GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

How to Bootstrap Information Security in your Organization

Mark Gryparis, GCIA
GSEC Practical Assignment v1.2c

1 Introduction

This paper is a roadmap for implementing Information Security in the following situations:

- When you get your first job as an Information Security Administrator (Security Admin) with a new company
- When you volunteer (or get volunteered) to be the Security Admin with your current company
- If you are a company with little or no effort or thought currently spent on security, and need to ramp up

This paper assumes the following proficiency on the part of the reader:

- Broad, general understanding of IT systems and technologies
- Solid understanding of Computer Networking and TCP/IP

The focus is on breadth, rather than depth; to touch on all topics, and provide enough information in each area for you to determine if/how deep you need to go. If you decide you need to go down a particular path, you will have to do some research. Research resources are provided whenever possible.

The steps in this roadmap are presented in "optimum order", that is, the way to do it if you had the freedom and luxury of time to do things right. Of course, in the real world this is very rarely the case. You will have to do things out-of-order, in parallel and hastily, hoping for the time to clean it up later. (Just like the rest of life.)

2 Orient Yourself

Information Security is a job that requires a significant authority and power to execute, either your own, or that of higher-ups who support you. It is a very political role, in which every statement and proposal you make must first be calculated for effect with all the players. Those who ignore this fact or miscalculate the effect of a critical act risk coming in to work one day to find the tides of human emotion raging against you.

2.1 Get to know the local culture

If you are new to the company or organization, this is the most critical step. Culture, in this sense, is defined as "the set of shared attitudes, values, goals, and practices that characterizes a company or corporation."[1] It is always a force to be reckoned with, and, in some situations, the most powerful force you'll have to deal with.

Security requires some effort on the part of every User and Administrator of the Information System. Therefore, many people feel it as a burden. How they react can often be predicted by examining the local culture. These are the questions you must answer about it:

- How open to security is it? Has it ever been burned by a security incident? Cultures that are new to the overhead of security will have to be convinced that it is necessary. Users that have never dealt with security before will complain that it will hurt their productivity.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

You must keep user productivity concerns - both real and imagined - in mind when you design security solutions. IT Staff that has been very autonomous or is overworked/understaffed will balk. You must be prepared to work with them and provide solutions that are realistic and automated enough to be practical.

- Is it averse to change? You may have to focus on first convincing management of the need for change, and then let them mandate the changes you need to make.
- What's the internal power structure? Does power flow down from top management or does it have many centers? The Security Admin (or his/her manager) must have enough authority to meet the responsibility of security. This means that many people in the organization will have to give up some of their control and give it to you. Are there individuals in the organization that will fight you simply because it means a lessening of their control? You should identify them and try to make them stakeholders and participants. If you can't, then prepare to fight. If you are of the type that avoids politics like the plague, you should find another line of work.

If you find yourself in a culture that is hostile to your mission, you will have to work to change how security is perceived in that culture. The best approach is to convince those with the power (hopefully management) that security is a good thing, and to make them your willing proxies in implementing change. If that is not possible, then you are in the difficult position of trying to change a culture from the grass roots-up - a lengthy and difficult process at best.

2.2 Get to know the management

Everyone needs to build a good relationship with his/her boss. For Security Admins, the need is far greater than normal. Your ability to do your job depends on:

- Your manager's values, beliefs and perceptions regarding security
- How well your manager understands your mission, and the organization's vulnerabilities, threats and risks
- How willing and able he/she is to implement change on your behalf
- How much your manager trusts you

You must get to know your manager and his/her position on each point. A lack of understanding or trust here is a high-priority problem that you must fix.

Through your manager and other sources, you need to get to know the upper management of your organization. Get to know the names and personalities of each top manager. Your goal is to build a behavior model for each, so that when you're formulating changes to policy, procedure and culture, you can predict how each manager will react.

If you're not granted authority by management, and/or can't depend on the authority of management to support you, then you have responsibility without authority, and you run a non-trivial personal risk. (See section 4.1 Protect Yourself)

2.3 Get to know the users

It is important to get to know:

- <u>The Company</u>. What is the company's product? How does it create, sell and deliver that product? Information Security - and IT in general - is NOT the same from company to company, or between different stages in a company's growth and development. A company that manufactures washing machines has very different requirements on its IT infrastructure than one that provides on-line stock trading services. It is critical to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

thoroughly understand the flow from Business Requirements to IT Requirements to Information Security Requirements before you can design Information Security solutions.

- The Departments. Each department has different IT needs, i.e.: Accounting needs to produce regular reports on time; HR needs to keep its records confidential; Engineering likes to keep odd hours; the IT Staff is overworked, etc, etc. Each group has one or two capabilities, tasks or resource limitations that will make or break their success. You must identify these and keep them in mind when proposing changes in policy/procedure that affect their lives. Implementing or even proposing a security-related change that could cause a department to fail in their mission will only hurt your credibility.
- The Power Users. Every organization that uses IT has a few Power Users. These are local IT user/experts that have mastery of the technology and understanding of the user community matching or surpassing that of the IT staff. You must identify and get to know these people, listen to what they say and gain their trust. They are often the best sources of information you'll find on the organization, its culture, and how IT is used. They can also be powerful advocates when you need to propose a new security procedure that will likely be unpopular. Occasionally, you will run across a Power User that opposes and derides Information Security at every opportunity. These people can be your worst enemy – especially if you are new to the organization. In this situation, you must either convert them to your cause, or use your patrons in management to override them: there is no middle ground.
- The Admin Assistants to the Big Kahunas. As anyone who has worked in IT for more than a year or two can tell you, one of the keys to winning the trust and support of a manager is winning the trust and support of his/her Admin Assistant (archaic: Secretary.) If a new security policy or requirement makes the life of an Admin difficult, their manager will oppose it. If you must go down a road that you know they will not like, take the time to inform, educate and even hold their hands - it is a good investment.

2.4 Get to know the IT Staff

The IT Staff is usually a mixed bag in terms of security. Some individuals understand the need for Information Security and even support it. Others see it as irrelevant to their job at best, and at worst, an obstacle to getting their job done. Still others will interpret the controls of Information Security as arrogance and power-hunger on your part, and despise you.

The best strategy with the IT staff is this:

- Get to know the IT staff, their style, environment and tools
- Identify those tools, conveniences and short-cuts they have implemented that are a risk to security (i.e. that modem on the server that accepts dial-in with no password)
- In your proposals, design a way to achieve the same functionality securely

If you are consistently considerate in this way, you will at best gain their support, and at worst keep the grumbling merely grumbling.

2.5 Get to know the Network Admin

The domains, fates and lives of the Network Admin and the Security Admin are inextricably entwined, since their domains include a common set of resources, but their goals are at odds. The job of the network Admin is to provide the highest degree of connectivity possible, and the job the Security Admin is to limit that connectivity to the minimum necessary – and then control even that. Both parties must understand neither mission can succeed (for long) without the success and cooperation of the other side. An antagonistic relationship here can very quickly devolve to all-out war – which would spell disaster for both parties.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

You must build a friendly and solid working relationship with the Network Admin. Below is some sage advice on how to do this:

- Understand the Network Admin's personality, working style, tools and resource limitations
- Consider all these factors in proposed changes to policy and procedures
- Involve the Network Admin in the development of relevant proposals in policies and procedures
- Lend a hand to help the Network Admin do his/her job when possible. It will build goodwill, and will educate you on the networking infrastructure.

