What is your Current Security Risk Level ?

James G. McIntyre

McIntyre & Associates, Inc.
Radford, VA

HP WORLD 2003
Solutions and Technology Conference & Expo

Overview

- Why are we talking about this ?
  - TMP – Time Money People
- So many machines and so little time.
- So many of them and so few of us.
- Too much work too few assets.
- Only have so much money.
- HIPPA
- Where do I start ?

So where do we start ? I need a plan !

- Shotgun Approach
  - Fix something and hope for the best
- Analytical/Business Approach
  - Defined process to assess your environment
  - Repeatable process – Security is ongoing
  - Develop baseline comparison for next year
  - Quantifiable
    - If you can not measure it, you can not manage it.
  - Offer the best return on TMP –
    - Time
    - Money
    - Personnel

Risk Analysis

Involves identification and assessment of the levels of risks calculated from the known values of assets

and

the levels of threats to, and vulnerabilities of, those assets.

Risk Analysis Overview

- Identify what you're trying to protect
- Determine what you're trying to protect it from
- Determine how likely are the threats
- Implement measures which will protect the assets in a cost-effective manner
- Review and refine the above process

Overall Risk Analysis Strategy

- Determine the Risk Team/Committee Members
- Organize and Prioritize Assets
- Organize and Prioritize Risks
- Map Assets to Risks
- Organize Controls
- Map Controls to Assets/Risk pair
- Develop Business Recovery Plan (Disaster Recovery)
  - Define the business process and its criticality to the organization.

The RA Team/Committee

- *Obtain Management commitment*
  - Select the BIA/RA team. Minimum of 3 people on the team from the technical, staff and management areas of the business process.
  - Formally delegate authority and responsibility for the task
  - Review and support the team's findings
  - Make final decision on any specific security implementations

Sample R/A Committee

- *Management **AND** Technical Personnel from the major areas of IS*
  - Upper Management
  - Middle Management
  - Sys-Admins
  - Net-Admins
  - Applications Development
  - Applications Support
  - DB-Admins

Identify Assets

Constructing an Asset Matrix

HP WORLD 2003
Solutions and Technology Conference & Expo

What are Assets?

- *Compile a list of assets.*
  - Hardware: CPU, keyboards, computers, printers, monitors, routers, cable, etc.
  - Software: source programs, OS, diagnostic programs
  - Data: logs, online info, databases
  - People: users, admins, HW maintainers
  - Doc/Supplies: manuals, paper, forms
  - Services: email
  - Business Practices: Payroll, Manufacturing Plant 1

Open Events
Maintenance
Enter an Event
My Info

Search Events
Machines:

All Machines
Browse Events
Statistics

dock.cc.vt.edu details

Application: Matlab/ARC Info/SUN License Manager/IMSL

Location: BX31

Serial Number [redacted] SunOS . Other ID:

Manuf	model	CPU Type	# of CPUs	Megs of Ram
SUN	600-2933-05	Mhz		

IP Address	Recepticle	Voltage	Contract Info
198.82.160.248	PDU2-A-39	110	Refer to Contracts Notebook in Machine Room

Maintenance

Application Contacts	Contact Order	Office Phone	Home Phone	E-mail	Cell/Pager	URL
Randy Marchany	1	540-231-9523		marchany@vt.edu		

System Contacts	Contact Order	Office Phone	Home Phone	E-mail	Cell/Pager	URL
Randy Marchany	1	540-231-9523		marchany@vt.edu		

Management Contacts	Contact Order	Office Phone	[redacted]	E-mail	Cell/Pager	URL
Mary Dunker	5	19327		dunker@vt.edu	[redacted]	
Marshall Fisher	9	15178		mfisher@vt.edu		

Search Results

There are no events in the database matching your criteria.

Generated on Wednesday, August 1 2001 at 18:49Comments/Questions/Complaints to cmcnabb@vt.edu

Associate IT Assets

- Define at the appropriate level of granularity.
  - List individually
  - Combine by function (all workstation for floor traders)
  - Application (Mail server, Oracle DB engine, Active Directory Server)
- Define who is accountable for the asset.
- The **network** (router, bridges, cabling, etc.) may be treated as a single entity and deemed critical.

