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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Risk Measurements in an Uncertain World

Name: Thomas William Oliver
Date: February 19, 2002

Version 2.0 (Draft)

© SANS Institute 2000 - 2005 Author retains full rights.

Course/Certification: GIAC Security Essentials Certification (GSEC)
Assignment Version: Version 1.3 (Amended December 12, 2001)
Submission: Original
Group: SANS Boot Camp – San Diego, Ca (2001)

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

Information Technology (IT) Security is one of the fastest growing fields within the IT industry, yet sound measurements of its' value and effects are drastically under-developed. Determining the need, how much to invest, where to place the shrinking budget for the most effective return on investment and many other issues will be raised within this paper. Through the understanding of some basic components that exist in the security landscape, a study of existing risk measurement models, and enhancements to those models, this paper will explore the gray area between the bits and the business in an effort to identify and hopefully, resolve some of the vagueness in an effective IT Security solution.

Introduction

Computers were originally developed to make life's tedious tasks easier and more expeditious. However, once the computers gained more power and networks became ubiquitous, then the information and power of the computers quickly outpaced their initial design and they started to be used for more than the resolution of everyday conundrums. Computers became an integral part of the businesses that used them and even a more integral part of the economy. As such, certain elements, driven by various desires, started to infiltrate systems and pilfer either computing resources or information, or both. Thus, the need for and growth in the field of Information Technology Security (ITS).

The dispute of the need for an IT Security person, group, or department is generally not a controversial issue within today's ***e***-conomy. However, the management and financial personnel continue to dispute the breadth and responsibility of this security element within the IT organization. Effective Return on Security Investment (ROSI) is now being coined to bring fiscal reality to a very diverse and nebulous area of IT. In an effort to comprehend the issues, several key aspects have been presented below in terms of questions. This in no way is a comprehensive list, but could be used as the genesis of a survey for your own corporation. Additionally, throughout this paper the term "corporation" will be used to simplify an organization, government agency, company, etc.

Key Aspects

- What is the size of the corporation in terms of a) personnel, b) computer users, and c) network nodes?
- What is the revenue generated in terms of Internet usage?
- What is the industry of the corporation?
- What is the overall IT Budget of the corporation?
- Is an Intranet or Extranet required?
- What is the qualitative and quantitative costs for an outage for a – 1) hour, 2) day, 3) week, or 4) indefinite to a –1) file, 2) system, or 3) network (site)?

© SANS Institute 2000 - 2005 Author retains full rights.

It is beneficial for the reader to refer to the key aspects throughout this paper to better understand the gravity of the issue(s), as well as to conceptualize solutions for their environment.

Components of IT Security

Inevitably, when you make a list of something, anything, you will leave at least one item out that someone feels is the most important element that should be accounted for above all else. Likewise, with a list of components with respect to IT Security, I am sure that there are other elements that are not listed and should carry just as much weight, as those that made the list. For simplicity, I have limited my list to 6 elements –1) Policy and Guidance, 2) Training and Awareness, 3) Vulnerabilities, 4) Threats, 5) Staff/Personnel, and 6) Defensive Measures. Once these key elements are defined, then they will be used to create a formula for the assessment of risk.

Policy and Guidance

Corporate computer security policies and guidance are needed. However, they must be understandable, comprehensive and known by all individuals across the corporation. For example, a corporate policy that states that employees shall do what is in the best interest of the company at all times with regards to computers and information technology is not sufficient in today's era of computer usage. A good place to discuss and refer to issues with respect to IT Security policies is the SANS Policy Project. Your corporate security policy should be able to cover issues that arise in everyday operations, as well as give guidance for addressing those issues and anomalies. Until the IT Security Community develops a way to measure an IT Security Policy it might be best to develop a measurement within you company that can be referenced and adapted when necessary. Here are some key elements to look at when assessing your IT security policy:

1) Does the policy or does your IT organization have a configuration management process defined that will attest to systems on your network?
2) Does the policy define the authorization of personnel who have access to computer resources within your environment?
3) Does the policy define password makeup, revocation, periods between changes, etc?
4) Does the policy define a minimal security perimeter?
5) Does the policy define the process for reporting security incidents, as well as security handling?
6) Does the policy define remote access?
7) Does the policy define anti-virus processes?
8) Does the policy define levels of systems (i.e. Critical, Support, Administrative, etc.)?
9) Does the policy define a chain of responsibility for systems?
10) Does the policy define information classifications?