3 Understand your playing field

3.1 The Legal Environment

You must understand the laws that apply to Information and IT resources. These are the legal supports behind Information Security activities. If you are transitioning from the world of IT Support to that of Information Security, this is the biggest 'new thing' that you're going to have to worry about. The relevant laws define both your responsibilities and your potential legal liabilities (see Section 4.1 – Protecting Yourself). Below are the four most important transgressions to remember[2,3], along with URLs for further reference.

Transgression	***Details / Source***
Accessing privately-owned Information without the owner's authorization is a crime	Federal Communications Privacy Act – US Code, Title 18, Section 2701 http://www4.law.cornell.edu/uscode/18/2701.html
Damaging or Denying the use of a Computer System while accessing privately-owned Information without the owner's authorization is a crime	Damaging or denying the use of a computer, intentionally or unintentionally with reckless disregard for the risk, is illegal. Note that "damage" does not have to be physical, it only has to cost money to make right. Federal Computer Fraud and Abuse Act - US Code, Title 18, Section 1030 http://www4.law.cornell.edu/uscode/18/1030.html
Hacking for Profit is a crime	The following activities are illegal when done with intent to defraud: • Trafficking in unauthorized access to computer systems (i.e. selling passwords or the locations of compromised computers). • Possessing, producing or trafficking in counterfeit or unauthorized "access devices" (PINs, Credit Cards, Credit Card Numbers, etc.) • Possessing, producing or trafficking in hardware or software that grants unauthorized access • Tricking someone into providing their "access device" to you or for your purposes Federal Computer Fraud and Abuse Act – US Code, Title 18, 1029

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	http://www4.law.cornell.edu/uscode/18/1029.html
Accessing Trade Secrets without authorization is a crime	Covers compromise of Non-patented information critical to a business or the US Gov't with intent to benefit economically (also includes international economic espionage) US Code, Title 18, Section 1832 - http://www4.law.cornell.edu/uscode/18/1832.html

Note that we do not even mention:

- The many, many more Laws that come into play when the computer or information in question is owned and operated by the US Federal Government.
- Any of the State laws that may apply
- Patented information (since a patent is not infringed by someone having knowledge of the patented technology, only by someone profiting form it.)

Cardinal Rule: When in doubt, consult your company's legal counsel.

3.2 Company Policies

You must understand your company's policies and requirements with respect to Information Security. Whereas transgression of the applicable laws can land you in jail, transgression of Company Policy (by an employee) can be grounds for termination or other disciplinary actions.

Understand that greatly varying company cultures lead to greatly varying company policies. When walking into a new situation, assume nothing. Policies that seem reasonable to one organization may be thought scandalous by the next. It's up to the user to understand these policies before accessing the company's IT systems or the data thereon – and it's up to you to understand these policies before attempting the far more intrusive activities required to implement security.

If there are no defined applicable company policies, consider yourself lucky – you are now in a position to create or help shape them. (See section 4.3.3.2.1 Policies and Procedures)

Another good reason to understand the Company Policies is that you will eventually teach them to the users.

3.3 Level of Service

Information Security solutions can be intrusive: they can limit IT performance, accessibility and functionality. You must understand the level of service required and expected from the IT infrastructure before designing those solutions. You must also understand what the company's popular expectation of availability is.

Level of Service is most often defined in terms of "the required number of nines." The statement "Availability must be 99.9%" means that the Information System must be 'available' (however that is defined) 99.9% of required uptime. For instance, consider an Information System that's:

- Required to be available from 6 am to 12 midnight Monday through Saturday (18 x 6 hours)
- Required to be available from 8am to 5 PM on Sunday (9 hours)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For a total operational requirement of 117 hours of availability per week. Then:

- 90% availability ("1 Nine") during the 117 hours of required availability per week, means that the system can be unavailable no more than 11 hours and 42 minutes per week during required uptime, to meet operational requirements
- 99% availability ("2 Nines") permits no more than 1 hour and 10 minutes of downtime per week
- 99.9% availability ("3 Nines") permits no more than 7 minutes of downtime per week
- 99.99% availability ("4 Nines") permits no more than 42 seconds of downtime per week

Then you must define "availability." Delving into this can of worms will probably whittle down to a few specific servers, resources and networks to which the availability requirement really applies.

Consider the following questions:

- <u>What level of service is required for business reasons?</u> A company whose income comes from internet-based sales will need a much higher level of IT service than one that makes washing machines.
- <u>What level of service is expected?</u> Due to history or lack of understanding, a company may have unrealistically high or low assumptions of what level of service is required from its IT infrastructure. If so, the company may resist your proposed security solutions. You must be prepared to back up your proposals with sound business reasons. If you can translate security risks into dollars, justifying the high/low cost of the security solution is much easier.

4 Take Aim

4.1 Protect Yourself

Just like a law enforcement officer, you will run some personal risk simply in doing your job. You will have to manage that risk just like any other. Below are some good places to start.

4.1.1 Define your job

1. Keeping Company Policies in mind, create a document that clearly defines:
   a) Your job responsibilities to as great a level of detail as possible, for example:
      - Sole responsibility for determining password policies on all servers, and shared responsibility with the server team for implementing that policy
      - Sole responsibility for conducting all Server access audits, and maintaining audit records
      - Sole responsibility for maintaining and configuring the Firewall and Intrusion Detection Systems
      - Shared responsibility, with the network team, for configuring all border routers
      - Shared responsibility, with management, for defining and maintaining Information Security Policies
      - Etc., etc.
   b) What IT components you will need access to and to what degree, for example:
      - Admin access on the company NT Domain
      - Root access on all Unix fileservers
      - Root access to the border routers
      - Read access to all internal routers
      - Exclusive, root access for myself [and my backup] to the Firewall
      - Read access to the network team's syslog server

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Etc., etc.

c) Exactly what company information you will need access to, for example:
   - All data stored on users' hard drives
   - All user data stored on company fileservers
   - All user passwords
   - Any data that can be captured by sniffer on the network
   - Etc., etc.

2. Get agreement and buy-in from your manager on this document
3. Get your manager to get agreement and buy-in from company management on this document
4. Sign this document, and get your manager to sign it.
5. Ensure that all IT resource administrators are made aware (preferably by management) of your responsibilities.

4.1.2 Get Permission

For each potentially sensitive security assessment activity you plan to undertake, get documented, signed authorization from management. This should include things like:

- Host and Port Scanning
- Capturing Data on the Network (sniffing)
- Attempting to crack user passwords
- Identifying vulnerabilities on any IT system by examination (Blue Teaming)
- Identifying vulnerabilities on any IT system by attempting to break in (Red Teaming)
- Accessing any company data, regardless of sensitivity, in the course of doing your job
- Etc., etc.

Why bother? Well here's what can happen: In 1995, Randall Schwartz, a well-respected security professional, was convicted of three felony counts under Oregon's Computer Crime Law, due to his completely legitimate security activities as a consultant to the Intel Corporation. Get the full details at http://www.lightlink.com/spacenka/fors/. This can happen to you!

Your goal is to get the authorizations required to protect you from becoming criminally liable or getting fired for breaking company policy by:

- Accessing sensitive company data
- Inadvertently affecting the availability or integrity of company IT resources

4.1.3 Identify all Stakeholders

Before implementing new policies/procedures, identify everyone who could be affected. You may, in the end, decide to promote a policy that will affect the way things are done, but this should be done consciously, rather than by surprise (for the sake of courtesy and your career.)

Before undertaking potentially sensitive security assessment activities, identify everyone who could be affected by a change in the availability or integrity of the IT resources you'll be working with. If the risk is non-trivial, try to schedule the activity to minimize potential impact to the stakeholders.