Example Asset List

Asset	Description
Bigguy	DNS Name Server (primary)
PPES	Physical Plant/Environ. Servers
Network	Network routers, servers, modems, etc
Penguin	HR DataBase Server
Payme	Payroll Servers
ProdControl	Production Control Servers – (kirk, spock, enterprise)
Littleguy	DNS Name Server (secondary)
PLC	Plant Line Control Servers

Categorize the Assets

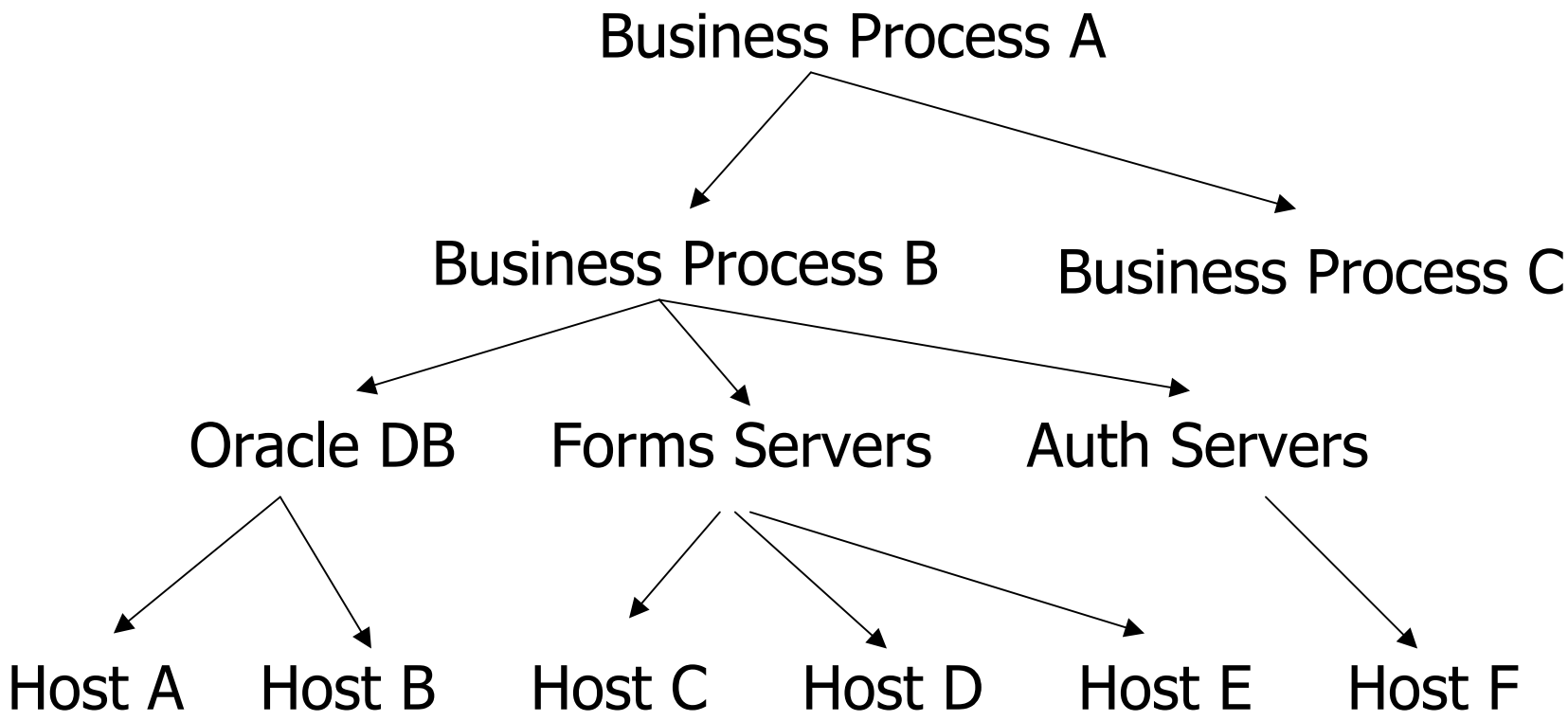
- Categorize as Critical, Essential, Normal
  - **Critical** – can not operate w/o this asset for even a short period of time.
  - **Essential** - could work around the loss of the asset for up to a week. The asset needs to be returned to service asap.
  - **Normal** - could operate w/o this asset for a finite period but entities may need to identify alternatives.

Categorize IT Assets

- Sample Criteria
  - Criticality of business function
  - Cost of failure
  - Negative Publicity
  - Legal and ethical issues
- The team must agree on the criteria.
- Consider criteria and use judgment and experience to classify the assets.
- Keep the number of critical assets low.
  - 12 is a good number.