© SANS Institute 2000 - 2005 Author retains full rights.

11) Does the policy define a disaster recovery site/methodology?

These are just some elements that should be within your overall IT security policy, but there are many more. Additionally, your policy should also have an "audit" clause that will allow either an internal and/or external element to selectively audit the execution of the corporate security policy. Since technology is a fluid business tool, an audit should be done annually at a minimum and should be graded on a point system to ensure a quantitative result and demonstrated improvements over a given period of time.

Once a policy is defined, then you will need to determine the policies affect on risk. Obviously, a lax policy will increase risk, likewise a more robust policy will decrease risk. Also, you must ensure that your security policy is an enabler for both computer security and your business practices. A security policy that prohibits business activity places a choke-hold on your core business value(s) and objectives.

Thus far, we have discussed the policy side of this section and have not addressed the guidance element. Guidance is extremely critical in policy definition, as it outlines a course of action for "*what if*" scenarios. What if my machine gets compromised? – Look to the policy for guidance! What if I get a virus? – Look to the policy for guidance!! There is no possible way to define every scenario, but in lieu of an exhaustive definition, default guidance should take precedence. For that matter, one should not expect every member of a corporation to know how to handle every "what if" case that arises, so it is advisable to create a terse guidance criteria. Perhaps one that simply directs the employee to call the help desk. Then internal procedures for the helpdesk can direct the issue to the IT security team, then the IT security team can have detailed procedures for many of the issues that they discover within their domain.

Training and Awareness

The computer security training for the company's population can be divided into two essential elements – 1) Basic Computer Security and 2) Threats/Awareness. These training elements are not for the IT Security staff, but more for the average use, as well as other personnel in the IT organization. The training for the IT Security staff will be in greater detail, as well as provide counter measures, proper handling of events, etc. These training elements have another factor that contributes to their value and that is time or duration between training. Let's assume that basic computer security training is done annually and that the threats/awareness training are done quarterly. This will allow for at least a quarterly assessment of the risks that affect your organizations IT environment. Likewise, since your security policy is a living and growing document, then that training should be done more often than at the hire date. Additionally, training and awareness is also a product of the population (i.e. are 100% trained, or are only 10%?). So training can be summed up as a combination of the type, time/duration, and percentage of population.

Vulnerabilities

© SANS Institute 2000 - 2005 Author retains full rights.

By definition, being vulnerable is to be open to attack or damage. From an IT perspective, being vulnerable means that you have holes(from an operational perspective) or bugs from a software point of view. Either definition means that merely the existence will increase your risks. We can further break vulnerabilities down through the use of Confidentiality, Integrity, and Availability within our IT environment. Then determine if the vulnerability can be used to exploit one or several of these concepts. For example, with respect to domain name servers (DNS), DNS poisoning can affect the integrity of the service. A buffer overflow in DNS can affect the availability and potentially the confidentiality of the service and/or information, respectively.

The main tracking mechanism for vulnerabilities can be found in either the Computer Emergency Response Team (CERT) or the Common Vulnerabilities and Exposures (CVE) database. The CERT works with various elements in industry, academia, and government throughout the world in an effort to notify and track vulnerabilities for the computer industry. The CVE is a database of vulnerabilities and exposures that are directed to standardize the terminology that the industry uses in an effort to better communicate about events and resolve issues. The CVE is a community effort, but is mainly sponsored by the U.S. government.

Threats

Threats generally have a direct impact on risk. If threats rise, then risk should rise, so threats are directly related to risks. As such, threats can be broken down into two major categories – Internal Threats (Ti) and External Threats (Te). In the SANS Reading Room, there is a paper by Arthur Nichols, “A perspective on Threats in the Risk Analysis Process”, that outlines threats in greater detail than I will go into in this paper. I would suggest that you read Mr. Nichols’ paper if this area interests you. External threats can be anything from a competitor, governmental entity, rogue hacker, natural disaster, etc that can pose an impact to your business environment either through denial of service, lose of information or lose of credibility. Many external threats can be quantified. For example, the weather service can provide a chance of a natural disaster in your geographical areas. From intrusion detection devices, one can see how many times a day (roughly) malicious activities hit or enter your IT perimeter.

Internal threats are a little more difficult to quantify. Internal threats could be everything from a disgruntled employee deleting files to a poor operating procedure that missed a backup. A brief summary of these types of threats can be defined as disgruntled employees, business partners, temporary employees, contractor employees, poor procedures or essentially anyone or thing (i.e. computer system) that has access to your internal computer infrastructure. Perhaps a more quantifiable solution for internal threats could be to ensure that –

1) Proper redundancy is created on critical systems/information.
2) Backup and recovery procedures are routinely tested.
3) Projects are managed with redundancy in mind to help ensure proper

© SANS Institute 2000 - 2005 Author retains full rights.

completion within resource limits.

Through the completion of these items, a quantified internal threat can be obtained. This coupled with the external threats can help quantify the total threat exposure of the corporation.

Staff/Personnel

An important and often forgotten element of risk has to do with the IT staff that the business has on hand to support eventual mishaps, breaches, and unidentified computer anomalies (UCA). These personnel are essential to the well being of your IT environment. Below are some key pieces of information that you should consider when determining if you have the right number and type of people to support the IT Security mission of your organization.

1) Number of Staff – The number of IT personnel that you have on staff has a great impact on your ability to respond and counter any and all events that occur.
2) Average Years of experience – If you have a staff of 10 people that have a cumulative 10 years of experience in running a large operational environmental, then you probably are not as prepared as you are if you have a staff of 10 people with a cumulative 100 years of experience running a large operational environment.
3) Staff Credentials – This can be determined in many ways – education, certifications, etc. One way is to award specific points for education – degree in a related filed equals 5 points, degree in unrelated field equals 3 points, advanced degree in related field equals 8 points, advanced degree in an unrelated field equals 6 points. For certifications – a type of administration certification equals 2 points; a type of "engineering" certification equals 4 points. A specialty certification equals 3 points. It would be nice if our industry had such a point system, however any consistent system in your area will do to measure the value of your staff's credentials.
4) Size of the environment – Determining the size of the environment can be done in many ways, but generally takes on either the number of computer nodes or the size of the personnel population. In other words the number of people that your IT staff has to support and/or the number of computers is directly related to their ability to perform their job. For example, 5 people supporting 500 people/computers will not be able to check logs effectively or watch the system stats effectively.

It is obvious that a small staff with very little experience and few credentials in support of a large number of people with increase the risk that something will occur or could occur and spread. Likewise, a large, experienced staff with several degrees and certifications that supports a small to medium size organization will have a greater chance of catching something before it happens or as early as possible after it occurs.

© SANS Institute 2000 - 2005 Author retains full rights.

Defensive Measures

The range of defensive measures can be as varied as the use of IT itself. In order to bring a confined solution with respect to defensive measures, I have listed five – 1) Firewalls, 2) Intrusion Detection, 3) Virus Protection, 4) Incident Response, and 5) Security Plans.

Firewalls: The firewall has been around in some form or fashion since before the hacker. Initially, it was simply isolation, then access control lists in a router and today there are stateful and proxy based firewalls. Regardless of the means and relative cost, the firewall is used to contain (either out or in) what is undesirable and to allow what is needed for business communications.

Intrusion Detection: Intrusion detection tools are becoming more prevalent in today's IT infrastructure, because they can monitor and alert on traffic anomalies or intruder signatures. Intrusion detection systems are mainly used in a reactive scenario within the industry by notifying only after an incident has occurred. However, some are becoming more proactive and can block an attack once it is identified.

Virus Protection: Viruses are possibly the largest threat to information integrity and resource availability within today's IT environment. Although a distributed denial of service attack will make major headlines once a year, the viruses are a continuous problem and are becoming more robust in their attacks and damage. With an increase in application integration, the viruses of tomorrow will only be more powerful and damaging. The main dilemma that faces the IT specialist is not whether to have virus protection or not, but where to place the protection (desktop or central server).

Incident Response: The reality of implementing all of the safeguards that have been discussed thus far is that the intruder/hacker will get into your environment if they are determined and savvy. This inevitable reality leads to an effective incident response team to contain the damage once the intrusion occurs.

Security Plans: One common mistake that a corporation makes is that they will purchase a firewall and perhaps some intrusion detection, but they will forget one easily cost effective deterrent – the Security Plan. A common should take their IT Security Policy and develop a security plan that covers some, if not all, of the major portions of the security policy. Then the corporation should divide up their IT systems by some common criteria, either functionally (e.g. administrative, infrastructure, business applications, etc) or organizationally (e.g. marketing, finance, human resources, etc.). Once the systems have been logically divided, then each of the systems should have a security plan to addresses issues like password, incident response, disaster recovery, contingency plan, account administration, configuration management, etc. By performing this planned analysis on each system within a corporation, then the IT Security staff will be able to identify vulnerabilities within their environment, as well as allow the CIO to address the risks within the systems.

© SANS Institute 2000 - 2005 Author retains full rights.

Risk Measurements Models

The general formula for measuring risks is defined as threats plus vulnerabilities (Risks = Threats + Vulnerabilities). Within some presentations or papers, threats may be multiplied by vulnerabilities, but regardless of the operation, the outcome is the same – risk is a measure of combining threats and vulnerabilities. While this simplistic formula identifies the two major components in defining risks, it falls short in determining whether enough money is being spent to protect a businesses IT infrastructure. Or more importantly, where should additional resources be placed to get the greatest decrease in risk. Certain papers from the SANS Reading Room, such as "Cost-effective Information Security (Information Security from a business perspective)", have added business value to this equation and determined that risk should be defined as -

Risk = Business Value X Vulnerabilities X Threats

By bring business value into the equation this paper expands upon the first equation through a key element that many managers and executive staff would like to see when defining risk. How will it (risk) affect my business? But how do you measure the business value of your domain name server? This element perhaps has more to do with actual return on security investment than defining risk. However, it is extremely difficult to determine the exact measure of this impact, which is the basis of this paper. Furthermore, the first formula added the elements of threats and vulnerabilities, while the second multiplied these two elements with a third element – business value. Both formulas define the same element – risk, so which is correct?

By building upon these formulas, we can further determine that the corporations' security policy/guidance, staff, defensive measures, and training/awareness have some effect on the risks within an environment in addition to threats and vulnerabilities. So, let's start with risk as a function ($\mathbf{R_f}$) and the six elements as variables within that function. Thus, the general definition will look like this –

$$\mathbf{R_f = fn\ (T, V, S, T_a, D_m, P)}$$

Where,

T = Threats
V = Vulnerbailities
S = Staff
$\mathbf{T_a}$ = Training and Awareness
$\mathbf{D_m}$ = Defensive Measures
P = Policy and Guidance

Now, before we precede on a mathematical tirade, let's re-exam why we should study risk. First, we should determine the proper environment for measuring risk. In other words, is it wise to measure risk on a micro or macro-environmental stage. For the

© SANS Institute 2000 - 2005 Author retains full rights.

efforts within this paper, we will determine that we will estimate risk based on the macro-environmental IT environment for the corporation. The objectives in determining risks should be as follows:

1) Determine the desired funding levels that are required to meet the company goals. In a sense, using risk as a return on investment for the company or an element in determining return on investment for a project.
2) Determine the next step for your IT security program. In other words, if you have a choice of adding a firewall or a web-caching server to your environment, and the cost is equal, which should you invest in for the most benefit? Which implementation would have a greater reduction toward risk?
3) Determine whether your risks are rising or falling given changes in your environment, the external environment and time.

Given these objectives for risk, let's determine some relationship between the six elements and risk. For example, if a new distributed Denial of Service (DDoS) attack is released, then the threats increase and so does your risk. Therefore, threats and risk are directly related - $\uparrow T \Rightarrow \uparrow R_f$. If you add a new firewall to your environment, then your defensive measures would increase and your risk would decrease. Therefore, defensive measures are inversely related to risk - $\uparrow D_m \Rightarrow \downarrow R_f$. Below is a relationship of the six elements toward the risk function:

$$\uparrow T \Rightarrow \uparrow R_f$$
$$\uparrow V \Rightarrow \uparrow R_f$$
$$\uparrow S \Rightarrow \downarrow R_f$$
$$\uparrow T_a \Rightarrow \downarrow R_f$$
$$\uparrow D_m \Rightarrow \downarrow R_f$$
$$\uparrow P \Rightarrow \downarrow R_f$$

If we treat all of the elements equally, then we can determine a formula similar to the following:

$$R_f = (T \times V)/(S \times T_a \times D_m \times P)$$

However, this equation is missing one major constant - size. The size of the environment affects this equation greatly. The size of the corporation has a greater impact on the exposure with respect to threats and vulnerabilities. Likewise, the larger the corporation the greater the need for more staff, awareness and specific defensive measures. A table like the one below can help with the use of size as a measurement in the risk equation.

Lower End	Upper End	Value (S_v)
1	100	2
101	1000	3

© SANS Institute 2000 - 2005 Author retains full rights.

1001	10000	4
10001	50000	5
50001	No limit	6

The size table above is completely arbitrary, but is useful to discuss how size can affect the six different elements and ultimately the risk that is within the environment. The following list describes the six elements with respect to size:

1. Policy and Guidance – A good set of IT Security policies and guidelines are necessary, whether your organization is made up of 100 network nodes or 1000. Naturally, a larger organization will have a wider variety of policies and perhaps additional enforcement issues, but essentially, the basic policies shall remain the same. It is for this reason that I feel that the size of the organization does not hold a major impact on the policy and guidance element.
2. Training and Awareness – The value of training and awareness will be measured as a percentage of the population. So, the size of the organization is somewhat irrelevant.
3. Vulnerabilities – The size of the organization affects the vulnerabilities because the larger the organization the larger the exposure.
4. Threats – Threats are also affected by the size of the organization due to an increase in exposure.
5. Staff – The staff should be measured as a relation to size ($\mathbf{S/S_v}$).
6. Defensive Measures – When you think of the components that make-up or can make-up the defensive measures you can derive arguments that indicate that the size of the organization has an impact. Likewise, you can also make an argument that the size has not major impact on the defensive makeup of the organization. I have chosen this later approach for the final formula.

Now, the final formula is derived as –

$$\mathbf{R_f = [(S_v)(T \text{ X } V)]/[((S/S_v) \text{ X } T_a \text{ X } D_m \text{ X } P)]}$$

From this formula, you can see that the size of the organization can increase the exposure to threats and vulnerabilities, as well as decrease the effectiveness of your IT Security staff if the staff is not adequately increased.

Summary

This paper has attempted to expand the elements of the risk equation and moved forward on relating those elements to one another, risk and the size of the organization. Obviously, further research is needed in this area, but it will take organizations like SANS and ISC^2 to sponsor such industry studies to actively pursue a true quantitative measure for risk and thus provide senior management with a return on security investment that they can evaluate on par with other business ventures.

© SANS Institute 2000 - 2005 Author retains full rights.

References

The SANS Security Policy web site was used in the preparation of this paper, but I was unable to relocate the site for reference - SANS Policy web site.

CVE - http://cve.mitre.org/ - General use.

CERT - http://www.cert.org/ - General use.

Scott Berinato. "*Finally, a Real Return on Security Spending*", February 15, 2002
http://www.cio.com/archive/021502/security.html

Scott Berinato. "*Coming up ROSI*", October 26, 2001
http://www.cio.com/security/edit/a102601_rosi.html

Arthur Nichols. "*A Perspective on Threats in the Risk Analysis Process*"
http://rr.sans.org/audit/risk_analysis.php

Eric Piepers. "*Cost-effective Information Security*"
http://rr.sans.org/audit/cost-effective.php

Micki Krause and Harold F. Tipton, "*Handbook on Information Security Management*"
http://www.detectiondesintrus.com/Documents/HISM/ewtoc.html

Gangemi, G.T. and Russell, Deborah, *Computer Security Basics*, O'Reilly & Associates, Inc., 1991

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.