4.1.4 Communicate, Communicate, Communicate

The more aware people are of upcoming changes, the better they can prepare for that change and its potential side effects – and the more they will appreciate it. Consider the following:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Changes in policy/procedure that will affect large groups of people should be formally announced by management
- If only a small, well-defined group(s) of people will be affected, inform them of the new policies/procedures directly and informally
- The longer notice you can give, the more people will appreciate it
- Spread the news by whatever it takes: send emails, post paper notices on the wall, publish in the company newsletter, attend the staff meetings of other departments, etc.

4.1.5 Get Training

A well-rounded security administrator is comfortable with both the policy/procedure and the technical sides of Information Security. If you are weak in one of these areas, ask for and get training. You may wish to go beyond this and get certified in one or more areas of Information Security.

An excellent list of many of the certifications available today is available at:

- http://www.sans.org/infosecFAQ/start/how_to.htm

In addition, there are most likely several commercial IT training providers local to you that offer security-related training.

4.1.6 Become Paranoid

As the security administrator, it is your responsibility to cultivate an appropriate degree of paranoia. You should assume that:

- Hackers are trying to break in right now - you just haven't noticed yet
- Hackers have already successfully compromised machines on your network – you just haven't found it yet
- There are vulnerabilities on your hosts and network that you haven't found yet
- Unauthorized users are accessing data and resources right now for well-meaning purposes
- Unauthorized users are accessing data and resources right now for nefarious purposes
- Unauthorized users are sending proprietary company data across the internet in the clear and/or to unauthorized individuals
- Users are making proprietary company data available to unauthorized individuals (within and without the company) through wide-open web servers, ftp sites, NT shares, modems on their desktop machines.
- Users are making proprietary company data available to unauthorized individuals (within and without the company) through inappropriate placement on official company web servers, ftp sites, etc.
- Etc., etc.

This may seem strange at first, especially if you were previously an administrator of IT resources (when connectivity and access was a good thing.)

4.2 Determine what you're Defending

Before you can properly secure your company's Crown Jewels, you have to identify them.

4.2.1 The Crown Jewels

Information Security is built on the following three fundamental principles:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Confidentiality The capability of an Information System to protect its data from access by unauthorized individuals or their agents.

Availability The capability of an Information System to keep its resources and data available to its users despite disruptive events or conditions.

Integrity The capability of an Information System to provide its services and process its data such that its data is never altered (changed, corrupted, moved or destroyed) except as intended by authorized users.

To identify the Crown Jewels, you must review Information System resources in each of these three areas.

To identify the Crown Jewels of Confidentiality, ask and find the answers to the following types of questions:

- What company data, if divulged to a business competitor, would hurt our competitiveness or put us out of business? For example:
  - Trade secrets
  - Business plans
  - Project schedules & budgets
- What company data are we legally required to keep private? For example:
  - Data belonging to another company, that's covered by a non-disclosure agreement
  - Data involved in a lawsuit or other legal action
- What company data would we be wise to keep private? For example:
  - Salaries, personnel reviews and other HR-related information
- What company data, if available to hackers on the Internet, would open us up to attack?
  - Network diagrams and configurations of network devices
  - DNS Tables
  - Company Directory (email and/or phone)
- What company data, if available to a disgruntled employee, would open us up to attack?
  - His cube-mate's password written on a Post-it and stuck to the bottom of his mouse pad
  - The combination to the cabinet where the server backup tapes are stored
- Etc., etc.

The Crown Jewels of Availability can be determined by ranking Information System resources according to how tolerant business operations are to their unavailability. Ask and find the answers to the following types of questions:

- What Information System resources, if unavailable or degraded in availability for a matter of minutes, could do non-trivial damage to business operations? For example:
  - E-Commerce Web Servers
  - UPS Power in the Data Center
- What Information System resources, if unavailable or degraded in availability for a matter of hours, could do non-trivial damage to business operations? For example:
  - DNS Servers
  - Mission-critical Database Servers
  - The Computers running an Assembly Line
  - The company network
  - Power to the Data Center

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

  - Environmental Controls in the Data Center (e.g. Air Conditioning)
- What Information System resources, if unavailable or degraded in availability for a matter of days or weeks, could do non-trivial damage to business operations? For example:
  - Email Servers
  - Internet Access
  - Desktop Workstations
  - Data Backup Servers and Peripherals
  - Information System Administrators

The Crown Jewels of Integrity are those resources whose alteration or corruption could do non-trivial damage to business operations. For example:

- Mission-critical Databases
- Company Accounting and Financial Data
- The email accounts of company officers
- Critical Data that resides on a User's workstation, rather than a server, and does not get regularly backed up.
- The Company Website
- The Company Firewall, Intrusion Detection Systems and other devices the implement and monitor security

4.2.2 Perform a Risk Analysis

A Risk Analysis is a formal determination of the level of risk to the confidentiality, availability and integrity of an information system. It is a document that you will create and present to management to give them the information they need to determine:

- What the risks are to the company from a business point of view (think dollars)
- Which risks are acceptable to them, and which are not
- How much money and effort they can/should/must spend to counter the unacceptable risks
- If/what changes should be made in the way business is done

4.2.2.1 Identify Vulnerabilities

Vulnerabilities are <u>those aspects of the Information System</u> that open it up to risk of loss of confidentiality, availability or integrity. Vulnerabilities come in many flavors, examples of which are listed below:

- Technical
  - Application
    - Poorly configured applications such as ftp servers with accounts but no passwords, tftp servers configured to serve from the root of a filesystem, PC Anywhere running on a user's desktop with no password
    - Applications that are inherently insecure due to their design, such as rlogin, rcp, rexec, etc.
    - Applications with known vulnerabilities that have not been patched, updated or removed, such as ToolTalk, Calendar Manager and rpc.statd
  - Host
    - Hosts running unnecessary daemons and services
    - Computers not up-to-date on their operating system patches
    - Shared C:\ drives on Windows computers

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

  - Network
    - Lack of network perimeter protection such as router filters and firewalls
    - Lack of internal network protections for the more critical resources
    - Disclosing too much information by allowing ICMP in from the Internet
    - Disclosing too much information by allowing full DNS access from the Internet
- Non-Technical
  - Physical & Environmental
    - Uncontrolled physical access to spaces containing critical Information System resources
    - Insufficient electrical power capacity in the Data Center
    - Water-sprinkler-based fire suppression system in the Data Center
    - Data Center located in the basement of a building prone to flooding
    - Backup Tapes stored in close proximity to the Servers they backup
  - Policy & Procedure
    - Out-of-date, insufficient or non-existent Information System Security Policy
    - Undocumented or nonexistent procedures for System Administrators
    - Lack of defined roles and responsibilities within the Administration staff
  - Education, Training & Awareness
    - Lack of awareness of security risks, policy, procedures, responsibilities on the part of System Administrators and Users
    - Lack of System Administrator training on how to securely configure applications, hosts and networks
    - Lack of User training on how to use the security-relevant tools available to them
  - Lack of commitment to security by management

Your job is to identify and rank the vulnerabilities to start building your game plan.

4.2.2.2 Identify Threats

Threats are those agents and conditions <u>external to the Information System</u> that can exploit vulnerabilities to compromise the confidentiality, availability or integrity of the Information System.

Threats can be categorized along the following two axes:

Physical vs. Virtual Physical Threats are those threats over which you have some degree of control due to the Information System's physical environment and security controls. Virtual threats are those that can strike regardless of the physical security measures you put in place.