Critical, Essential, Normal

Asset Classification – Tree Structure



Critical, Essential, Normal

Example – Categorized Asset List

C – Bigguy	DNS Name Server (primary)
E – PPES	Physical Plant/Environ. Servers
C – Network	Network routers, servers, modems, etc
E – Penguin	HR DataBase Server
C – Payme	Payroll Server
C – ProdControl	Production Control Servers – (kirk, spock, enterprise)
E – Littleguy	DNS Name Server (secondary)
C – PLC	Plant Line Control Servers

Critical, Essential, Normal

Prioritizing the Assets

- Which assets do I start with ?
  - Critical
- Each asset compared to every other asset.
- Need to rank order using a Matrix Prioritization Technique.
- Members vote on their **relative** importance.
  - Votes can be split

Matrix Prioritization Technique

- Utilize the matrix prioritization technique which compares all assets to each other.
- Asset weight values calculated by a simple formula
  - Weight = sum of vote values.
- Voting Criteria:
  - Criticality
  - Value to the Organization
  - Impact of Outage

Example Asset Matrix Chart

Asset	Bigguy	Ppes	Payroll	Email	Network	Total (WT)
Bigguy						
Ppes						
Payroll						
Email						
Network						

Is "Column Asset" more important than "Row Asset" ?

Example Asset Matrix

Asset	Bigguy	Ppes	Payroll	Email	Network	Total (WT)
Bigguy		9	9	9	5	32
Ppes	0		2	4	0	6
Payroll	0	7		5	0	12
Email	0	5	4		0	9
Network	4	9	9	9		31

Is "Column Asset" more important than "Row Asset" ?

Assets Wrap-Up

- *What have we accomplished ?*
  - Identified primary assets.
  - Associated functional assets.
  - Categorized Assets by Critical/Essential/Normal.
  - Prioritized Critical Assets with a Matrix.

Identify Risks

Constructing a Risk Matrix

HP WORLD 2003
Solutions and Technology Conference & Expo

Identify the Risks

- *A **RISK** is selected if it can cause an incident that would:*
  - Be extremely expensive to fix
  - Result in the loss of a critical service
  - Result in heavy, negative publicity internally or externally
  - Have a high probability of occurring

Risks from SEC Form 10-K

- Public non-acceptance of e-commerce
- Non-acceptance of e-advertising
- Non-acceptance of e-products
- Government Internet Intervention
- Internet technology change
- Unavailable domain names

Paper by Michael Ettredge & Vernon Richardson U. of Kansas

GAO Risk List

- Lack of formal IT planning mechanisms
- Lack of formal security policies
- Inadequate program change control
- Little or no awareness of key security issues, inadequate technical staff to address the issues
- Failure to take full advantage of all security software features

National State Auditors Association & GAO

GAO Risk List

- Inadequate user involvement in testing and sign-off for new applications
- Installation of software or upgrades w/o adequate attention to the default configurations
- Virus definitions not current
- Inadequate continuity of operation plans
- Failure to formally assign security administration responsibilities to technically competent staff

National State Auditors Association & GAO

Technical Risk List

- 12 common risks
  - System administration Training
  - Desktop Access Control
  - Operational Policies
  - Key Person Dependency
  - Bad Passwords
  - Data Disclosure
  - Internal Physical Security
  - External Physical Security
  - Cleartext
  - Spoofing/Forgery
  - Natural Disaster
  - Construction Mistakes

Risk List - FBI/SANS Top 10 Vulnerabilities Windows

- IIS
- MS Data Acess Componets – Remote Data Services
- SQL Server
- NETBIOS – unprotected shares
- Anonymous Logon – null sessions
- LAN Manger Authentication – Weak LM Hashing
- Windows Authentication – No passwords or weak passwords
- Internet Explorer
- Remote Registry Access
- Windows Scripting Host

Risk List - FBI/SANS Top 10 Vulnerabilities Unix

- Remote Procedure Calls (RPC)
- Apache Web Server
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- File Transfer Protocol (FTP)
- R-Services – Trust Relationships
- Line Printer Daemon (LPD)
- Sendmail
- BIND/DNS
- Unix Authentication – no passwords, weak passwords

Prioritizing the Risks

- Categorize Risks
  - Critical
  - Non-Critical
- Utilize the Matrix Prioritizing Technique
- Criteria:
  - Scope of Impact
  - Negative Publicity
  - Cost to correct failure
  - Probability of an incident
- Weight = sum of vote values

Example Risk Matrix

Risk	Fire	Bad Passwd's	Sharing accounts	Spam	Operational policies	Total (WT)
Fire						
Bad Passwords						
Sharing accounts						
Spam						
Operational policies						

Is "Column Risk" more important than "Row Risk" ?

Example Risk Matrix

Risk	Fire	Bad Passwd's	Sharing Acct's	Spam	Operational Policies	Total (WT)
Fire		9	9	9	9	36
Bad Passwords	0		7	2	3	12
Sharing Accounts	0	2		5	0	7
Spam	0	7	4		0	11
Operational Policies	0	6	9	9		24

Is "Column Risk" more important than "Row Risk" ?

Wrap-Up Risk

Mapping Risks to Assets

Constructing a Risk-Asset Matrix

HP WORLD 2003
Solutions and Technology Conference & Expo

Mapping Risks and Assets

- We build a matrix that maps the ordered list of critical assets against the ordered list of risks regardless of whether or not
  - A particular risk actually applied to the asset
  - Controls exist and/or already in place
- The matrix provides general guidance about the order each asset/risk is examined.
- All assets/risks need to be examined eventually.

Mapping Risks and Assets

- Build a matrix of Risks & Assets
- The prioritized critical assets listed in order (high to low) down the left side.
- The prioritized risks are listed in order (high to low) across the top.
- Asset-Risk Weight = Asset Weight * Risk Weight

Asset / Risk Matrix

R/A Matrix	Risks	Fire	Oper. Policies	Bad Passwd's	Spam	Share Accts
Assets	WT	36	24	12	11	7
Bigguy	32	32x36	32x24	32x12	32x11	32x7
Network	31					
Payroll	12					
Email	9					
Ppes	6					

*Final R/A Matrix Weight = Asset Wt. * Risk Wt.*

Asset / Risk Matrix

R/A Matrix	Risks	Fire	Oper. Policies	Bad Passwd's	Spam	Share Accts.
Assets	WT	36	24	12	11	7
Bigguy	32	1152	768	384	352	224
Network	31	1116	744	372	341	217
Payroll	12	432	288	144	132	84
Email	9	324	216	48	99	63
Ppes	6	216	144	72	66	42

*Final R/A Matrix Weight = Asset Wt. * Risk Wt.*

Summary

- The Asset-Risk Matrix pairs the most critical risk/asset to least critical risk/asset.
- The most critical entries are in the upper left corner of the matrix.
- By using the weight formula, we can pick the top risks/assets that need to be addressed.
- This gives us a guideline for spending our security budget wisely.

Conclusions

- STAR provides a quantitative, **repeatable** method of prioritizing your assets.
- The matrices provide an easy to read summary of the state of your assets.
- These matrices can be used to provide your auditors with the information they need.
- The Asset/Risk Matrix contains the details to start building the audit/security check.
- The start of a baseline for Disaster Recovery.

Building Your IT Audit Plan/Checklist

Sample checklist/audit plans for Unix, NT and Windows 2000 Active Directory

HP WORLD 2003
Solutions and Technology Conference & Expo

CIS Rulers

- Rulers list a set of minimal actions that need to be done on a host system.
- This is a consensus list derived from security checklists provided by CIS charter members (VISA, IIA, ISACA, First Union, Pitney Bowes, Allstate Insurance, DOJ, Chevron, Shell Oil, VA Tech, Stanford, Catepillar, Pacific Gas & Electric, RCMP, DOD CIRT, Lucent, Edu Testing Services and others)
- Can't develop your own set? Use these!
- http://www.cisecurity.org

Applying Security to Assets

- General Strategy
  - Use STAR to identify critical risks and assets
  - Use CIS benchmarks to determine what computer services are required to allow the business function to work
  - Remove unnecessary services
  - Create the “security” script

Applying Security to Assets

- The CD to Production Cycle
  - Install OS from CD or “install” server.
  - Install applications
  - Apply vendor/application recommended and security patches
  - Install local tools (security, etc.)
  - Run CIS-based/STAR based customization
  - System is ready for production

The CIS Checklists

- CIS Solaris Benchmark Document
  - CIS Rating: After OS Installation - no patches
  - CIS Rating: After Security/Vendor Patch Installation
  - CIS Rating: After Applying Local Configuration Rules
- CIS Linux Benchmark Document
- CIS Windows 2000 Benchmark Document
- CIS Solaris Customization Script based on VT Risk Analysis

Require Vendor Security Compliance

- Terms and conditions of Purchase
  - Vendor must certify their product is not vulnerable to the threats listed in the SANS/FBI Top 20 Internet Vulnerabilities document (www.sans.org/top20.htm)
  - We've been doing this since 7/1/02. Only 2 vendors out of 700+ have declined.
- Prevent vendors from hampering our security efforts.

Summary

- Use STAR for Risk Analysis of IT assets.
- Use SANS/FBI Top 20 Internet Threats lists as a starting point.
- Use CIS benchmarks to get the actual commands needed to implement your policy based on your R/A.

References -

- Randy Marchany – Director of Security Lab, Virginia Tech
- WR Chisnal – “Applying Risk Analysis Methods to University Systems”
- Sans Institute, Zeki Yazar – A qualitative Risk Analysis and Management Tool – CRAMM
- Paper by Michael Ettredge & Vernon Richardson, U. of Kansas
- National State Auditors Association & GAO