files
 - No right of privacy
 - Possible prosecution

Banners have four primary functions:

- To generate consent to real-time monitoring under Title III.
- To generate consent to the retrieval of stored files and records pursuant to ECPA.
- In the case of government networks, banners might eliminate any Fourth Amendment "reasonable expectation of privacy."
- In the case of a non-government networks, banners might establish a system administrator's "common authority."

The following is a checklist of issues that you might consider when drafting a banner. Each answers a point of law:

- Does the banner state that use of the network constitutes consent to monitoring?
- Does the banner state that use of the network constitutes consent to the retrieval and disclosure of information stored on the network?
- In the case of a government network, does the banner state that a user of the network will have no reasonable expectation of privacy in the network?
- In the case of a non-government network, does the banner make clear that the network system administrator(s) can consent to a law enforcement search?
- Does the banner contain express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring?
- Does the banner state what users are authorized to access the network and the consequences of unauthorized use of the network?
- Does the banner require users to "click through" or otherwise acknowledge the banner before using the network?

Banner Examples

*WARNING! This computer system is the property of the United States Department of Justice and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. The Department **may monitor** any activity or communication on the system and **retrieve any information stored** within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. **Users should have no expectation of privacy** as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., floppy disks, PDAs, and other hand-held peripherals, CD-ROMs, and so on).*

Here are three examples of broad banners:

- 1. This computer system is the property of the United States Department of Justice and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. The Department may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., floppy disks, PDAs, and other hand-held peripherals, CD-ROMs, and so on).*
- 2. This is a Department of Defense (DoD) computer system. DoD computer systems are provided for the processing of official U.S. Government information only. All data contained within DoD computer systems is owned by the Department of Defense, and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DoD computer systems for any reason. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, or CAPTURING and DISCLOSURE.*
- 3. You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.*

Source:

<http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm>

Investigation Issues

- Attorneys
 - Helpful and costly
- Search and seizure
 - Let the law handle it

Attorneys can be very helpful and costly in an investigation. They can also slow the process down. It is best to ask the question, "How can I legally do (fill in the blank) and what is the precedence in such a case?" Do not ask the question, "Is this legal?" ... The answer is always, no.

Search and seizure is best left to law enforcement. Search and seizure is also best when you have a warrant. Assume that you need to seize computer equipment without law enforcement or a warrant. You must consider The Fourth Amendment's "Reasonable Expectation of Privacy." Electronic storage devices (computers) have been likened to closed containers. Exceptions to this rule are: consent (scope, third-party, and implied) exigent circumstances, plain view, search incident to a lawful arrest, inventory searches, border searches, and international issues. We focus on consent as CISSPs. Third-party consent mandates that if other people use the computer, such as administrators or co-workers, they can give you the right to search and seizure.

The Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official."

Rules of Evidence

- Types of evidence
 - Direct: Oral testimony by witness
 - Real: Tangible objects/physical evidence
 - Documentary: Printed business records, manuals, and printouts
 - Demonstrative: Used to aid the jury (models, illustrations, charts)
- Best evidence rule: To limit potential for alteration
- Exclusionary rule: Evidence must be gathered legally or it can't be used
 - Fourth Amendment
- Hearsay rule: Key for computer-generated evidence
 - Second-hand evidence
 - Admissibility based on veracity and competence of source
 - Exceptions: Rule 803 of Federal Rules of Evidence (business documents created at the time by person with knowledge, part of regular business, routinely kept, supported by testimony)

Evidence is the proof that is needed to take action against someone in a court of law. Therefore, how you gather, maintain, and protect information is critical. Evidence can come in many forms, including expert testimony and what people see. What someone sees today and what they remember several months from now might be quite different. Therefore, one of the common ways to preserve evidence is to write it down. This is why if you are a witness to a crime, you will usually have to give a written statement of what you saw and sign it. The evidence will be then be preserved for later use.

The final type of evidence we need to discuss is hearsay or, as it is sometimes called, third-party evidence. This is evidence that has been obtained from an outside source and, under the Federal Rules of Evidence, is inadmissible in court. Most business records that are generated electronically fall under the hearsay rule and are considered to be unreliable and inaccurate simply because there is no way to prove otherwise. However, there are exceptions to hearsay, including business records, admissions, and public records.