Friendly vs. Hostile Friendly Threats are unintentional threats, which can often be controlled through security training, education and awareness. Hostile Threats cannot be trained, educated or talked out of their course

You then start populating the resulting categories, for example:

- Physical/Friendly
  - Inexperienced and/or Overworked System Administrators

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

  - Company Executives walking out with sensitive company information on a floppy so they can work from home, and then copying it onto their unsecured home computer on the Internet via an "always-on" Cable modem
  - That Company Secretary willing to hand out copies of the Company Directory to anyone who asks (and thereby opens you up to Social Engineering attacks)
  - That eager-to-help System Administrator willing to create an account for a 'new employee' who begs for one at 11pm on a Sunday night (the same guy who finagled a copy of the Company Directory from the secretary)
- Physical/Hostile
  - That disgruntled employee
  - Thieves and Vandals breaking in at night
  - Corporate Spies
  - Natural disasters such as fire, flood, earthquake, etc.
- Virtual/Friendly
  - Inexperienced and/or Overworked System Administrators
  - Uninformed Users emailing sensitive company information outside the company
  - Company Executives emailing sensitive company information to their home email accounts so they can work from home
  - That uninformed user who opens up email attachments from unknown sources
  - An unreliable or inexperienced ISP
- Virtual/Hostile
  - Malicious Hackers (Cyber-vandals)
  - Cyber-criminals (Hacking for Profit)
  - Corporate Spies
  - That disgruntled employee

Note that the line between Threats and Vulnerabilities sometimes seems fuzzy. This is normal. Some risk assessment approaches do not try to make the distinctions crystal clear.

Also note the following:

Cardinal Rule: The greatest threat is always from the Inside

4.2.2.3 Determine and Document the Risks

Once the Threats and Vulnerabilities have been identified, it's time to determine the risk. For each Threat/Vulnerability pair, determine:

- Impact: The degree of damage that could be done
- Probability: The likelihood that a vulnerability could be exploited by a threat

To understand and assess the potential Impact of a Threat/Vulnerability pair, you must:

- Ask System Administrators:
  - ID Resources: If Threat A were to exploit Vulnerability B, what Information System resources could be compromised?
  - Confidentiality: If resource X was compromised what data could be disclosed to unauthorized persons?
  - Availability: If resource X was degraded in performance or unavailable for minutes/hours/days/weeks what business tasks and operations would be affected and how?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

  - Integrity: If the data on resource X were to be corrupted/altered/deleted, what business operations would be affected? How would the corruption/alteration/deletion be detected? Would a backup be available, or would the data have to be recreated from scratch? How long would it take to restore from a backup? How reliable is the restore process? Is it routinely tested? How long would it take to recreate the data from scratch?
- Then ask company management what the impact could be to business operations, company competitiveness and company viability if:
  - Confidentiality: Data X, Y and/or Z were to be disclosed to the wrong persons?
  - Availability: Business Tasks and Operations X, Y and/or Z were to be slowed or stopped for a matter of minutes/hours/days/weeks?
  - Integrity: Data X, Y and/or Z were corrupted? Inappropriately altered by unauthorized but well-meaning persons? Maliciously altered by unauthorized persons? Irretrievably lost and had to be re-created from scratch?

Once you know and understand the answers to these questions, you can assign qualitative labels or numerical values to the impacts.

To understand and assess the probability of an exploit, you must research each threat. You have to understand:

- How many hackers are searching the Internet at any given moment for the next notch on their belt?
- How many hackers are searching the Internet at any given moment for the next quick buck or stolen credit card number?
- How many organized criminal organizations at any given moment are targeting companies for purposes of information theft or extortion?
- How many users unthinkingly email out proprietary information to unauthorized persons?
- What's the likelihood of an engineer or manager's home PC being compromised? While storing company proprietary data?
- Which vulnerabilities require real technical skill to exploit, and which have exploit scripts widely posted on the web that can be run by any 13-year old with access to mom and dad's PC?
- Etc., etc.

This information is available in many Information Technology magazines and Information Security-related websites, such as:

- Windows NT Magazine
- Information Week Magazine
- Network World Magazine
- www.incidents.org Overall Threats and Trends across the Internet
- http://www.ntsecurity.net/ Windows NT Security
- http://www.yassp.org/ Host Security with the Solaris Operating System
- http://www.sonic.net/hypermail/security/ Host Security with the Linux Operating System
- http://www.sabernet.net/papers/hp-ux10.html Host Security with the HP/UX Operating System

There are many others.

Once you've identified and assessed the Threats and Vulnerabilities, you can assess the risk as:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk = Impact x Probability

You can do this using qualitative terms to come to qualitative results, or you can assign numerical values and calculate a quantitative result. For example[4]:

Assessment of Probability	***Qualitative Probability***	***Quantitative Probability***
Unlikely to occur	**Negligible**	**1/7**
Likely to occur once every five or more years	**Very Low**	**2/7**
Likely to occur once every year or less	**Low**	**3/7**
Likely to occur once every six months or less	**Medium**	**4/7**
Likely to occur once per month or less	**High**	**5/7**
Likely to occur multiple times per month or less	**Very High**	**6/7**
Likely to occur multiple times per day	**Extreme**	**7/7**

Assessment of Impact	***Qualitative Impact***	***Quantitative Impact***
No significant impact.	**Trivial**	**1**
Minor, perhaps localized, effect to business operations and objectives. Minor effort required to repair the damage.	**Minor**	**2**
Significant effect on business operations and objectives. Significant effort required to repair the damage.	**Significant**	**4**
Serious effect on business operations and objectives. May result in the loss of customers or business confidence. May result in marked drop in business competitiveness and stability. Effort required to repair the damage would seriously tax the company's resources	**Serious**	**7**
Could put the company out of business. Effort required to repair the damage may be beyond the company's resources.	**Grave**	**10**

The two scales given above would define a 35-point risk scale ranging from 0 to 10 in value, to which you can assign qualitative descriptions:

Description of Risk	***Qualitative Risk***	***Quantitative Risk***
No significant impact.	**Trivial**	**1**
Minor, perhaps localized, effect to business operations and objectives. Minor effort required to repair the damage.	**Low**	**2**
Significant effect on business operations and objectives. Significant effort required to repair the damage.	**Moderate**	**4**
Serious effect on business operations and objectives. May result in the loss of customers or business confidence. May result in marked drop in business competitiveness and stability. Effort required to repair the damage would seriously tax the company's resources	**Dangerous**	**7**
Could put the company out of business. Effort required to repair the damage may be beyond the company's resources.	**Fatal**	**10**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The definitions given for probabilities, impacts and risks are only an example. It is important that you come up with scales and definitions that apply to your situation and environment.

Cardinal Rule: Good security is always a custom fit.

The final Risk Assessment Document should include the following sections:

- Purpose: What is the purpose of this document?
- System Definition: List/Description of all the components of the Information System. Should define exactly what it is we're assessing the risk to.
- Vulnerabilities: Should list all the vulnerabilities you've identified, and discuss the more serious ones in detail
- Threats: Should list all the Threats you've identified, and discuss the more serious ones in detail
- Risk Assessment: Should list all the resulting risks, and discuss the greatest risks in detail

The Risk Assessment section should culminate in a table or list of all the risks in descending magnitude. Here's an example:

Risk	***Quantitative: Risk = Prob x Impact***	***Qualitative Risk***
Hacker compromise of many machines on our network due to the lack of a firewall on our Internet connection and Intrusion Detection Systems inside our network	**7/7 * 7 = 10**	**Fatal**
Potential Legal Liability due to Compromise of Customer Credit Card Numbers by Hackers	**5/7 * 8 = 5.7**	**Dangerous -**
Compromise of company proprietary information due to the current X-Windows-based database access design combined with the current policy of allowing employees to connect over the internet	**5/7 * 7 = 5.0**	**Moderate +**
Compromise of proprietary manufacturing process data (trade secrets) due to Engineers being allowed to carry work home on floppies	**5/7 * 6 = 4.3**	**Moderate +**
Compromise of proprietary business plan, financial and project data due to company executives being allowed to carry work home on floppies	**5/7 * 6 = 4.3**	**Moderate +**
Destruction of all Servers due to a fire or false alarm with the water-based sprinkler system in the Data Center	**3/7 * 10 = 4.3**	**Moderate +**
Compromise of multiple systems due to the lack of physical access controls to the Data Center	**3/7 * 10 = 4.3**	**Moderate +**
Loss of data due to unreliable backup devices and undocumented procedures	**6/7 * 4 = 3.4**	**Moderate -**
Compromise by hackers of our Unix workstations, most of which have the out-of-the-box configuration of many vulnerable and unneeded services running (i.e.: DNS, SMTP, NFS, SNMP)	**7/7 * 3 = 3.0**	**Moderate -**
Compromise by hackers of our external DNS server due to the old, unpatched version of RPC running on it.	**7/7 * 2 = 2.0**	**Low**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Corruption, loss or compromise of our Customer Database due to current network design of putting the database server on the same host as our email server	**5/7 * 3 = 2.1**	**Low**
Unauthorized employee access to proprietary information due to a non-existent password policy on our NT Domain	**6/7 * 2 = 1.7**	**Low -**
Etc, etc…	**…**	**…**

4.3 Plan your attack

Once you've completed a Risk Assessment, you're ready to plan your attack. This will be in the form of another document, the Network Security Plan (NSP), that you will create and present to management at the same time you present the Risk Analysis.

4.3.1 Include appropriate stakeholders

From the stakeholders you've identified, identify those you trust the most and include them in your planning. Show them outlines and drafts of your NSP as you develop it. They may find something you've missed, or inform you of a political or cultural obstacle you were not aware of.

4.3.2 Prioritize your targets

If you've done the Risk Assessment, you've done 90% of the prioritization for your NSP. Review your Risk Summary, look for the following things, and tweak the NSP's priorities appropriately:

- Chained risks. Some risks in your list, if mitigated, automatically mitigate other risks in your list. These should be given higher priority. For example, installing a firewall and intrusion detection system would generally lower the overall risks to hosts.
- Low or moderate risks that have low probability of occurrence, but would put you right of business. These may be good bets - but you're betting your life. For example, a fire in the data center may be unlikely, but triggering the water-based sprinkler system in your data center would destroy your most critical servers. These types of risks would not appear near the top of the Risk Summary, but should probably be in the high-priority section of your NSP.
- Low or moderate risks that are trivial to mitigate or eliminate. This is a good way to lower your overall risk with little effort.

4.3.3 Choose your weapons

To address each risk, you must choose a Risk Mitigation Measure (RMM) from one of the following two categories:

- Technical: A security-enhancing change or reconfiguration of the Information System itself
- Non-technical: Any other else you do to enhance the security of the Information System

It's easy to assume that a few strong Technical RMMS are good enough – don't be fooled. It takes an array of RMMs from both categories and at many levels to achieve good security. This is called Defense in Depth.

Cardinal Rule: Defense in Depth. Don't depend on network, host or application-level security alone.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4.3.3.1 The Non-Technical Arsenal

4.3.3.1.1 Policy & Procedure RMMs

An Information System Security Policy (ISSP) is ***THE*** most important RMM you can put in place. Everything else flows from the policy. The ISSP should clearly and succinctly describe[5]:

- The Purpose, Scope and Lifetime of the Policy, including cancellation and update requirements
- The Company Policy specific to each aspect of the Information System, for example:
  - Acceptable Use Policy: Defines what an employee is and is not allowed to do with company computing resources.
  - User Access Policy: Defines the policy, prerequisites and procedures for getting user-level access to company computing resources, and the responsibilities that come with that access. Should include policy for regular reviews and audits of access, access revocation, changes in access, etc.
  - Special Access Policy: Define the policy, prerequisites and procedures for getting Admin-level or other special access to company computing resources, and the responsibilities that come with that access. Should include policy for regular reviews, access revocation, changes in access, etc.
  - Network Connection Policy: Define the policy, prerequisites and procedures for connections to the company network, and the responsibilities of the connecting individual or entity. Should include policy for WAN/MAN links, dial-in connections, access from the Internet, wireless access, etc., as well as for regular reviews, link revocation, configuration changes, etc. This may also define the policy for special categories of connections, such as branch offices or business partners.
  - Incident Handling Procedures: Define the policy and procedures for handling Security Incidents
  - Security Incident Escalation Procedures: Define categories of Security Incidents, the policy and procedures for handling each category, and the escalation process from one category to another
  - Issue Specific Policies: Define the policy, requirements and procedures for specific issues such as
    - Password policies such as length, strength (complexity) and maximum lifetime, etc.
    - Account Policies such as lifetime, administrative lockout, concurrent logons, etc.
    - Anti-virus Policies such as the use of Anti-virus software at the desktop/server/firewall/email gateway level. Virus incident handling procedures
    - Data Backup Policies such as what data will be backed up and how often, how often the restoration of that data will be tested, and how/where the backup media will be stored
    - Proprietary Data Handling Policies such as defined categories of data sensitivity and the policies for handling each one
    - Etc., etc.
- Formal Roles and Responsibilities of Users, System Admins, Backup Operators, Network Administrators, Security Administrators
- Related Documents (References) such as charters, process definitions and procedures
- Special Cases and Exceptions to the Policy, if any
- Special topics particular to your Information System, if any

The policy must[6]:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Describe **What** must be done well enough that the **How** can be identified, measured and evaluated.
- Be clear, concise and realistic
- Be consistent with higher-level policy, if it exists
- Protect the company's information
- Protect the people who use and administer the Information System by empowering them to do the right thing
- Be well-publicized and easily accessible to all company personnel

Finally, you should seriously consider making the following mandatory:

- User Policy Agreement: A 1-page statement to be signed by the user that acknowledges full understanding of the ISSP and the user's roles, responsibilities and limitations. This statement must be signed before a user account is granted.
- Admin Policy Agreement: A 1-page statement to be signed by the System Admin that acknowledges full understanding of the ISSP and the Admin's roles, responsibilities and limitations. This statement must be signed before an Admin account is granted.
- Similar Agreements for any special case Roles you may have on your Information System.

Cardinal Rule: If the ISSP is complete and well written, everything else you need to do will flow naturally from it.

For more information and excellent samples of security policies, go to http://www.sans.org/newlook/resources/policies/policies.htm

Once the ISSP is written, and all the **Whats** are defined, then the **Hows** need to be defined, in the form of written procedures and processes. Each area of policy may need one or more procedures written to it. Procedures may change as hardware, software and people come and go within the Information System, but a change in policy is a change in how you do business and should only change for good reason. For example:

- Process for creating a User Account:
  - The requestor fills out the "User Account Request Form", specifying for which data access is requested, and get it signed by his/her manager
  - The requestor reads and signs the "User Policy Agreement"
  - If access to proprietary information is requested, the forms are routed to the Director of Engineering for approval
  - Once all required approvals are obtained, the form is routed to the Help Desk, who will check for completeness and then open a Trouble Ticket for the Accounts Manager
  - The Accounts Manager will create the account and grant the approved permissions
  - The Help Desk will confirm with the user that the account is functioning properly and then close the Trouble Ticket

Each procedure should be written by the individual in charge of the process. Expect to write the security-relevant processes yourself, and for System Admins and others to write the rest.

