Host Assessment and Risk Rating

Radhika Vedaraman

Version 1.4b, Option 1

5/31/04

ABSTRACT

"The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeros, little bits of data…"

- Dialogue from the movie Sneakers, MCA/Universal Pictures, 1992

Corporate websites get defaced; business activities of organizations get crippled; identity stolen; confidential information made public - all because of not securing information and resources, and not taking precautions necessary to protect against attacks. These attacks, apart from causing millions of dollars loss in revenue, also result in customer inconvenience, loss of customer confidence, loss of intellectual property and market advantage, liability for compromised customer data, and the time and money spent recovering from the attack.

According to surveys conducted recently,

- Hacker were able to steal up to 8M credit cards[1]
- Quantity of cyber security incidents reported has roughly doubled every year since 2000 – jumping from nearly 22,000 incidents for all of 2000 to 76,000 in the first half of 2003 alone [2]
- Viruses such as Blaster, Welchia, and Sobig.F have resulted in as much as $2 billion in damages. [3]
- Theft of proprietary information has caused a loss of $70,195,900, with the average reported loss being approximately $2.7 million. Denial of service has a caused a loss of $65,643,300.[4]

In the past few years, more businesses have gone online. Because of the growing list of vulnerabilities, and increased regulatory pressure, security has become a pressing business issue at the highest levels of most organizations. For example, any enterprise that deals with Visa Credit Card information must be in compliance with the VISA CISP, and any company that deals with health information must be in compliance with the HIPAA. According to a survey conducted by Ernst & Young [5], 38% of the survey responders cited these regulatory rules as having a major impact on their organization's security policy and structure.

A company's security infrastructure must be tightened so as to prevent unauthorized access, theft, and inappropriate usage. Inherent to each environment is a risk – a chance that the above-mentioned can happen. So there is a need for some mitigating or preventing controls. These controls can potentially reduce the probability of occurrence of such an attack. Industry's leading practices, which are a consensus of approaches, architectures, and solutions that protect network, systems, and data, must be employed while designing such controls.

This paper strives to develop a model that could be used to design a Minimum Security Baseline (MSB) for an enterprise. It also suggests a method to assess the existing infrastructure against the established MSB in order to find the gaps. Then it goes on to illustrate a procedure to resolve these gaps.

PURPOSE

[1] http://money.cnn.com/2003/02/18/technology/creditcards/
[2] Carnegie Mellon University's CERT Coordination Center
[3] www.computereconomics.com/article.cfm?id=867.
[4] CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 2003
[5] Global Information Security Survey 2003 by Ernst & Young

Host assessment and Risk rating helps in identifying threats, vulnerabilities, and risks to the infrastructure, and then in quantifying the impact of the potential vulnerabilities. The return of investment must be calculated to evaluate if the cost of mitigating a risk outweighs the cost incurred if the vulnerability is exploited so that management can decide which risks to prevent, limit, or accept.

An enterprise typically has a large number of servers and network devices. It becomes difficult to find the current state of each network component so as to fix the gaps. Even if we consider only a sample set of these components, it is easier if there is a tool to help summarize the results and present them along side so it is easier to compare them. An excel spreadsheet has been developed that helps to automate this process. The process is described in the following section, while the working of the tool is described later.

SCOPE

At present, this paper deals with assessing various platforms (E.g.: Windows, Solaris, Linux, and Mainframe). This could be very easily modified to accommodate network devices and others standards as required. This paper will take Windows 2000 as an example, and present a sample for the various steps. Few snapshots of the excel spreadsheet tool will be presented in this paper, while the actual tool is located at https://filebox.vt.edu/users/rvedaram/GSEC/

PROCEDURE

The sequence of steps involved in this process is as follows:

1. Identify the platforms
2. Develop Minimum Security Baseline (MSB) for those platforms
3. Identify a set of representative systems for each of those platforms.
4. Assess the representative systems against the MSB for each platform.
5. Identify Gaps
6. Develop the Risk Rating for each of the system.
7. Develop a Plan of Action based on the Risk Ratings.
8. Obtain approval for the mitigating measure from the necessary governance body.
9. Implement Plan of Action.