Chain of Evidence

Accountability and protection:

- Who obtained evidence?
- Where and when it was obtained?
- Who secured it?
- Who controlled it?
- Account for everyone who had access to or handled the evidence.
- Provide assurance against tampering.

The chain of evidence refers to what happened to the evidence from the time it was gathered until the present day. When evidence is used in a court of law, in addition to showing that it was gathered in a legal manner, you also have to show that you properly preserved that evidence to minimize the chance that it was modified or tampered with in anyway, shape, or form. If you want to use evidence against someone, that person will attempt to make the evidence inadmissible in a court. One of the ways a person can make evidence inadmissible is to prove that it has been tampered with and is not accurate.

Rules of Evidence:

Admissibility of Evidence

Computer-generated evidence is always suspect:

- Relevancy: Must prove a fact that is material to the case
- Reliability: Prove reliability of evidence and the process for producing it

From a court's perspective, you have to make sure that the evidence you use is reliable and accurate. Because the internal workings of a computer are not understood in detail by a lot of people including a judge, people always question the reliability of computer evidence.

Another key point is that any evidence you bring to bear on a case must be relevant to the case. If it is not relevant, the judge might throw it out. In other cases, the judge will allow the evidence, but the opposing attorney can use it against you and make your case harder to prove.

Evidence Life Cycle

- Collection and identification
- Storage, preservation, and transportation
- Presentation in court
- Return to victim (owner)

When an investigation is underway, evidence needs to be gathered to prove the case. The typical way this is done is by getting a search warrant. Law enforcement does this so that they can acquire the evidence. Although law enforcement confiscates the equipment and it is in their possession, it still belongs to you. However, you are not allowed to use it or have access to it because you could tamper with the evidence.

After the evidence is in the possession of law enforcement, they must store it and take measures to preserve the evidence so that it cannot be destroyed or modified. The evidence is usually presented in court during the proceedings of the case. When the case is over, the equipment is eventually returned back to the owner.

Legal Proceedings

- Discovery
 - Defense granted access to all investigative materials
 - Protective order limits who has access
- Grand jury and preliminary hearings
 - Witnesses called
 - Assign law enforcement liaison
- Trial: Unknown results
- Recovery of damages: Through civil courts

A series of steps happens before a case can go to court. After the judge determines there is enough evidence and orders a court date, discovery takes place. This is when the defense is given access to all of the evidence and is allowed to gather their own evidence and ask questions of witnesses. If you have a piece of evidence, you must make it available to the defense. Surprises in terms of new evidence are not allowed. If a new piece of evidence is discovered during the court case, the judge usually grants a recess to allow the defense to investigate it.

After the evidence has been reviewed, you have the preliminary hearings. This is followed by the actual trial. After the trial is done and a decision is made on the case, the consequences are meted out: possible damages are paid or jail time is served.

Legal Proceedings

Post Mortem Review

Analyze attack and close security holes:

- Incident response plan
- Information dissemination policy
- Incident reporting policy
- Electronic monitoring statement
- Audit trail policy
- Warning banner (Prohibit unauthorized access and give notice of monitoring)
- Need for additional personnel security controls

After you have been attacked, you will likely take action of two fronts: a legal side and a technical side. If your site had a computer crime committed against it, vulnerabilities allowed the attack to occur. This information needs to be reviewed and used to determine the next course of action. In the course of the review, critical documents need to be updated. The following are some of the documents that should be addressed:

- Incident response plan
- Information dissemination policy
- Incident reporting policy
- Electronic monitoring statement
- Audit trail policy
- Warning banner (Prohibit unauthorized access and give notice of monitoring)
- Need for additional personnel security controls

Search and Seizure

- Subpoena
 - Issued by the court to an individual
- Search Warrant
 - Issued to law enforcement
- Warrant should specify computer system (computer and related equipment, mouse, and keyboard)
- Warrant should specify computer's role in offense (attack tool and storage device)

Incident Handling Investigation

During the course of the incident-handling process, the chances are increasingly likely that you will be called upon to conduct an investigation that could lead to criminal or civil charges against the attacker. During an investigation you may need to seize a computer or obtain a warrant to further the investigation. There is also an unlikely chance that you would need to arrest someone. Each of these tasks mentioned require careful thought and planning, so it is very important to address these likelihoods when preparing your incident-handling policy and procedures.