4.3.3.1.2 Physical Security RMMs

You NSP should include whatever new or enhanced Physical Security controls are necessary to protect the Confidentiality, Availability and Integrity of the Information System from Physical Threats. For example:

- Locks on doors

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- New doors and walls installed where appropriate
- Automated access control systems that grant access to individuals based on a physical token, such as a keycard
- Security guards
- Relocation of equipment to more secure spaces
- Relocation of equipment to spaces or buildings more protected from natural disasters such as floods or earthquakes
- Relocation of equipment to spaces or buildings with more adequate or reliable power or environmental controls
- Locked cabinets and equipment racks
- Fireproof safes for storage of backup media
- Offsite storage of backup media, etc.

4.3.3.1.3 RMM: Insert yourself into appropriate processes

Your Security plan should insert you, the Security Administrator (or members of your staff, if appropriate), into existing business processes that need security-related controls and planning. For example:

- Add Security to the approval process for content changes on publicly available websites, FTP sites, etc.
- Add Security to the Training curriculum for all System Admins
- Require signed non-disclosure forms as a term of employment
- Require Security input into the design and layout of new facilities
- Require Security approval for Information System architecture changes
- Provide Security-related training for all new employees

4.3.3.1.4 RMM: Management Education and Awareness

It's easy for an organization to implement a few security measures, consider the problem solved and then forget about it. You need to ensure that management is aware that security must be maintained forever for good business reasons and then keep it on their minds. Find a way to regularly provide status and discuss issues with senior management face-to-face so that security awareness stays alive in their minds. For example, once a month, attend the weekly senior management meetings and give a brief report on the status, projects and open issues in Security.

Some managers feel they are above the law or feel they can bend the rules in a pinch. You will have to consistently find ways to demonstrate to them the actual value (preferably in dollars) of sticking to the rules. Scan the trade magazines and news websites for true stories of what can happen when security is neglected or ineffective, go over these stories at your meetings with management to hammer in that every employee is responsible for maintaining security. (You can also use them to back up your proposed projects and expenditures.)

Face time is the key - it should be part of your NSP.

4.3.3.1.5 RMM: User Education and Awareness

What you must do carefully with management, you can do more openly with users and System Admins. Create resources, preferably on a website, that anyone can go to to get the latest policies and procedures. Include links to Internet-based security resources, information and news. Hold regular, say semi-annual, security refresher briefs for all employees. Face time is the key - it should be part of your NSP.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For a smorgasbord of security awareness resources, go to:
http://www.sans.org/newlook/projects/cap_draft.htm

4.3.3.1.6 RMM: IT Staff Education

With System Admins, you must go beyond on the security education, training and awareness sessions given to all users. One good way to do this is to attend staff meetings. As with senior management, regularly attend, say once a month, weekly staff meetings to discuss new security news, developments, issues and projects. Give presentations on special technical topics, such as vulnerabilities of an operating system, daemon or application, or explain the company's firewall or split DNS configuration. Face time is the key.

4.3.3.2 The Technical Arsenal

Cardinal Rule: Prevent -> Detect -> Respond.

Prevention is best, but you'll never prevent all incursions (unless you turn your system off.) You must be able to detect what you did not prevent, and you must then be able to respond to the incursions you detect. The prevention and detection are usually automated (technical) or mostly so, and the response is usually manual action by individuals who know what they need to do and are empowered by an Incident Handling Policy and Procedures (non-technical).

Assuming reasonable Information System design and budgets, the intrusion of unauthorized persons – internal and external - is probably the biggest threat to the confidentiality, integrity and availability of your Information System and data. You will find that most of the Technical tools in the arsenal are geared to Prevent, Detect and Respond to that threat.

4.3.3.2.1 Network Perimeter Protection RMMs

Your network's perimeter consists of those points at which it connects to the outside world, such as:

- Your Internet connection(s)
- WAN Links to business partners or any other network outside your administrative domain
- Modems installed on computers on your network that are connected to the public telephone system
- Wireless LANs on your network that can be accessed by anyone with the right equipment who's close enough

Protecting your network perimeter amounts to having no unprotected connectivity with the outside world. For each point of connectivity, you must either put controls in place, or disconnect it.

Firewalls are the primary means of protecting your Internet connections and WAN links. Since the Internet is where the greatest number of hackers reside, this is a critical component. Firewalls come in several flavors:

- Filtering Routers: Filtering routers examine network traffic at the Network and Transport Layers. They know what types of packets are permitted between which source and destination IP addresses, and filter accordingly. Permitted packets are routed/forwarded and the rest are dropped. These devices are "stateless" in that they are unaware of the state of each network connection they support. This means that applications that have

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

even slightly complex behaviors cannot be handed securely. For example: a normal FTP session switches between an outbound connection on TCP Port 21 to an inbound connection on TCP Port 20. With only a filtering router you'll either have to block FTPs or open up a bigger hole than you really want to. Filtering routers provide a reasonable – if inflexible – level of security with a minimal network performance hit.

- Stateful-Inspection Firewalls: Like a filtering router, these firewalls examine network traffic up to the Transport Layer. The difference is that they are aware of the "state" of each connection in progress, know what behavior to expect next and can handle it securely. For example, these firewalls are aware of FTP's normal behavior, and can handle it securely. Stateful-inspection firewalls provide a good, flexible level of security with a low-to-moderate network performance hit.
- Proxying Firewalls: Also known as Application Gateways. These stateful firewalls examine network traffic content all the way up to the application level - to the commands issued and data exchanged within applications – and can filter accordingly. For example, they can be configured to
  - Allow certain FTP commands, but not others
  - Allow Web access but block Java or JavaScript
  - Monitor permitted connections for well-known exploits/hacks and break the connection upon detection

  Proxying Firewalls provide the greatest and most flexible security and come with the most expensive performance hit.

Many organizations implement firewalls in more than one category: one common configuration is a Proxying Firewall sandwiched between two Filtering Routers. This blocks most of the "bad" traffic before it gets to the Proxying Firewall therefore lightening its load and improving network performance. Other sites use Proxying firewalls for the services they're most concerned about, and lesser firewalls for the rest.

Commercial Firewalls are available in each of these categories, and some products have features from more than one category. Beware that the higher-end firewalls are not cheap – if you have a non-trivial network – say more than 50 nodes – you will spend some serious money here. You could take the path of implementing your own home-brewed Firewall or using the Gauntlet Firewall Toolkit - but these options take a considerable amount of technical skill, so be sure you know what you're getting into before committing to this path.

You could allow users to have modems in their machines, but you will then spend a large amount of your resources ensuring that they are configured securely. The vast majority of companies today forbid this by policy. Instead, the IT Staff provides a centralized dial-in capability that can be much more easily secured and controlled. This can provide capabilities such as:

- Username/password just to connect, in addition to the username/password to log into the network
- One-time passwords
- Node-to-network encrypted dial-in connections (Virtual Private Network or VPN Connections)

In addition, this centralized dial-in facility can itself be placed behind a Firewall, to add another layer of protection. This centralized, perhaps firewalled, dial-in capability is the recommended approach.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Wireless LANs are the newest hole in the network perimeter. If you use Wireless, an unauthorized person (malicious or not), can sit in his/her car parked just outside your building, and access your network: sniff the traffic of legitimate Wireless users, surf the web at your expense or access your proprietary information. There is a Wireless Encryption Protocol (WEP) built into the most popular version of Wireless, but this encryption is weak, and will stop only the casual intruder. Instead, you could implement a full-blown Virtual Private Network here, to encrypt the traffic more adequately. You can save some money here by implementing a single VPN and using it for both dial-in and Wireless network clients.

A Final Note on Firewalls:
It's very common to think of a Firewall as the ultimate protection against all evil. This is foolishness!