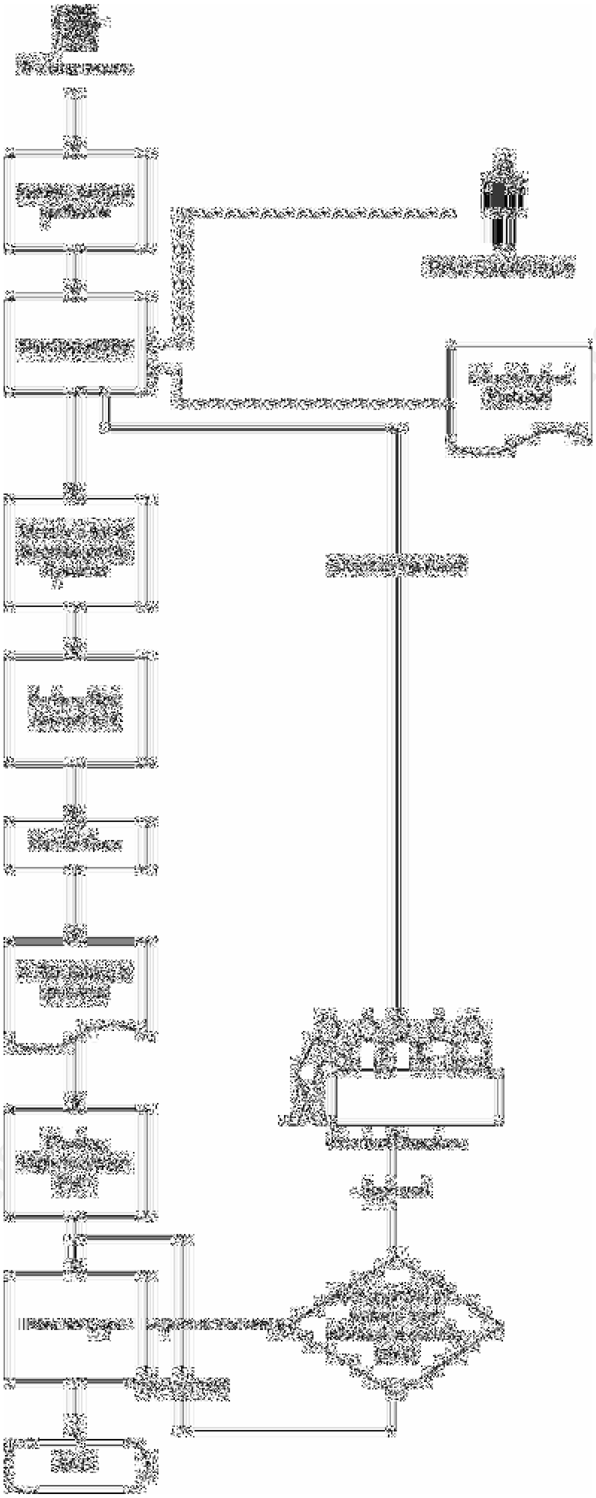


Figure 1: Flowchart of Host Assessment

DEVELOPMENT OF THE MSB

An enterprise must have a secure IT infrastructure, which must be incompliance with various regulatory rules and policies. Many of these Regulatory

Rules require that an enterprise wide Information Security Policy is developed and maintained. A set of standard configurations for various platforms and devices are also required. In order to develop these, the various working groups in the enterprise must reach consensus. Baselines are derived from associated security policies and procedures, and risk avoidance decisions made by the organization based upon its documented rationale for reasonable security protections and measures. These documents are then published and become the standards that need to be implemented throughout the organization.