Search and Seizure without a Warrant

There are generally three accepted provisions for seizing property without a search warrant. Property can be seized if (1) the suspect gives his consent; or (2) if he is arrested, and the property is in plain sight or on his person; or (3) if the employment policy governing the individual is explicit enough to cover search and seizure as conditions of employment.

If your organization fosters privacy, then seizure must occur by warrant. If there are warning banners, and the employee handbook is clear that the organization's computers are the sole property of the organization, then the handler has a wider degree of latitude. Another point to consider is having what is called a standing letter of consent, which should be part of the employment agreement if the organization actually owns the systems they operate. If you are asking for permission, try to make certain that several witnesses are present. Not only is this good policy in terms of future admissibility of the evidence, but it can work psychologically as well.

When seizing a computer, the best practice is to seize the computer, mark the serial number, then pull the hard drive and treat it as a separate piece of evidence. This allows the forensics expert the ability to analyze only the hard drive. The drive can be stored in a Ziploc bag that is carefully sealed with tape and marked with the date and time it was seized. Some handlers prefer to purchase police evidence bags that have built-in tamperproof seals and additional space on the bag to add more relevant information.

Issues

Fourth amendment (search and seizure):

- Fourth amendment rights
- Protects individuals from unlawful search and seizure
- Exception to fourth amendment rights is exigent circumstances doctrine
 - Seizure of evidence with probable cause in the event of pending destruction

Fourth amendment protections are not applicable to ordinary citizens unless the person performing the search is acting under direction of law enforcement.

In U.S., law enforcement personnel are bound by the fourth amendment.

Search warrants are issued when there is probable cause.

Evidence can be obtain from telephone records, audit trails, system logs, backups, witnesses, and e-mails.

Interrogation

- Suspect
 - Does the suspect have motive, opportunity, and means (mom) to commit a crime?
- Interrogation
 - Plan in advance.
 - Obtain information.
 - Avoid alerting suspects when they are scheduled for interrogation if possible.
 - Avoid providing suspect with useful information.
 - Conduct interrogation by more than one person.

Suspect might try to alter evidence when alerted to an investigation. Therefore suspects can be interrogated with the goal of trying to validate information and find out additional details. Sometimes there is not enough evidence to determine what happened and information must be obtained from the suspect. It is critical that when an interrogation is performed that the suspect does not have any of their rights violated.

Interrogation (2)

- Interrogation
 - Obtain expert help in conducting the interview.
 - Be aware that suspects may try to alter additional evidence, leave the premises, or warn other co-conspirators.
 - Obtain pertinent information relative to the crime and script the questions prior to an interrogation.

Original documents should not be used in the conduct of the interview. This will help avoid possible destruction of critical information by the suspect. Some additional tricks to follow are:

- Obtain expert help in conducting the interview.
- Be aware that suspect may try to alter additional evidence, leave the premises, or warn other co-conspirators.
- Obtain pertinent information relative to the crime and script the questions prior to an interrogation.

Enticement

For information security:

- Occurs after intruder has gained unauthorized access to a system
- Individual lured to an attractive area or "honeypot"
- Used to gather information to determine source of attack

Enticement occurs after an intruder has trespassed or committed a crime and is lured into a location from which administrator want to gather further evidence. A key example of enticement is a honeypot, which draws attackers in so additional information can be obtained. Enticement typically occurs after someone has broken into a system.

Entrapment

Encourages the commission of a crime that the individual initially had no intention of committing

There is no entrapment when a person is willing and able to break the law and a government agent provides an opportunity to commit the crime. Entrapment occurs only when a government agent encourages an individual to commit a crime they otherwise had no intention of committing.

Arrest/False Arrest

Arrest is a legal process to deprive an individual of his/her freedom. This can occur only in the unlikely case that you actually see a crime that occurs and are put in harm's way.