- Firewalls can be circumvented by a single user with a modem in their PC.
- Malicious hackers can exploit existing trust relationships that are allowed through the firewall.
- You and/or the System Admins may not be aware of all existing trust relationships. Some exist by design, and some may not. Some are only apparent after an analysis of the Firewall/DNS/Email/etc configuration.

Therefore we arrive at the following:

Cardinal Rule: Defense in Depth. Don't depend on network, host or application-level security alone.

4.3.3.2.2 Reconnaissance Information RMMs

Many hackers first gather reconnaissance information on a target before striking. Therefore it is important to keep the amount of information about your network that's available outside your network to the absolute minimum. Here are some common methods:

- Block ICMP: Do not allow ICMP in through your network perimeter (pings, traceroutes and ICMP error and control messages.) This allows external individuals to see that you're there, how many nodes you have, and to which point(s) on the Internet you connect.
- Split DNS: Implement internal and external DNS Servers. Populate the Internal DNS with the full set of info for your internal users. Keep the info on the External DNS pared down to the absolute minimum needed to do business, preferably only the externally-available servers: web servers, email servers, VPN access box, etc.
- Dedicated-purpose machines: Dedicate a machine to each service that must be accessible from the Internet. This will keep each machine's configuration and vulnerabilities simple and compromises easier to catch.

4.3.3.2.3 Encryption RMMs

Encryption is the best protection you can implement against the compromise of the confidentiality of your data, both at rest and in motion. Here are some common ways to use encryption, in increasing order of paranoia:

- Requiring that all users accessing the company network from the Internet use encrypted connections. This will protect against the capture of data as it traverses the Internet, and the identification of your network as a good target for active hacking.
- Requiring all dial-in connections to be encrypted. This will protect against the capture of data as it travels across public phone lines.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Requiring that all WAN Links be encrypted. This will protect against the capture of data as it travels across public data networks. Note that even Point-to-point WAN links traverse multiple items of your providers equipment.
- Requiring that all sensitive information be encrypted before being emailed outside the company. This is usually done with a tool such as PGP to produce an encrypted attachment that can be emailed.
- Requiring that all email sent and received be digitally signed. This assures the receiver that the information received actually came from the apparent sender.
- Requiring that all email send and received be encrypted. This protects all information leaving and entering the company from prying eyes
- Encrypting information stored on externally available servers. This adds a measure of protection to those machines that are most exposed to external threats.
- Encrypting information stored on internal servers. This adds a whole new layer to your total Defense in Depth.
- Requiring all Wireless LAN traffic to be encrypted.

Note that the encryption and digital signatures can be seamlessly integrated into your email system with the deployment of a Public Key Infrastructure (PKI). This is a large and expensive effort, however, and not every company can support or justify it.

4.3.3.2.4 RMM: Network Intrusion Detection

Using Firewalls, limiting reconnaissance information and using Encryption all fall into the Protection portion of the Protect -> Detect -> Respond cycle. Network Intrusion Detection is in the Detection portion.

Here's how it works:

- Most exploits used by hackers are well known, and each has a particular signature
- Some signatures can be quite complex, containing any of the following components: particular/common TCP or UDP ports used, bit-patterns contained, sequences of events, variable time between the events.
- Applications are written that capable of detecting these signatures in a stream of network traffic
- These applications are run on nodes that capture network traffic streams at critical points, such as:
  - The network feed into the Firewall from the Internet
  - The network feed into the internal network from the Firewall
  - The network backbone (if one exists)
  - The network feed to a critical LAN, server or other resource within the network
- Analysts monitor the Alarms and Logs of these Intrusion Detection System(s) (IDSs) and follow-up on suspicious events
- Confirmed intrusions (and other violations of policy) are turned over to those individuals identified as Incident Handlers to handle.

On the Internet, the number of hackers with real skill is actually quite small. These are the people who discover new host and network vulnerabilities and come up with ways to exploit them ("exploits".) However, when these skilled individuals come up with a new exploit, they usually package it up into a script or application and post it on the web. Then it's downloaded by every 13-year-old with access to a PC, a liking of computers, and too much time on their hands. This is what gives rise the vast sea of Internet hackers crashing on the beach of your

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

firewall. This is also why most exploit signatures are well-known. In the Intrusion Detection business, it's a race to discover new exploits, define the needed protections and inform the security community before the exploit becomes epidemic. To peek into this world of Internet-wide security, go to:

- incidents.org
- www.cert.org
- www.infowar.com (a portal to many other sites)

There are many commercial IDSs available today. Some scale to be quite large, usually consisting of many detection nodes logging back to a small set of analysis and management nodes. Some of these can automatically correlate events across several detection nodes, direct firewalls to shut down connections, send email to or page IDS Admins, etc. Be prepared to spend a lot of money on these.

However, there are a few well-known and well-respected public domain (free!) IDSs:

- TCPDUMP: a command-line utility that puts basic network IDS functionality in the hands of the technically knowledgeable (www.tcpdump.org)
- Shadow: a scalable network-based IDS based on TCPDUMP (www.nswc.navy.mil/ISSEC/CID/)
- Snort: A sophisticated and flexible command-line network IDS system (www.snort.org)

Note that a Snort-based version of Shadow is currently in development. Also, a nice summary of commercial and free IDS Systems is available at
http://www.networkintrusion.co.uk/N_ids.htm

4.3.3.2.5 RMM: Create Internal Enclaves

If your network is large and/or complex, or if the Crown Jewels can easily be isolated to a particular LAN or small set of hosts, you should consider this. Working with your Network and System Admins, you may be able to rearrange the resources and users on your network so that they can be easily segregated into logical Internal enclaves. Then you can apply Network Perimeter protections and Network Intrusion Detection to each enclave to further deepen your defense.

Note that this technique also protects your Crown Jewels against internal threats, both friendly and hostile.

4.3.3.2.6 Host Perimeter Protection RMMs

Hosts can be protected by firewall-like perimeter protections just like networks can. On Unix hosts, these usually take the form of tcpwrappers. Tcpwrappers are applications installed between a host's TCP/IP stack and its daemons to:

- Detect port scans (including stealthy ones)
- Control what IP addresses and users can access each daemon
- Control what commands they can execute once connected
- Watch for exploit signatures and break connections upon a detect
- Log all activity to whatever degree of detail is required.

The best-known free tcpwrapper for Unix systems is Psionic Software's PortSentry:
www.psionic.com

4.3.3.2.7 Host Intrusion Detection RMMs

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The most common Host-based IDSs are those that simply check for changed files on your system. The most widely used tool to do this is Tripwire. Tripwire first makes a baseline of your system by calculating checksums for every file you want to monitor. Then the checksums are simply recalculated periodically to look for changes.

Tripwire is available at www.tripwire.com. Commercial versions for a variety of operating systems are available, plus a freeware version for Linux.

More sophisticated host-bases IDSs are now starting to emerge. Psionic Software is developing a product for Unix systems called HostSentry that does host-based IDS based on behavioral signatures. This product is currently available as an alpha "release."

4.3.3.2.8 Application Security RMMs

Application Security is the topmost layer in your Defense in Depth stack. This is simply building into applications the means to protect the confidentiality and integrity of the data handed, and the availability of the application itself (or selecting applications that have them built-in.)

This can take the following forms:

- Confidentiality
  - Usernames/passwords on databases, possibly with record-level permissions
  - Usernames/passwords on any custom applications you develop and use
- Integrity
  - Using supported commercial software rather than shareware or freeware
  - Thorough testing of new applications before deployment
- Availability
  - Mirroring applications or data across multiple resources, possibly in different physical locations
  - Selecting commercial applications with built-in high-availability features
- General
  - Considering security features in your criteria for selecting commercial applications
  - Actually using the security options/features that come with commercial applications

There is no formula for this. You simply have to select applications that meet your security requirements/policy, or write them yourself.