Developing a Minimum Security Baseline for Windows 2000 ensures that a uniform set of standards is applied on all Windows 2000 Systems (Servers and Workstations) across the enterprise. All Windows 2000 systems must be incompliance with this standard. If there is a valid business reason that prevents the implementation of a control in the standard, then an exception or a waiver as required must be submitted. This document must be reviewed periodically and maintained as new changes occur in the environment.

COMPONENTS OF A MSB

Control Title: This is a short statement that identifies the crux of the control statement.

Control Statement: This statement describes what the control hopes to achieve in technical terms. It is intended for a technical person.

Business Risk: This section describes the risk of not implementing a control, and how it would affect the business. This is intended for the management.

Implementation Procedure: This is a detailed account of how to implement the control for the given environment.

Assessment Procedure: This is an account of how to verify if this control is satisfied. It could be done using an automated tool, or by manually verifying some settings. This procedure could be used for assessing the Host.

DEVELOPMENT OF CONTROLS

A MSB is composed of a set of controls that describe the security features necessary. Controls must be developed using Industry Best Practices, and prior experience. For example, in order to develop a MSB for Windows 2000, refer to the recommendation by Microsoft, Security configuration guide from NSA etc.

Types of controls

An MSB should typically cover the following sections.

General: These are controls that cannot be classified into the following sections.

Eg. Keep security patches up-to-date.

Network Related: Controls that describe how a system/device must be connected to a network, and configured. These are specific to the network architecture and how the components communicate within that framework.

Eg. Require SMB Signing

Account Management: Controls that deal with how user accounts must be created, modified, deleted and other controls needed to safeguard the userID, and User sessions
Eg. Do not display last login name, set account lockout policy as per the corporate policy.

Authentication: Controls that deal with passwords and how authentication takes place.
Eg. User Password must be set according to the corporate policy, use at least NTLMV2 for authentication.

Authorization: These are control that deals with permissions: who can access which file and how, what kinds rights they possess etc.
Eg. Limit the users who can debug programs

Confidentiality: This section deals with data classification, and how sensitive information is protected.
Eg. Encrypt sensitive user data using EFS, or other encryption mechanism

Logging & Monitoring: This section deals with what to log, how long to retain them, and how sensitive activities and files are monitored.
Eg. Audit successful access to files and folders

Policies and Procedures: Policies are needed, as many regulatory rules require them. Also without documented policies it will be difficult to prosecute intruders and other malicious users. This section describes the various policies, guidelines and procedures required.
Eg. Implement and maintain information Security Policy

Things to consider while designing controls

1. All the controls must be discrete. They must evaluate to a boolean value. A control statement such as "*All critical events must be logged and they must be monitored periodically*" would be unacceptable as it cannot be evaluated to True or a False (Compliance/Non Compliance), as events could be logged, but not monitored. Alternatively, consider splitting this into two separate discrete controls.

2. All the controls must be measurable. A statemen such as "*A good, complex password must be used*" is inappropriate. Goodness is a relative concept and this control by itself could not be evaluated or measured. It should be modified to something like "*The password must be set according to the corporate security policy*".

   This achieves two goals

   1. If there is a change in the corporate policy, it is enough if it is changed at one place, as other standards just refer to this policy

2. There is a consistent value across all platforms in the enterprise, and it now becomes measurable.

However, it is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practical for all organizations. There must be an applicability column in the MSB, which specifies the environment that a control can be applied to.
In Windows 2000, the different environments could be classified as

1) DC- Domain Controller
2) Application Server
3) File and Print Server
4) Workstation
5) Exchange Server

A control such as, "*Use Active Directory Integrated Zone for DNS*" is applicable only to the Domain Controller, while a control such as "*Use EFS*" is applicable to a workstation. A control such as "*Install all latest service packs and hot fixes*" is applicable to the entire environment.

EXCEPTION & WAIVERS

An Exception is an indefinite variance from the standard that has a valid business justification. This is applicable to only Low to Medium risk controls. There could be a control that states "*Disable default shares*". But if the enterprise is using Microsoft's SMS, then these shares may be needed. In such cases an exception is filed for each system that requires it.

A Waiver should only be used in exceptional situations and must be limited to a specific period and to a specific system. A waiver could be obtained for a High-risk control. A waiver request must specify the duration of the waiver, the mitigation plan, and an alternate solution, if any, that could be implemented immediately. A Windows 2000 MSB would typically have a control that states "*Use Kerberos for authentication*". But if there are Windows NT systems in the domain, Kerberos authentication is not possible. Either the system must be upgraded to windows 2000, or the NT service pack must be updated and must use NTLMv2. A waiver must be obtained for the duration of the test and implementation of this project.

RISK RATING

A threat profile must be developed initially. The development of a threat profile helps in deciding what types of threats exist in a particular environment, what the probability that a threat manifests itself into an actual problem, and what the ramifications, costs and consequences are of those threats being realized. Some factors to consider while developing the threat profile:

- Do the threats come from external or internal sources?
- What would the impact be if the vulnerable applications were not present?
- What would the impact be if the systems were compromised?
- What would the impact be if the controls were not implemented?

Based on the threat profile, the criticality of a control is determined. These are classified as High, Medium, or Low risks.

LOW. Residual vulnerabilities have been identified, but would require a high level of resource and skill for any attack using lack of this control to succeed.
Eg: Disable Direct Draw

MEDIUM. Attackers with moderate levels of resource and skill could exploit the identified vulnerabilities in this control
Eg: Use SMB Signing

HIGH. A limited opportunity and little specialized knowledge would be needed to succeed in using the lack of this control to launch an attack.
Eg: Use encrypted, secure channel for communication

Risk rating is very subjective and the working group must decide on the Risk Rating when the MSB is developed. The risk of not implementing a control is not the same for different environment.
For example, "*Use of IPSec*" might be a Low risk within the Intranet, while it might be a Medium risk on the DMZ. "*Extensive Logging*" could be "non applicable" in an Intranet, while it is a High Risk (Requirement) in case of system that must be incompliance with VISA CISP.

Sample control from a MSB

Control Standard	Standard Description	Business Impact / Risk	Implementation Procedure	Assessment Procedure	Applicability			Risk
					DC	APP	F/P	
Change the dll Library Search Order (For Windows 2000 Service Pack 3 or greater only)	Change the DLL library search order to search the '%SYSTEM ROOT%' folder first.	By default, Windows 2000 searches the current directory when a DLL is needed. A potential intruder could use this weakness to introduce a Trojan DLL that may be used in place of a genuine DLL once the appropriate program is launched or appropriate action is taken. Such Trojan code could lead to the compromise of an entire domain, if not secured.	The value of registry key '*SafeDllSearchMode"* controls the order in which directories are searched for DLL (Dynamic Link Library) files. The default value of '0' causes the current directory to be searched before the system and Windows directories. Changing the value to '1' causes the search to occur in the following order: 1. %SystemRoot%\System32 2. %SystemRoot% 3. The current directory 4. The folders in user's %PATH% environment variable. To set the Registry key, Click on **Start → run → type "regedt32"** and click **OK** Locate *HIVE:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manage* *Key: SafeDllSearchMode*	Check the registry to see if Click on **Start → run → type "regedt32"** and click **OK** Locate *HIVE:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet* *Key:SafeDllSearchMode is set to value:"1"*	X	X	X	H

	Data Type: REG_DWORD *(DWORD Value)* *Value Data:1*				

HOST ASSESSMENT

A set of systems must be identified as being representative of the entire platform in the corporate infrastructure. These systems must be evaluated against each of the controls listed in the MSB.
A host assessment report would consist of the following components and each of the controls in the assessment report must refer to the control in the MSB for traceability.

- Date of the Review
- Assessment done by
- Host Name
- Host Type: Domain Controller, Workstation etc
- Host Location: DMZ, Intranet etc.
- Control Title: From the MSB
- Status of control: Compliance, Non Compliance, Not Applicable
- Observation: This is the reason for the status of the control. Also specify if an alternate solution is in place to the suggested one.
- Supporting Document: Name of the work paper that substantiates the finding

Automated tools such as the Microsoft Baseline Analyzer, GFI LANguard, Dumpsec could be used for the assessment. Custom scripts could be used to verify registry setting and file permissions. Also, some controls require manually verification on the representative server.

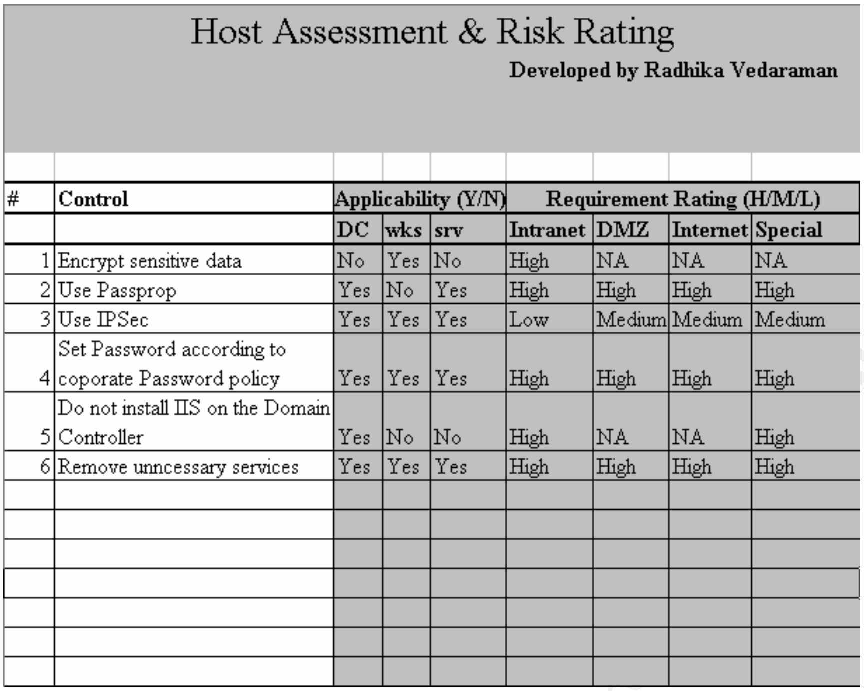
RISK ASSESSMENT TOOL

There are numerous checklists available that could be used to assess a system. But they do not help in presenting all the systems alongside so that we can analyze the trend and develop a method to correct the problem. An excel spreadsheet tool was developed to solve this problem. This tool attempts to take a snapshot of the environment, and use it to arrive at the risk present in the various hosts.

The working of the tool closely reflects the procedure described above. This tool is configured currently for 20 controls and for 10 hosts. Excel Macros are used in these calculations.

CONTROLS SECTION

The first section deals with the MSB. A set of controls is identified first. Then the risk associated with not implementing each of the control is determined, according to its environment. Also the area of applicability (eg. DMZ, Intranet, Internet; or Workstation, Server, Domain Controller) is established. The controls are entered in the second column. The users are presented with the possible options in a dropdown menu for the subsequent cells to help simplify things.



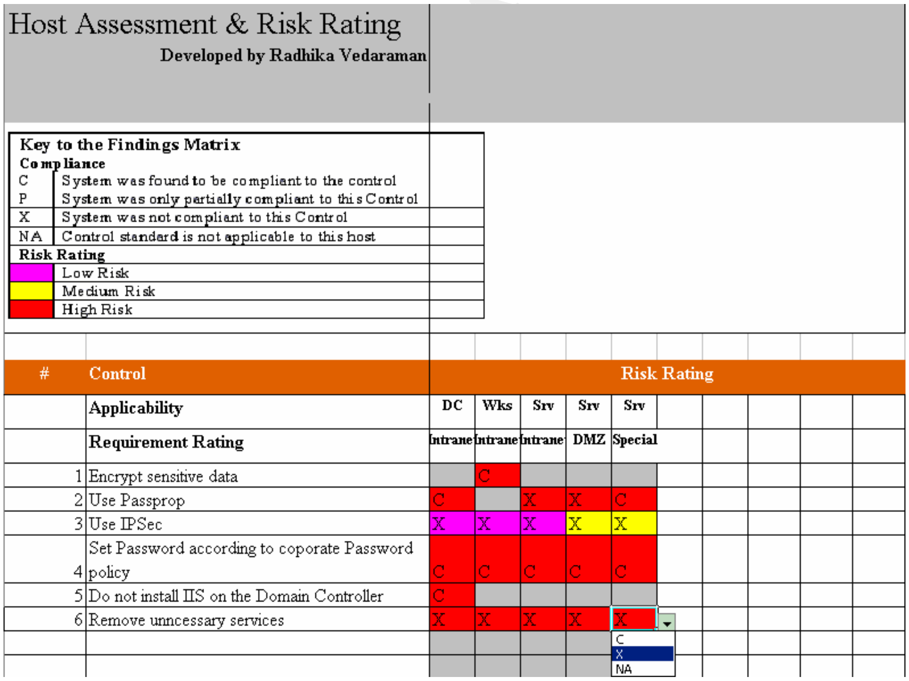
Host Assessment & Risk Rating

Developed by Radhika Vedaraman

#	Control	Applicability (Y/N)			Requirement Rating (H/M/L)			
		DC	wks	srv	Intranet	DMZ	Internet	Special
1	Encrypt sensitive data	No	Yes	No	High	NA	NA	NA
2	Use Passprop	Yes	No	Yes	High	High	High	High
3	Use IPSec	Yes	Yes	Yes	Low	Medium	Medium	Medium
4	Set Password according to coporate Password policy	Yes	Yes	Yes	High	High	High	High
5	Do not install IIS on the Domain Controller	Yes	No	No	High	NA	NA	High
6	Remove unncessary services	Yes	Yes	Yes	High	High	High	High

Figure 2: Worksheet1, List of controls and Risk Rating

HOST ASSESSMENT



Host Assessment & Risk Rating

Developed by Radhika Vedaraman

Key to the Findings Matrix	
Compliance	
C	System was found to be compliant to the control
P	System was only partially compliant to this Control
X	System was not compliant to this Control
NA	Control standard is not applicable to this host
Risk Rating	
🟪	Low Risk
🟨	Medium Risk
🟥	High Risk

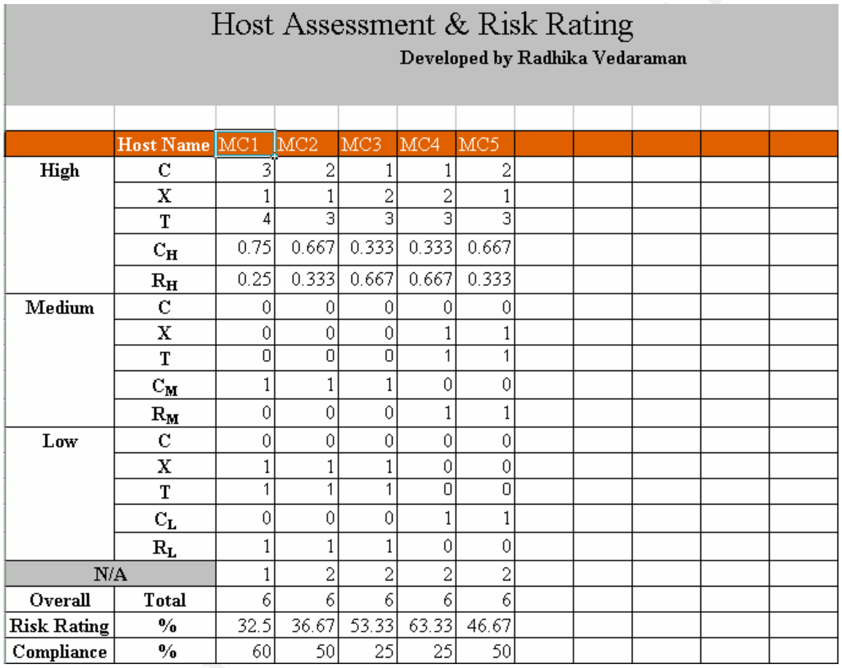
#	Control	Risk Rating				
	Applicability	DC	Wks	Srv	Srv	Srv
	Requirement Rating	Intrane	Intrane	Intrane	DMZ	Special
1	Encrypt sensitive data		🟥 C			
2	Use Passprop	🟥 C		🟥 X	🟥 X	🟥 C
3	Use IPSec	🟪 X	🟪 X	🟪 X	🟨 X	🟨 X
4	Set Password according to coporate Password policy	🟥 C	🟥 C	🟥 C	🟥 C	🟥 C
5	Do not install IIS on the Domain Controller	🟥 C				
6	Remove unncessary services	🟥 X	🟥 X	🟥 X	🟥 X	🟥 X

Figure 3: Worksheet 2, Host Assessment

The controls are automatically populated form the previous worksheet. The hosts that are assessed are entered in the second row. The applicability and the requirement rating are then selected for each control, for each hosts using dropdown menus. The cell background colors identify the risk. If a control was marked as not applicable in worksheet 1, then that control is marked in grey. If the risk, or the applicability is modified in worksheet 1, or if the environment of the host is changed in this worksheet 2, then click on "Update Risk" button to update the risk colors. This color is used in the subsequent sheets for risk rating calculations, and so needs to be accurate.

Risk Summary

In the final section, the finding from the previous worksheet is summarized and presented as numbers for easy interpretation. For each hosts, the number of cells marked as compliant in a particular risk category is calculated. Risk colors are used for these calculations and so the colors marked in worksheet 2 must be accurate.



Host Assessment & Risk Rating

Developed by Radhika Vedaraman

	Host Name	MC1	MC2	MC3	MC4	MC5					
High	C	3	2	1	1	2					
	X	1	1	2	2	1					
	T	4	3	3	3	3					
	C_H	0.75	0.667	0.333	0.333	0.667					
	R_H	0.25	0.333	0.667	0.667	0.333					
Medium	C	0	0	0	0	0					
	X	0	0	0	1	1					
	T	0	0	0	1	1					
	C_M	1	1	1	0	0					
	R_M	0	0	0	1	1					
Low	C	0	0	0	0	0					
	X	1	1	1	0	0					
	T	1	1	1	0	0					
	C_L	0	0	0	1	1					
	R_L	1	1	1	0	0					
N/A		1	2	2	2	2					
Overall	Total	6	6	6	6	6					
Risk Rating	%	32.5	36.67	53.33	63.33	46.67					
Compliance	%	60	50	25	25	50					

Figure 4: Worksheet 3, Risk Summary

C_H is the compliance ratio calculated as

Total number of control that was compliant in a Risk category/ total number of controls in that Risk category

R_H is the Risk Ratio calculated as

Total number of control that was Non Compliant in a Risk category / total number of controls in that Risk category

Overall Compliance Ratio is calculated as

Total number of control that was compliant in **all** Risk category/ total number of controls

If there is a need to distinguish the Risk Category, (ie. non compliance of a high risk control is riskier than the non compliance of a low risk control), suitable weights could be applied so that

Overall Risk Rating is

$$\frac{\Sigma (X_R * R_R)}{\Sigma T_R}, \text{ Where } R \in (\text{High, Medium, Low}),$$

X: Number of controls that are not in compliance
T: Number of controls

Excel Macros were used to automate the calculations of the Risk and the Compliance Rating. With any change in the previous worksheets, this page automatically updates to present the current ratings.

ADDRESSING RISK

Risk Assessment techniques identify and quantify potential business risks, such as the impact of a breach of computer network security. Risk Mitigation measures minimize or eliminate many of these risks. When considering which system to tackle first, the risk rating of the systems and its environment must be considered. Systems that are subjected to regulatory controls must be made compliant before the deadline imposed by the act. Even when there is flexibility of deadline, the environment must be considered first, as a vulnerable system in the DMZ is more likely to be exploited than a vulnerable system in the intranet. Within an environment, the role of the system and the type of information that it holds must be considered next. Finally the risk rating value could be used to prioritize.

There are several ways to control risk. A "*preventive*" action will prevent an incident from occurring. "*Protective"* actions reduce the impact of a potential loss, "*corrective"* actions permanently addresses a risk, and "*interim*" actions partially address a risk before longer term measures are implemented.

Another aspect of risk mitigating is Cyber-insurance. It is a specialized type of insurance policy that provides both insurance and risk management services against various types of cyber-risk[1]. The biggest players in this area include Insuretrust.com LLC in Atlanta, Hamilton, Bermuda-based Ace Ltd.'s information technology products group and Okemos, Mich.-based J. S. Wurzler Underwriting Managers Inc.'s Website Insurance & Security Program.

CONCLUSION

A current inventory of the network hardware and software should be maintained. By not maintaining a current inventory the risk is increased that non-standard or obsolete software may be introduced into the network. Additionally there is a risk that software changes will not be identified in a timely manner.

With new vulnerabilities coming out everyday, the Minimum Baseline must be constantly updated and maintained. Host assessments and vulnerability scanning must be periodically performed to evaluate and strengthen the overall security of the company. Any change in the environment would alter the risk ratings of the controls. This tool must be updated accordingly in order to produce accurate results.

[1] Definition by Ty Sagalow, chief operating officer and executive VP of New York City based AIG eBusiness Risk Solutions

The choice of risk metrics and the procedure to resolve the gaps would vary depending on the environment, and available resources. This paper explores **one** such option. This idea could be extended to other Network Devices too. After all, this tool is as useful as the user chooses it to be.

REFERENCE

1. "Information technology — Code of practice for information security management", Reference number ISO/IEC 17799:2000(E)

2. Cardholder Information Security Program
URL: http://usa.visa.com/business/merchants/cisp_index.html?ep=v_sym_cisp#b

3. PROVIDER HIPAA READINESS CHECKLIST – GETTING STARTED
URL: http://cms.hhs.gov/hipaa/hipaa2/readinesschklst.pdf

4. Department of Information Technology,
URL: http://www.mit.gov.in/stqcit/Riskassessment.asp, January 20, 2003

5. Windows 2000 Security Hardening Guide Version 1.2,
URL: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

6. Windows 2000 Security Checklist,
URL: http://labmice.techtarget.com/articles/securingwin2000.htm, December 10, 2003

7. Macros, VBA Functions
URL: http://www.contextures.com/xlfaqMac.html#WSChange

8. Davis, Glenn, A Risk Assessment Approach to NT Security
URL: www.giac.org/practical/Glenn_Davis.doc, September 2000

9. Bartock, Paul F.Jr., "Microsoft Windows 2000 Network Architecture Guide", Version 1.0 Report Number: C4-051R-00, Updated: April 19, 2001

10. Berryman, Paul, Risk Assessment: The Basics
URL: www.giac.org/practical/Paul_Berryman_GSEC.doc, February 16, 2002

11. Innovative E-Business Insurance Protection for Customers of Counterpane Internet Security, Inc. prepared by Frank Crystal & Co., Inc. and Counterpane Internet Security, Inc.
URL: http://www.counterpane.com/pr-lloydswp.html

12. RISK ANALYSIS OF GOVERNMENT COMPUTER SYSTEMS, New Zealand Security of Information Technology Publication 104
URL: http://www.gcsb.govt.nz/nzsit/104/104chap6.htm, Chapter 6