Arrest/False Arrest

Arrest is a legal process to deprive an individual of her freedom. The arrest of a suspect isn't to be taken lightly, and if you suspect the eventual outcome of the incident will lead to prosecution, then it is recommended to get law enforcement involved as soon as possible. The key point is that if you did not witness the incident firsthand, and it is not considered an urgent matter, then do not deprive the suspect of her freedom. Work closely with law enforcement officials and provide them with as much information as possible to help them make the decision as to whether arresting a suspect is the best course of action. Arresting someone should be considered an absolute last course of action.

Evidence Must Be Admissible

- Relevant to the case: Directly related cases are already complex.
- Submitted evidence should lead to a decision — not a hung jury.
- Reliable!

Incident Handling Evidence

During the course of incident handling, there may be times when evidence must be collected to help prove the facts of the case. Evidence collected must be relevant to the case and preserved in such a way as to not do any damage to the integrity of the investigation. The goal is to attest to the evidence, collect the evidence, and, in the process, ensure the evidence is auditable. Finally, the evidence must be signed and sealed to prevent any signs of tampering that may render the evidence useless in a court case.

Chain of Custody

Maintain a provable chain of custody:

- Attestation
- Collect
- Ensure evidence is auditable
- Sign and seal

Chain of Custody

Chain of custody is an important application of the Federal rules of evidence. The methods and procedures used can affect the admissibility of the evidence collected. Although this is not generally considered a problem, maintaining good procedures will ensure that any evidence gathered will be admissible in a court of law.

The first step in maintaining chain of custody is to establish the basics of the situation like who, what, where, and when. Before you touch the computer, it is a good idea to write down where you are, describe the situation, and note all serial numbers of the machine(s) in question. Once the baseline has been established the collection phase can begin. If at all possible, a binary backup of the information should be performed to prevent any further steps from possibly weakening your case.

Real and Direct

- Real evidence is the tangible item: the seized computer, the diskette, the printout.
- Direct evidence comes from what the handler actually saw; it is not surmised.

When it comes to presenting evidence in court, it is generally accepted that real, direct, and best evidence can usually make or break a case. Real evidence is always a luxury to have in a courtroom and can often sway the opinion of jurors simply because they are able to see tangible items such as the seized computer, diskettes, or printouts. For example, which do you think would be better to see in a court case, the actual computer used to launch an attack or an 8mm tape said to contain the contents of the hard drive on the computer?

Direct evidence usually comes in the form of oral testimony by an incident handler or system administrator to discuss what they saw occur and not what they speculate occurred during an attack. In cyber crimes it is usually quite easy to demonstrate the what, where, and when of a case, but it can be difficult to prove the who behind the attack. A person can claim someone else was using their password at the time of the attack and so forth. This may be one of the two best reasons to adopt a watch and learn approach to incident handling. This may allow you to establish, through a variety of collected evidence, who is actually committing the crime instead of speculating who the perpetrator may have been during the time of the attack.

Best Evidence

If a tractor trailer crossing a bridge was hit by a helicopter, you wouldn't normally expect the real evidence to be brought to the courtroom. Instead, photos, models, and drawings are used. Cyber cases happen at the speed of light and there are times when screen shots, network traces, and so forth must be used. Be ready to prove that this is the best evidence available.

If it is not possible to have tangible items that were used during a crime, then you need to demonstrate that you have the best evidence available. Best evidence usually comes in the forms of models, photos, and screenshots to depict how an attack occurred. The key point is that the evidence presented is both accurate and the best evidence that was reasonably available. An example of this would be a small ISP that does not have the means to give up the equipment-such as DNS servers, firewalls, and e-mail gateways-attacked during a crime for a long period of time. In this case, they may opt to use the backed up contents of each of the servers to demonstrate their case. This would be considered best evidence.

Summary

- Ethics are critical to a security professional.
- The impact of the law on security must be understood.
- It is critical to know your job and get outside expert assistance when necessary.

Because security is such a sensitive area, it is critical that those who work in security have ethics and understand what it means to behave in an ethical manner. Although we do not expect a security professional to have a law degree, it is critical that security professionals understand some of the law. In cases where the law is too complex, it is critical to know when to seek outside expertise.