4.3.4 Get Management Buy-in

Ok. You now have a Risk Assessment and draft NSP containing a fully fleshed-out ISSP. You now add the following things to your NSP to make it complete:

- Put a dollar value on as many of the risks you've identified as possible
- Add a mapping of each Policy statement to the RMMs selected from the Technical and Non-technical arsenals
- Add an implementation schedule and manpower required
- Add a spreadsheet containing the cost of implementing your NSP. Include new HW/SW purchases, the labor needed to implement it, and the recurring costs needed to maintain it.

Now you can have your big meeting with Management. Your goal is to sell them an insurance policy in the form of your NSP. The reasons they should buy it are described in your Risk

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assessment and quantified by your mapping of risks to dollars. The cost to them is summarized on your spreadsheet. Note that, if the cost to them exceeds the potential cost of compromise, you're going to have a hard sell.

Wear a suit.

How can you tell if you've succeeded? If you've got management's buy in? Only if the following three events occur:

- Your ISSP is signed into law by management, and distributed to all employees
- You are given the budget you need
- You are given access to the manpower you need

5 Fire

If you have successfully sold management on your NSP, you are now ready to rock'n'roll:

- Assign the proper individuals to write the procedures specified/implied by the policy statements in the ISSP.
- Work with the System Admins, Network Admins and all other stakeholders to implement the NSP according to schedule.
- Publish to all users a summary of the implementation plan and schedule, including any planned and potential service outages.
- Hold briefings open to all users to cover the ISSP, the implementation plan and schedule, and any planned and potential service outages. Distribute in hardcopy the implementation summary.
- Get memos signed by management granting permission for the more sensitive security-related activities.
- Do it.

6 Reload

6.1 Setup automated systems

Once the plan has been implemented, and the worst bugs have been worked out of the procedures and systems, it's time to automate. Everything that you do, from updating the ISSP, to monitoring the firewalls and IDSs, should be as automated as possible. Specifically:

- Automate all repetitive tasks in your daily administration – it will save you time and prevent you from making mistakes
- Have alerts pushed to you, rather than having to sit down at a workstation and pull them to you. If possible, have them emailed to you and have the high-priority ones sent to your pager.
- Automate the collection of logs. Create scripts to sort and filter them and email them to you daily.
- Automatically and regularly generate reports and statistics from the various log files. If possible, output these reports as html and automatically post them on a website. This not only makes it easier for you, but it makes it easier to advertise your good work.
- Automate the backups of critical security device configurations – like firewalls – so that you won't forget.

Automation is the best way to ensure that:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Activities are done in a consistent fashion
- Regularly scheduled activities are actually done regularly
- You make fewer errors and forget fewer things you have to do
- When you scale up your capabilities, such as adding a new firewall, you'll know exactly how to set it up

6.2 Watch the Horizon

Find websites, mailing lists and other resources that you're comfortable with that will keep you in touch with the latest security news, trends, threats, vulnerabilities, exploits, tools, laws, etc. Find and subscribe to the relevant magazines to keep up with the news. Become a member of the Information Security community. Watch these all carefully and act proactively. Strive to be aware of these before they affect you.

6.2.1 Stay in Touch

Stay in touch with your company, including:

- Higher-level IT and Information Security groups, if any
- Higher-level policies, if any
- The Stakeholders: Management, Users, the IT Staff, Power Users
- New projects, contracts and other developments that could require new IT resources

6.2.2 Review what you're defending

Constantly review what you're defending. With regards to the Crown Jewels:

- Are any of yesterday's Crown Jewels no longer Crown Jewels?
- Are there any new Crown Jewels?
- Have any of the priorities changed?
- Does your organization have new producers (users, departments) of potential Crown Jewels?
- Have the System Admins removed, changed or added any applications, servers, hosts or services that may have eliminated or introduced new threats or vulnerabilities?
- Have the Network Admins introduced any new WAN Links or other connections that are potential back doors into the network?
- Has management introduced or changed any policies that change the status or applicability of the ISSP?

6.2.3 Review your Plan of Attack

Constantly review and evaluate your selected RMMs, technical and non-technical.

- Do they each actually accomplish the job you intended?
- Are changes merited to increase effectiveness?
- Have any of the vulnerabilities/threats/risks changed so much that the RMMs you targeted at them are no longer effective or applicable?
- Has technology changed enough that new and better RMMs are available?

6.2.4 Review your Self-protection

Constantly review and evaluate your personal risk and liability.

- Ensure that the signed memos that grant you permission to perform activities like, sniffing network traffic, troubleshooting email problems and cracking passwords are up to date and relevant.
- If the scope of your job changes enough, update your job description and get it signed by your manager.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- If your get a new manager, go over your job description with him/her and get it signed.
- If there are major changes in your company's upper management, re-baseline your job, the ISSP and your RMMs with that new management
- If the stakeholders change, ensure you know and understand their needs
- Communicate, communicate, communicate with everyone, all the time
- Embark on a regular routine of training to stay up to date on all matters, especially the technical. If you become certified, maintain your certification
- Stay paranoid. It's part of your job

6.3 Recalibrate your Aim and Fire again as needed

Most needed changes in your plan of attack can be incorporated into a constant stream of low-level tuning activities, simply because large or sudden changes in your security profile are rare. However, you may find that some events may force you to plan more drastic and sudden changes - events such as:

- A major compromise on your network
- The introduction of a new technology on your network
- Sweeping change in your IT infrastructure
- A new threat or vulnerability appearing on the Internet

When you get to this point, you will have to repeat this entire process, from Sections 3 to 5, in miniature. Don't fear this – a chance to rethink and redesign things is always a good thing.

7 Parting Shot

Remember the Cardinal Rules:
Cardinal Rule: When in doubt, consult your company's legal counsel.
Cardinal Rule: The greatest threat is always from the Inside
Cardinal Rule: Good security is always a custom fit.
Cardinal Rule: If the ISSP is complete and well written, everything else you need to do will flow naturally from it.
Cardinal Rule: Defense in Depth. Don't depend on network, host or application-level security alone.
Cardinal Rule: Prevent -> Detect -> Respond.

You are entering a new world, with priorities and perspectives that may take some getting used to. Although you must take care, don't let the risks make you fearful. When you act, base your actions on a sound understanding of the situation. When you act based on fear, you can

- Make preventable mistakes
- Be manipulated

You will truly learn this process only by doing it, living it. Dive in.

[1] **Merriam Webster's Collegiate Dictionary**". Online. 22 April 2001. http://www.m-w.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[2] Staggs, Jimmy. "**Computer Security and the Law**". Online. 1 December 2000. http://www.sans.org/infosecFAQ/legal/law.htm
[3] Icove, David; Seger, Karl; VonStorch, William. **Computer Crime: A Crimefighter's Handbook**. Sebastopol, CA: 1995. Chapter 4, p71-85
[4] Australian Defense Signals Directorate "**Australian Communications-Electronic Security Instruction 33 (ACSI 33**)" Online. 13 May 2001. http://www.dsd.gov.au/infosec/
[5] Michele Crabb-Guel. **"Building An Effective Security Infrastructure: Model Security Policies".** Online. 15 May 2001. http://www.sans.org/newlook/resources/policies/policies.htm
[6] The SANS Institute. "Track 1: Security Essentials 1: Basic Policy" The SANS Institute Virtual Press: 2000. Page 5-3 to 5-24.

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS