



Introduction to IT Security Risk Analysis

**Arthur L. Coleman
Chief Strategy Officer
Polivec, Inc.**

October 6, 2004

1.866.POLIVEC

www.polivec.com

Overview

- **Why IT risk analysis has become an issue**
- **Definitions**
- **Where Risk Analysis Has to Go**
- **Where we Are Today**
 - Qualitative Risk Models
 - Quantitative Risk Models
- **Sample Bottom-Up Model**
- **Questions/Discussion**

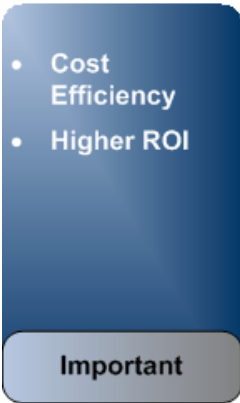
Polivec, Inc.



- The leader in security policy compliance solutions
- Foremost provider of standards & regulatory content
- Polivec Awards:
 - Best New Security Technology of 2002
 - Best Security Management Software 2003
 - Best of the Tests Finalist - Security Management, 2004
- 100+ customers
- Key partnerships include CSC, Unisys, HP, Center for Internet Security

The Issue: C-Level Demands on IT Have Changed Dramatically

- Internal and External Stakeholders**
- CEO
 - Board of Directors
 - CFO
 - Audit Committee
 - COO
 - Shareholders
 - Head of IA
 - Regulators
 - Directors
 - Capital Markets
 - Business Partners
 - Employees
 - Others



Pre-1990s



1990s

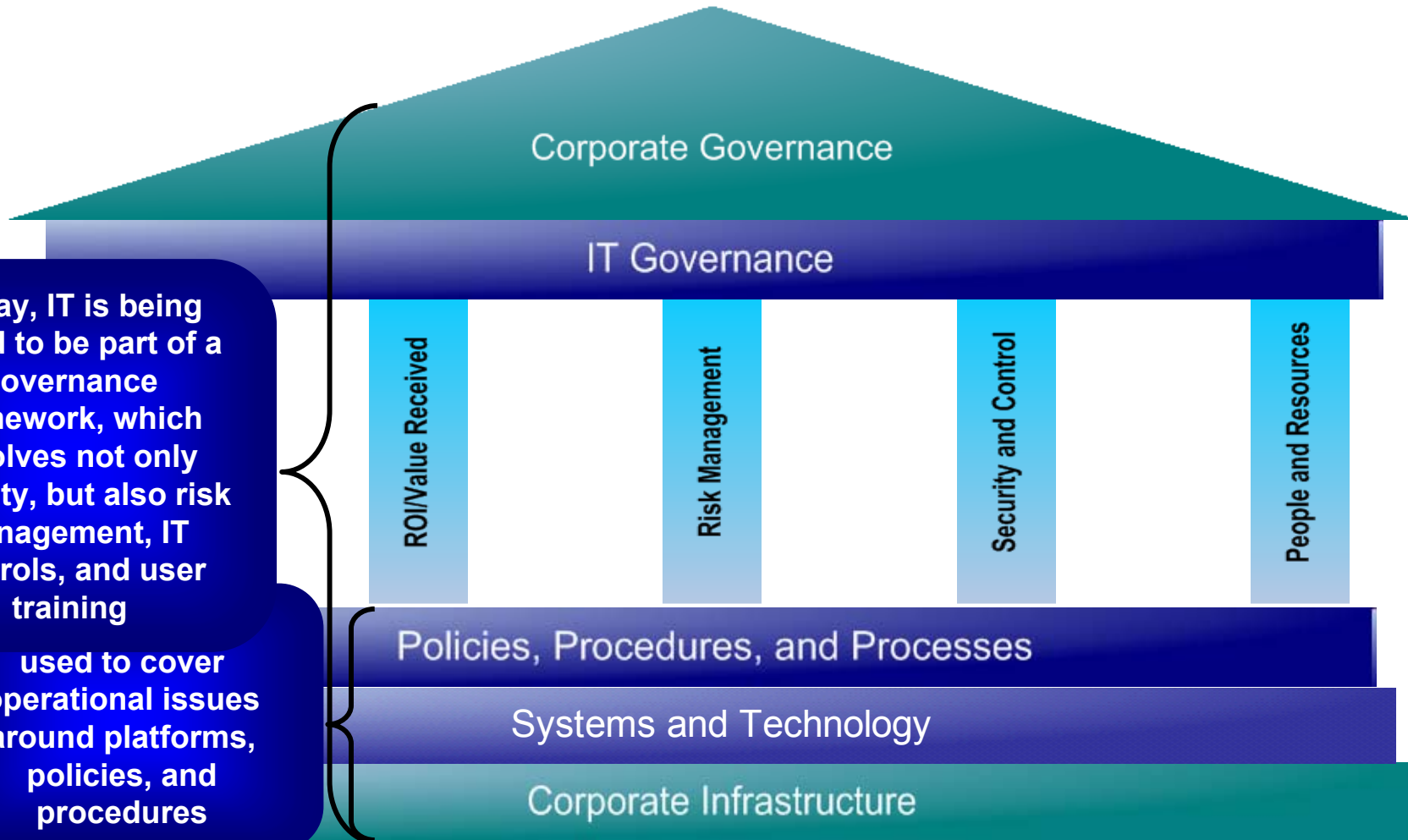


Post Sarbanes-Oxley

The Issue: IT Governance is a More Complex Mandate

Today, IT is being asked to be part of a governance framework, which involves not only security, but also risk management, IT controls, and user training

used to cover operational issues around platforms, policies, and procedures



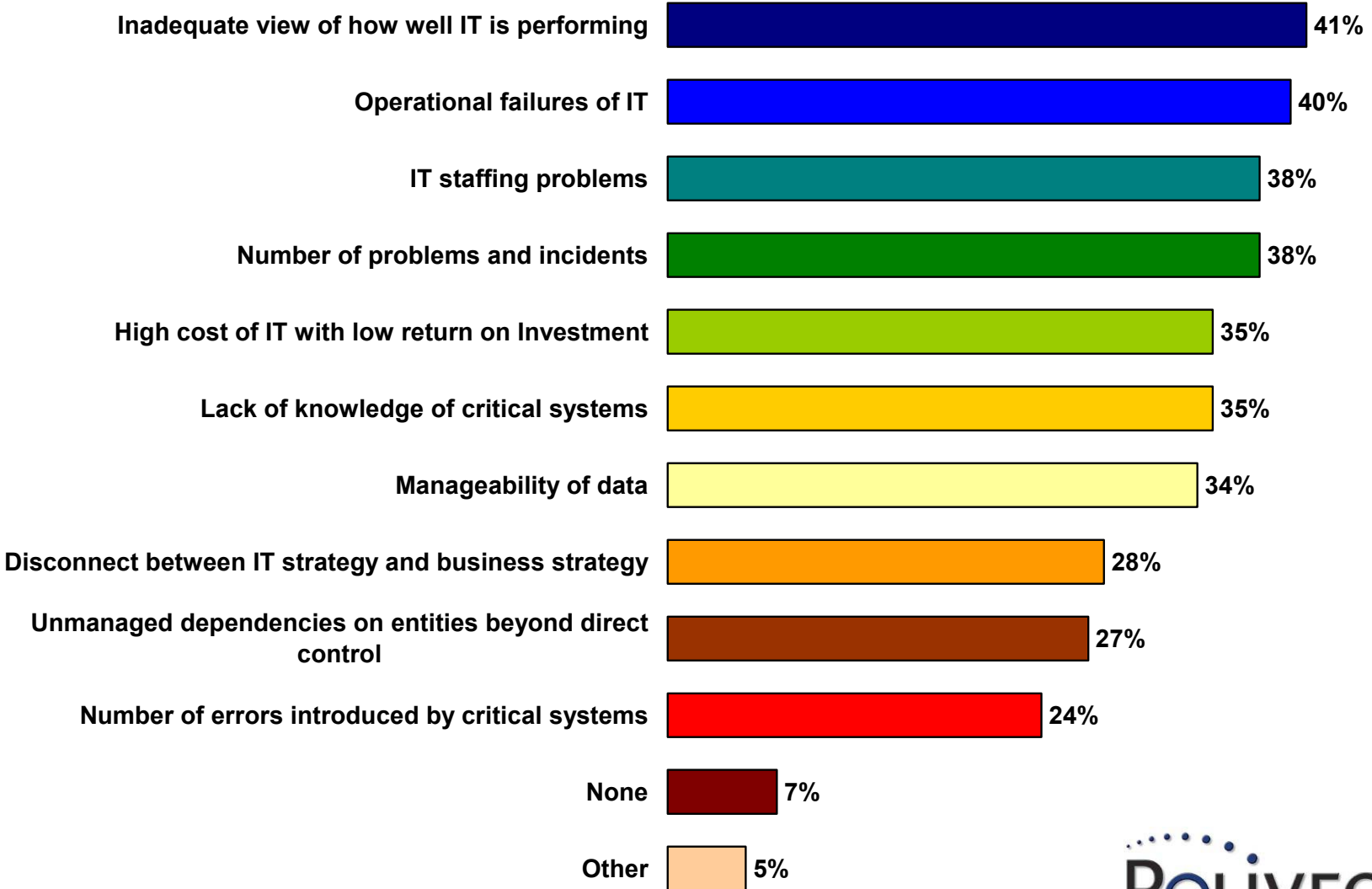
Why The Change: Significant Penalties, Personal Liability, Name & Shame

- **Example: Section 404 of Sarbanes-Oxley requires a constant evaluation of internal controls and procedures on company data.**
- **In cases of material non-compliance:**
 - the chief executive officer and the chief financial officer shall "reimburse the issuer for any bonus or other incentive-based or equity-based compensation received" during the twelve months following the issuance or filing of the non-compliant document and "any profits realized from the sale of securities of the issuer" during that period.

- Sarbanes-Oxley, Section 304



Problems Encountered with IT in the Last 12 Months



Source: IT Governance Institute

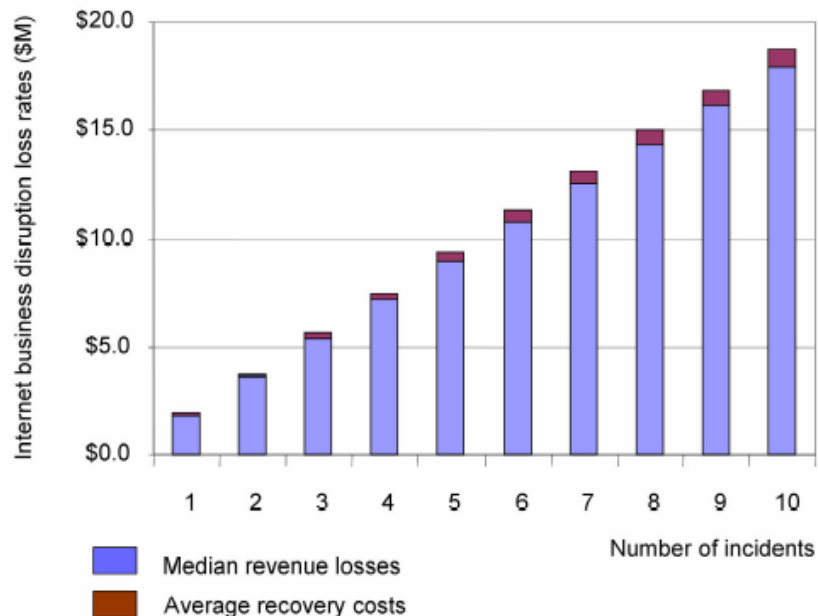
What are These Problems Costing Us

- **Symantec:**

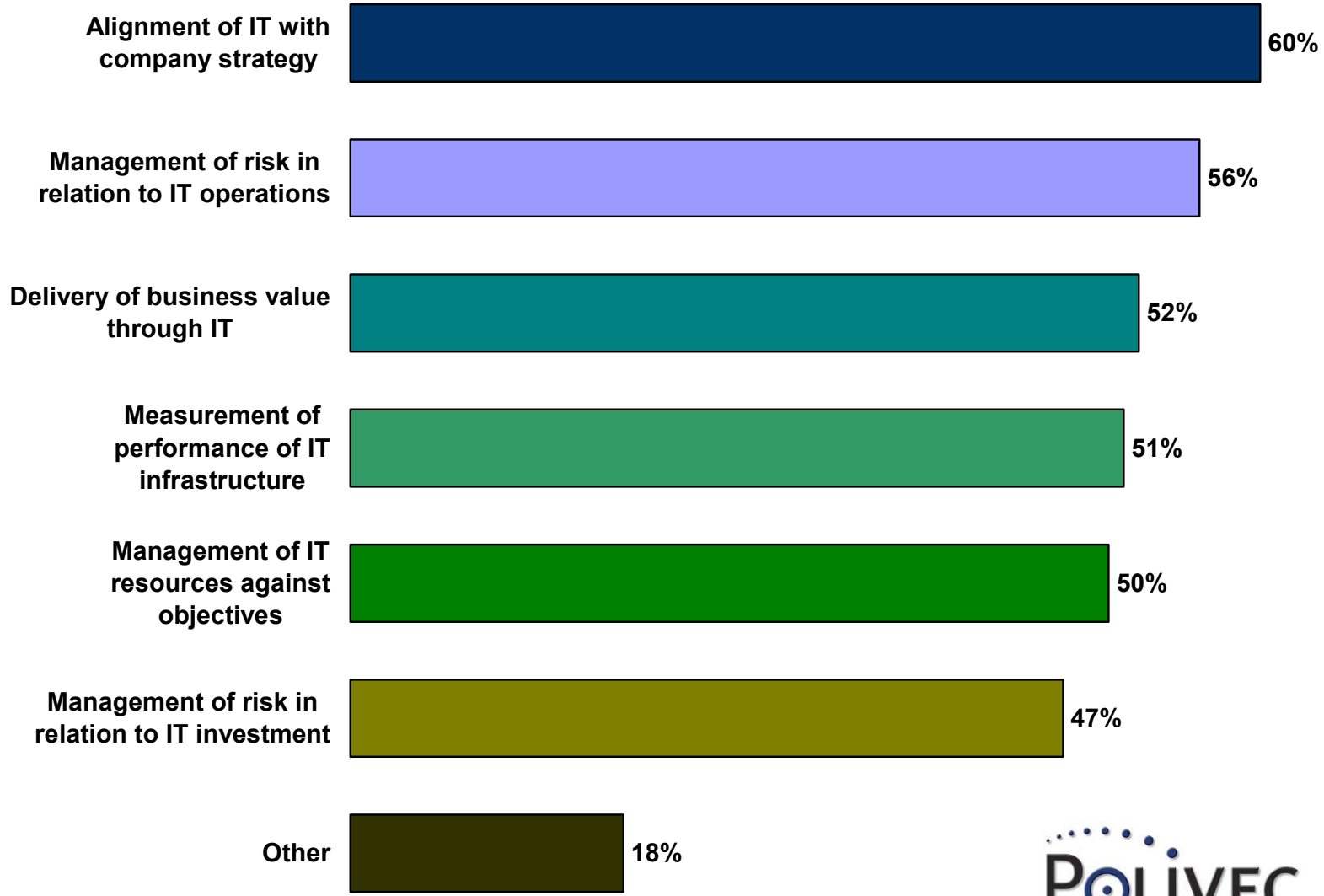
- 400% increase in attacks against e-commerce in last six months
- 7 new vulnerabilities every day
- 82% categorized as “easy to exploit”
- Monitored BOTs: grew from avg 2,000 to 30,000/day
- Time to exploit: 5.8 days
- Cost of compliance failure or breach of privacy
- Cost to brand

- **Aberdeen**

- Size of losses
 - 0.067% of revenue
 - Average of \$2mm/incident
 - One incident per year



What C-Level Execs Hope to Gain Through Better IT Governance



Source: IT Governance Institute

C-Level Needs from IT

- **Clear, auditable, IT policies and guidelines**
- **Tight linkage of policies to implementation**
- **Near-continuous monitoring of systems against policies/implementation standards**
- **Employees who operate by the policies**
- **Security performance metrics**
 - Compliance, operational, security quality of service
- **Security risk metrics**
- **Clear ROI/Payback for IT security investment**
 - Risk dashboards



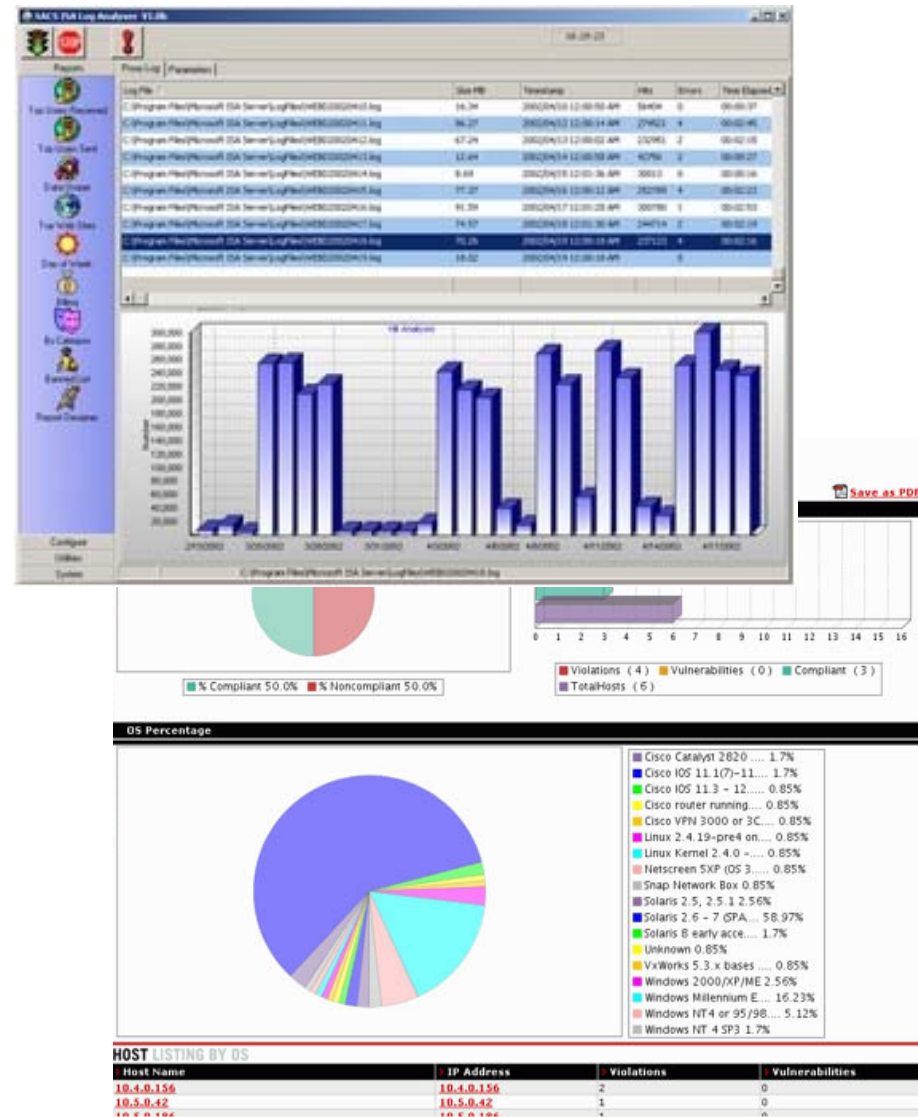
Why Do We Care About IT Security Risk Analysis

- **More business is being done on “open networks”**
 - 75% of firms doing sales and customer service over the Web
 - There is a trade off between securing systems and productivity benefits of access
- **Number of network connections exponentially increases the number of vulnerabilities**
 - IT is losing the battle
 - e.g. “Defense in depth” is “feel good” security



Why Do We Care About IT Security Risk Analysis

- Compliance issues have increased the exposure of C-Level executives
 - They want risk dashboards – can't run the business!
 - Compliance burden on IT has increased – can't run the business!
- Risk analysis is a critical tool to help us break the vicious cycle



Risk Analysis: What are the Goals of the Exercise

- To provide a structured methodology for mitigating IT security attacks
- To provide a cost/benefit framework for measuring how to apply limited resources to a business problem
 - Improve network design to reduce attack surface
 - Improve software design
 - Invest in high-value technologies
- To allow us to get back to running an agile business
- To provide a mechanism for summarizing the business issues to management



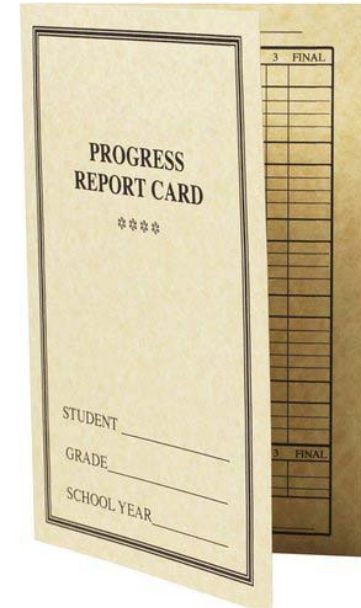
Definitions: Basic Concepts

- **Asset**
 - A device, software, information store, person, or process
- **Threat**
 - Any activity that represents a risk to information assets
- **Vulnerability**
 - A IT security weakness in an asset that can be exploited by a threat
- **Exploit**
 - A vulnerability that is known to have been exploited
- **Risk**
 - The likelihood of “loss” (e.g. financial loss) from a specific set of circumstances



Definitions: Basic Concepts

- **Countermeasure**
 - Any activity which is taken to minimize an IT security risk
- **(IT Security) Control**
 - A specific countermeasure that attempts to mitigate a specific vulnerability or vulnerabilities
- **(Risk) Mitigation**
 - The act of applying a countermeasure to reduce a risk
- **Policy**
 - A statement that provides a measurable target for a specific IT security control, process, or procedure



Definitions: Basic Concepts

- **Vulnerability Analysis**
 - The review of a network, a network segment, and associated people and processes (IT assets) to determine the type, number and significance of security vulnerabilities vs. known threats
- **Policy Analysis**
 - The review of IT assets against a defined set of policy statements
- **Financial Analysis**
 - An analysis of the financial impact of a set of IT security failures
- **Failure Analysis**
 - The review of IT assets, security vulnerabilities,
- **Risk Analysis**
 - The art of determining the real and potential losses on IT assets based on known failure modes and application of mitigating security controls



Risk Analysis Models

- **Analysis models come in a variety of types**
 - Early work goes back as far as 1970s
- **No one model is necessarily adequate**
- **Most analyses are concentrated on willful attacks**
 - Most risks are due to mistakes and accidents – operator error
- **Two general forms**
 - Qualitative
 - Quantitative
- **Ideal is quantitative (we are talking \$\$ after all)**
 - Reality: we are a long way from an ideal quantitative analysis
- **Qualitative does provide some useful insights in conjunction with quantitative**
 - Provides initial “range of value” and “do we care” estimates about specific failure modes.

Generation of Risk Analysis Methodologies

Generation of Method	Primary Features/Objective	System Development Methods and Means	Security Development Methods and Tools	Challenge	Weaknesses
First Generation: Checklist Methods (1972 – 1981)	Mapping limited solutions onto the information security problem	Surveys of available elements	Security checklists (eg. IBM AFIPS Checklist (1979))	Mapping problem to solution space	<ul style="list-style-type: none"> • Oversimplify problem • Checklists outdate quickly • High maintenance costs
Second Generation: Mechanistic Engineering Methods (1981 – present)	A partitioned solution that maps to specific IT assets, vulnerabilities, and threats	Mechanical analysis of assets, vulnerabilities and exploits	CRAMM BDSS COBRA Polivec CMS Pentana	<ul style="list-style-type: none"> • Organizing and integrating a complex set of elements • Volume of data to be collected 	<ul style="list-style-type: none"> • Complex design process • High degree of training required • Volume of data required • Bottom-up methods outdate quickly • No accurate database for event probabilities
Third Generation: Logical/Transformational Methods (2004??? - ????)	Highly abstracted design expressing problem and solution space	Flexible, probabilistic, structured analysis that accounts for continuous change, known and unknown vulnerabilities	None	<ul style="list-style-type: none"> • Compilation of accurate statistical databases • Complexity of topology analysis • Applying systems analysis to widely varying organizations 	<ul style="list-style-type: none"> • Cannot be done manually • Volume of data to be collected and maintained • Extensive computing power required • Underlying models complex and need extensive development time

Risk Analysis: The Ideal Includes Network Effects

- **Single event risk calculation:**
 - Risk = $P_{avg}(\text{Event}) * EL_{avg}(\text{Event})$ in monetary value (dollars)
 - where
 - P_{avg} = avg probability of an event occurring
 - EL_{avg} = expected \$ value of loss
- **Annualized risk calculation**
 - Adds time period element to calculation
 - Annualized Risk (Event) = $P_{avg}(\text{Event}) * EL_{avg}(\text{Event}) * N_{avg}(\text{Event})$
 - Where
 - $N_{avg}(\text{Event})$ = avg number of times event will occur per period

Risk Analysis: The Ideal Includes Network Effects

Single-point failure calculation

$$P_{\text{avg}}(\text{Event}, A) = P(A)$$

$$P(A) = P(\text{Threat}_i / V(A)_j)$$

$$R(A) = \sum_{i=1}^m \sum_{j=1}^n P(\text{Threat}_i / V(A)_j \times L_{ij})$$

Where

A = an IT Asset

T = a fault tree consisting of a cascading failure that occurs due to a specific threat i

P(A) = the avg probability that threat i will successfully exploit the Vulnerability j on Asset A

R(A) = IT Risk (in dollars) associated with IT Asset A

Threat i = a specific threat i

P(Threat i /V(A) j) = the avg probability that threat i will successfully exploit the vulnerability j on Asset A

L ij = the dollar value of a loss associated with the successful exploit of vulnerability j by threat i

Risk Analysis: The Ideal Includes Network Effects

- “Network effect” calculations:

$$P(T_{Threati}) = \sum_{R=1}^S P(R_{Threati}) \bigcap P(S_{Threati})$$

- Complete Analysis:

$$R(T) = P(T) \times L_T$$

$$\text{Total Risk} = \sum_{k=1}^z R(A_z) + R(T)$$

Where:

$L_{ij} =$	the dollar value of a loss associated with the successful exploit of vulnerability j by threat i
$P(T_{Threati}) =$	the cumulative probability that a combined exploit will occur for specific threat across all the fault trees associated with threat i
$R(T) =$	the IT risk (in dollars) associated with the exploit that occurs across all the fault trees associated with threat i

Why the Ideal is Unreachable Today

- **Only deals with known threats and vulnerabilities**
- **No existing historical databases to give accurate probabilities for:**
 - Vulnerability exploit
 - Single-point failure modes
 - Multi-level failure modes
- **Constant change:**
 - Underlying technologies changing daily
 - Network topologies changing continuously
 - Processes changing continuously
 - People changing continuously
- **No single point probabilities for anything**
 - Everything is a probability curve
- **May be a case of Goedel's incompleteness theorem**

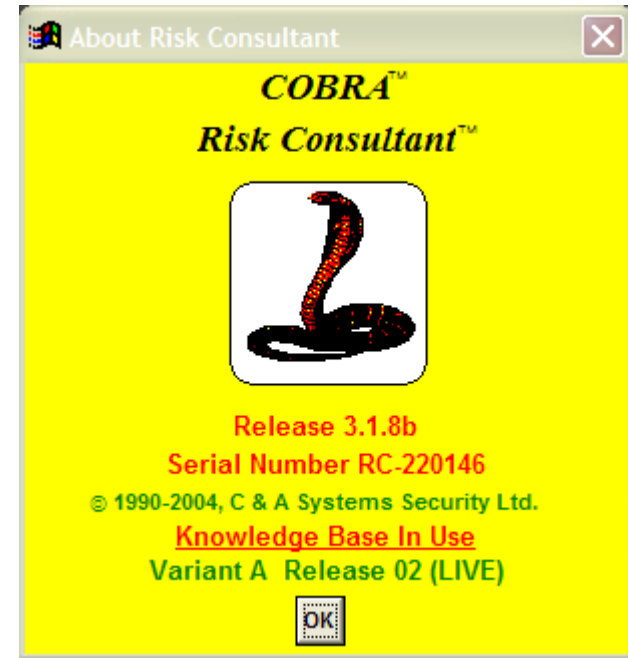


Qualitative Analysis Pros and Cons: An Example

- **Pros:**
 - Easy to perform
- **Cons:**
 - Results skewed by personal opinion
 - Without #s, management has a hard time making decisions
 - Without hard data – just a guess
- **Example:**
 - I'd like to buy something on line
 - There are lots of hackers
 - There have been numerous instances of identity theft
 - This web site is asking me for a credit card number

Example: COBRA

- From C&A Systems in the UK
- Questionnaire-driven expert system
- Provides a semi-quantitative (still really qualitative) view of IT security risks



Qualitative Analysis: Pros and Cons

Analysis So Far:

- **Threat: Lots of hackers**
- **Threat: Identity theft**
- **Vulnerability (perceived): site wants a credit card**
- **Conclusion: THIS IS RISKY. I won't buy**

Take it Further:

- **Compare to giving credit card to waiter in restaurant**
- **Which is riskier?**
 - 50% of credit card (present fraud due to card given to third party)
 - Likelihood of single card theft on internet: ???
- **Conclusion: No objectivity**

Quantitative Risk Models

- **Failure Mode, Effects and Criticality Analysis (FMECA)**
- **Cause Consequence Analysis**
 - Fault Tree Analysis
 - Event Tree Analysis
- **Security Plan Analysis**
- **Risk Dynamics**
- **Time Based**
- **Monte-Carlo Simulation**
- **Bayesian Probability Models (e.g. LRAM)**

Example: Bottom-up Risk Analysis using Existing Auditing Tools

- Physical asset only
- Looks at known vulnerabilities on each platform/application
- Mechanical, non-probabilistic
- Risk Level of Asset
- Danger level of vulnerability
- Likely cost of specific security breach
- No ability to consider network effects risk
- **Single-mode analysis only**

Step 1: Create a Checklist for a Specific Platform and Assign Danger Levels

- Create a list of every vulnerability or misconfiguration on a specific platform
- Vulnerabilities can rank in the hundreds for any platform
- How to create:
 - Software vendors
 - NSA, NIST, CIS lists
 - .inf files with Windows
- Shortcut:
 - What cumulative number of vulnerabilities represent 95% of the risk
 - Usually top 50

Description	ServiceName	Danger Level
Adapter Switching	IntelRoam	3
Alerter	Alerter	5
Application Layer Gateway Service	ALG	1
Application Management	AppMgmt	7
Ati HotKey Poller	Ati HotKey Poller	6
Automatic Updates	wuauerv	4
Background Intelligent Transfer Service	BITS	3
C-DillaCdaC11BA	C-DillaCdaC11BA	3
COM+ Event System	EventSystem	3
COM+ System Application	COMSysApp	3
Cisco Systems, Inc. VPN Service	CVPND	10
ClipBook	ClipSrv	1
Computer Browser	Browser	10
Crypkey License	Crypkey License	10
Cryptographic Services	CryptSvc	3
DHCP Client	Dhcp	5
DNS Client	Dnscache	1
Distributed Link Tracking Client	TrkWks	4
Distributed Transaction Coordinator	MSDTC	3
EPSON Printer Status Agent2	EPSONStatusAgent2	3
EpsonBidirectionalAgent	EpsonBidirectionalAgent	3
EpsonBidirectionalService	EpsonBidirectionalService	3
Error Reporting Service	ERSvc	10
Event Log	Eventlog	1
FTP Publishing	MSFtpsvc	10
Fast User Switching Compatibility	FastUserSwitchingCompatibility	10
HID Input Service	HidSrv	3
Help and Support	helpsvc	5
IIS Admin	IISADMIN	2
IMAPI CD-Burning COM Service	ImapiService	4
IPSEC Services	PolicyAgent	5
IPv6 Internet Connection Firewall	Ip6FwHlp	7
Indexing Service	cisvc	4
Intel NCS NetService	NetSvc	2
Internet Connection Firewall (ICF) / Internet C	SharedAccess	4
Logical Disk Manager	dmsrvr	7
Logical Disk Manager Administrative Service	dmadmin	8
MS Software Shadow Copy Provider	SwPrv	5
Machine Debug Manager	MDM	2
Message Queuing	MSMQ	4
Message Queuing Triggers	MSMQTriggers	3
Messenger	Messenger	5
NT LM Security Support Provider	NtLmSsp	2
Net Logon	Netlogon	4
NetMeeting Remote Desktop Sharing	mnmsvc	2
Network Connections	Netman	4
Network DDE	NetDDE	2

Step 2: Identify and Rank Assets for Risk

- Let's be clear – physical asset losses are least of our risks
- Rank assets based on value of information on them
 - Compliance risk
 - Regulatory risk
 - Privacy risk
- Best methods are simple:
 - 3 level is common
 - Government uses 5 level
 - Polivec recommends 4 level

Asset	Type	Category	Maximum Loss Value
acoleman	ExecPortable	3	\$ 100,000
pstaubs	Portable	1	\$ 10,000
ramaini	Portable	1	\$ 10,000
ramaral	Workstation	1	\$ 10,000
bney	ExecWorkstation	3	\$ 250,000
kgorsak	ExecWorkstation	3	\$ 10,000,000
rhendricks	Workstation	1	\$ 10,000
kstone	Portable	1	\$ 10,000
MarketingServer	File Server	2	\$ 1,000,000
AccountingData	File Server	4	\$ 8,000,000
AccountingPrint	Print Server	1	\$ 25,000
WebBastionHost	WebServer	2	\$ 75,000
NY_Server	Email Server	3	\$ 2,000,000
NY_Sales	File Server	2	\$ 1,000,000
Intranet_Server	Web Server	1	\$ 50,000
Cisco_VPN	VPN	1	\$ 7,500
Chicago_Branch1	File Server	1	\$ 1,000,000
Win2003LabServer	File Server	1	\$ 50,000
SF_Windows2003_MOM	MOM Server	1	\$ 50,000

Step 3: Assign Avg Loss Values to Checks/Assets for Each Category of Asset

- For each check, determine the \$\$ value or percentage of asset value at risk

Description	ServiceName	Danger Level	Percent of Exposure
Adapter Switching	IntelRoom	3	8.000%
Alerter	Alerter	5	10.000%
Application Layer Gateway	ALG	1	0.450%
Application Management	AppMgmt	7	2.300%
Ati HotKey Poller	Ati HotKey Poller	6	4.000%
Automatic Updates	wuauerv	4	20.000%
Background Intelligent Tran	BITS	3	0.650%
C-DillaCdaC11BA	C-DillaCdaC11BA	3	0.450%
COM+ Event System	EventSystem	3	0.012%
COM+ System Application	COMSysApp	3	1.200%
Cisco Systems, Inc. VPN Se	CVPND	10	8.900%
ClipBook	ClipSrv	1	6.000%
Computer Browser	Browser	10	7.500%
Crypkey License	Crypkey License	10	0.338%
Cryptographic Services	CryptSvc	3	1.725%
DHCP Client	Dhcp	5	3.000%
DNS Client	Dnscache	1	15.000%
Distributed Link Tracking C	TrkWks	4	0.488%
Distributed Transaction Co	MSDTC	3	0.338%
EPSON Printer Status Agen	EPSONStatusAgent2	3	0.009%
EpsonBidirectionalAgent	EpsonBidirectionalAg	3	0.900%
EpsonBidirectionalService	EpsonBidirectionalSe	3	6.675%
Error Reporting Service	ERSvc	10	4.500%
Event Log	Eventlog	1	5.625%
FTP Publishing	MSFtpsvc	10	0.253%
Fast User Switching Compa	FastUserSwitchingCo	10	1.294%
HID Input Service	HidServ	3	2.250%
Help and Support	helpsvc	5	11.250%
IIS Admin	IISADMIN	2	0.366%
IMAPI CD-Burning COM Se	ImapiService	4	0.253%
IPSEC Services	PolicyAgent	5	0.007%
IPv6 Internet Connection Fi	Ip6FwHlp	7	0.675%
Indexing Service	cisvc	4	5.006%
Intel NCS NetService	NetSvc	2	3.375%
Internet Connection Firewa	SharedAccess	4	4.219%
Logical Disk Manager	dmserver	7	0.190%
Logical Disk Manager Admi	dmadmin	8	0.970%
MS Software Shadow Copy	SwPrv	5	1.688%
Machine Debug Manager	MDM	2	8.438%
Message Queuing	MSMQ	4	0.274%
Message Queuing Triggers	MSMQTriggers	3	0.190%
Messenger	Messenger	5	0.005%
NT LM Security Support Pro	NtLmSsp	2	0.506%
Net Logon	Netlogon	4	3.755%
NetMeeting Remote Deskto	mnmsrvc	2	2.531%
Network Connections	Netman	4	3.164%
Network DDE	NetDDE	2	0.142%

Step 5: Perform a Vulnerability Analysis

Asset Name: AccountingData					
Date of Scan: October 3, 2004		Scanned By: Arthur L. Coleman		Scan Type: Full	
Description	ServiceName	Danger Level	Percent of Exposure	Policy	Actual
Adapter Switching	IntelRoam	3	8.000%	Automatic, Running	Manual
Alerter	Alerter	5	10.000%	Manual	Automatic, Running
Application Layer Gateway Service	ALG	1	0.450%	Manual	Automatic, Running
Application Management	AppMgmt	7	2.300%	Manual	Automatic, Running
Automatic Updates	wuauerv	4	20.000%	Automatic, Running	Manual
Background Intelligent Transfer Service	BITS	3	0.650%	Automatic, Running	Manual
COM+ System Application	COMSysApp	3	1.200%	Manual	Automatic, Running
ClipBook	ClipSrv	1	6.000%	Manual	Automatic, Running
DHCP Client	Dhcp	5	3.000%	Automatic, Running	Manual
Distributed Transaction Coordinator	MSDTC	3	0.338%	Manual	Automatic, Running
Error Reporting Service	ERSvc	10	4.500%	Automatic, Running	Manual
Fast User Switching Compatibility	FastUserSwitchingCom	10	1.294%	Manual	Automatic, Running
HID Input Service	HidServ	3	2.250%	Automatic, Running	Manual
Help and Support	helpsvc	5	11.250%	Automatic, Running	Disabled
IIS Admin	IISADMIN	2	0.366%	Automatic, Running	Manual
IMAPI CD-Burning COM Service	ImapiService	4	0.253%	Manual	Automatic, Running
IPSEC Services	PolicyAgent	5	0.007%	Disabled	Manual
Logical Disk Manager Administrative Service	dmadmin	8	0.970%	Manual	Automatic, Running
MS Software Shadow Copy Provider	SwPrv	5	1.688%	Manual	Automatic, Running
Message Queuing	MSMQ	4	0.274%	Automatic, Running	Manual
Message Queuing Triggers	MSMQTriggers	3	0.190%	Automatic, Running	Manual
Messenger	Messenger	5	0.005%	Automatic, Running	Manual

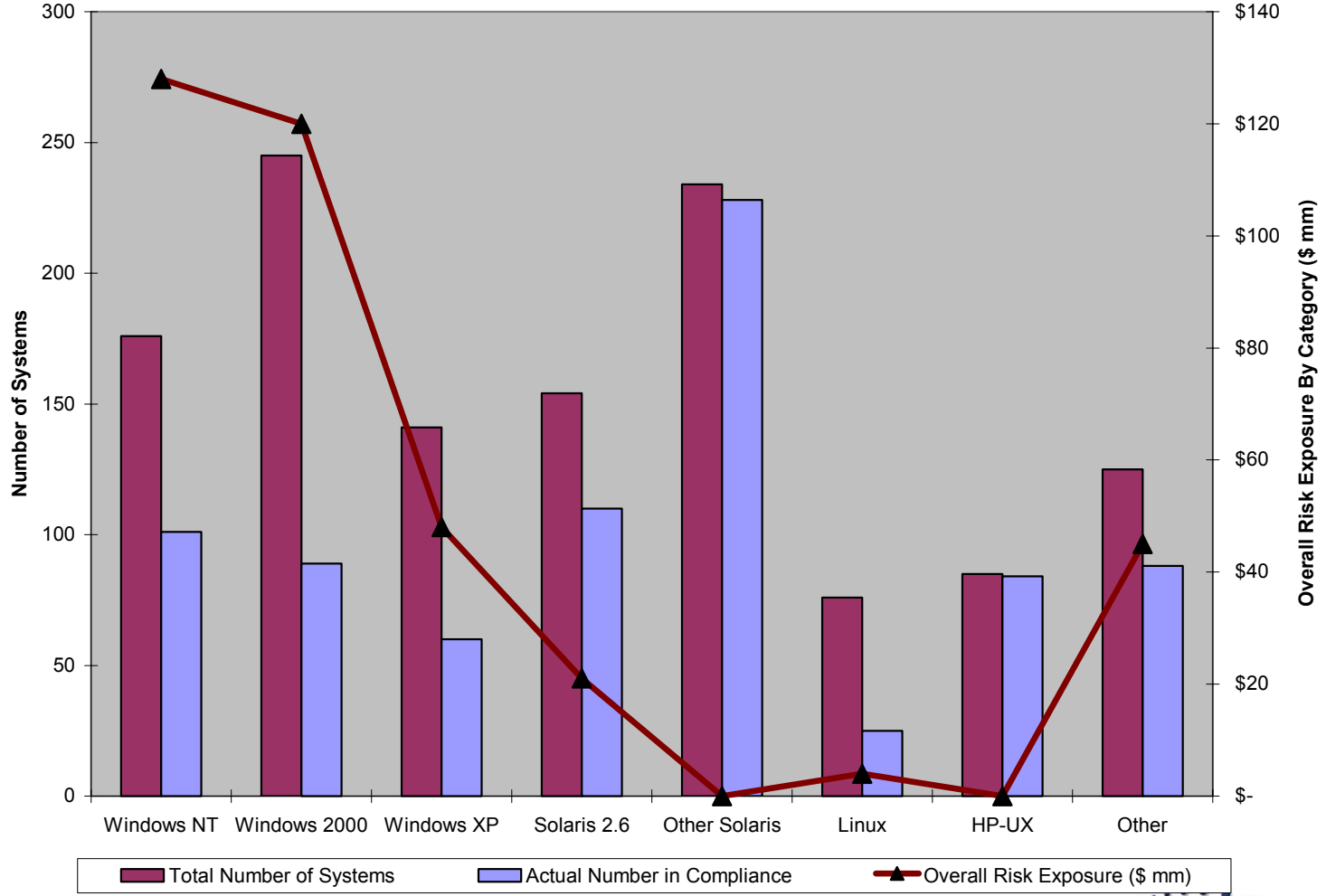
Step 6: Sum the exposures on a single machine

Asset Name: AccountingData							
Date of Scan: October 3, 2004		Scanned By: Arthur L. Coleman			Scan Type: Full		
Description	ServiceName	Metric Calculation			Dollar-Value Calculation		
		Danger Level	Asset Risk Category	Total Setting Exposure	Asset Exposure	Percent of Exposure	Total Setting Exposure
Adapter Switching	IntelRoam	3	4	12	\$ 8,000,000	8.000%	\$ 640,000
Alerter	Alerter	5	4	20	\$ 8,000,000	10.000%	\$ 800,000
Application Layer Gateway Service	ALG	1	4	4	\$ 8,000,000	0.450%	\$ 36,000
Application Management	AppMgmt	7	4	28	\$ 8,000,000	2.300%	\$ 184,000
Automatic Updates	wuuser	4	4	16	\$ 8,000,000	20.000%	\$ 1,600,000
Background Intelligent Transfer Service	BITS	3	4	12	\$ 8,000,000	0.650%	\$ 52,000
COM+ System Application	COMSysApp	3	4	12	\$ 8,000,000	1.200%	\$ 96,000
ClipBook	ClipSrv	1	4	4	\$ 8,000,000	6.000%	\$ 480,000
DHCP Client	Dhcp	5	4	20	\$ 8,000,000	3.000%	\$ 240,000
Distributed Transaction Coordinator	MSDTC	3	4	12	\$ 8,000,000	0.338%	\$ 27,000
Error Reporting Service	ERSvc	10	4	40	\$ 8,000,000	4.500%	\$ 360,000
Fast User Switching Compatibility	FastUserSwitchingCom	10	4	40	\$ 8,000,000	1.294%	\$ 103,500
HID Input Service	HidServ	3	4	12	\$ 8,000,000	2.250%	\$ 180,000
Help and Support	helpsvc	5	4	20	\$ 8,000,000	11.250%	\$ 900,000
IIS Admin	IISADMIN	2	4	8	\$ 8,000,000	0.366%	\$ 29,250
IMAPI CD-Burning COM Service	ImapiService	4	4	16	\$ 8,000,000	0.253%	\$ 20,250
IPSEC Services	PolicyAgent	5	4	20	\$ 8,000,000	0.007%	\$ 554
Logical Disk Manager Administrative Service	dmadmin	8	4	32	\$ 8,000,000	0.970%	\$ 77,625
MS Software Shadow Copy Provider	SwPrv	5	4	20	\$ 8,000,000	1.688%	\$ 135,000
Message Queuing	MSMQ	4	4	16	\$ 8,000,000	0.274%	\$ 21,938
Message Queuing Triggers	MSMQTriggers	3	4	12	\$ 8,000,000	0.190%	\$ 15,188
Messenger	Messenger	5	4	20	\$ 8,000,000	0.005%	\$ 415
Total for Accounting Data				396		74.984%	\$ 5,998,719

Step 7: Sum Exposures Across All Machines

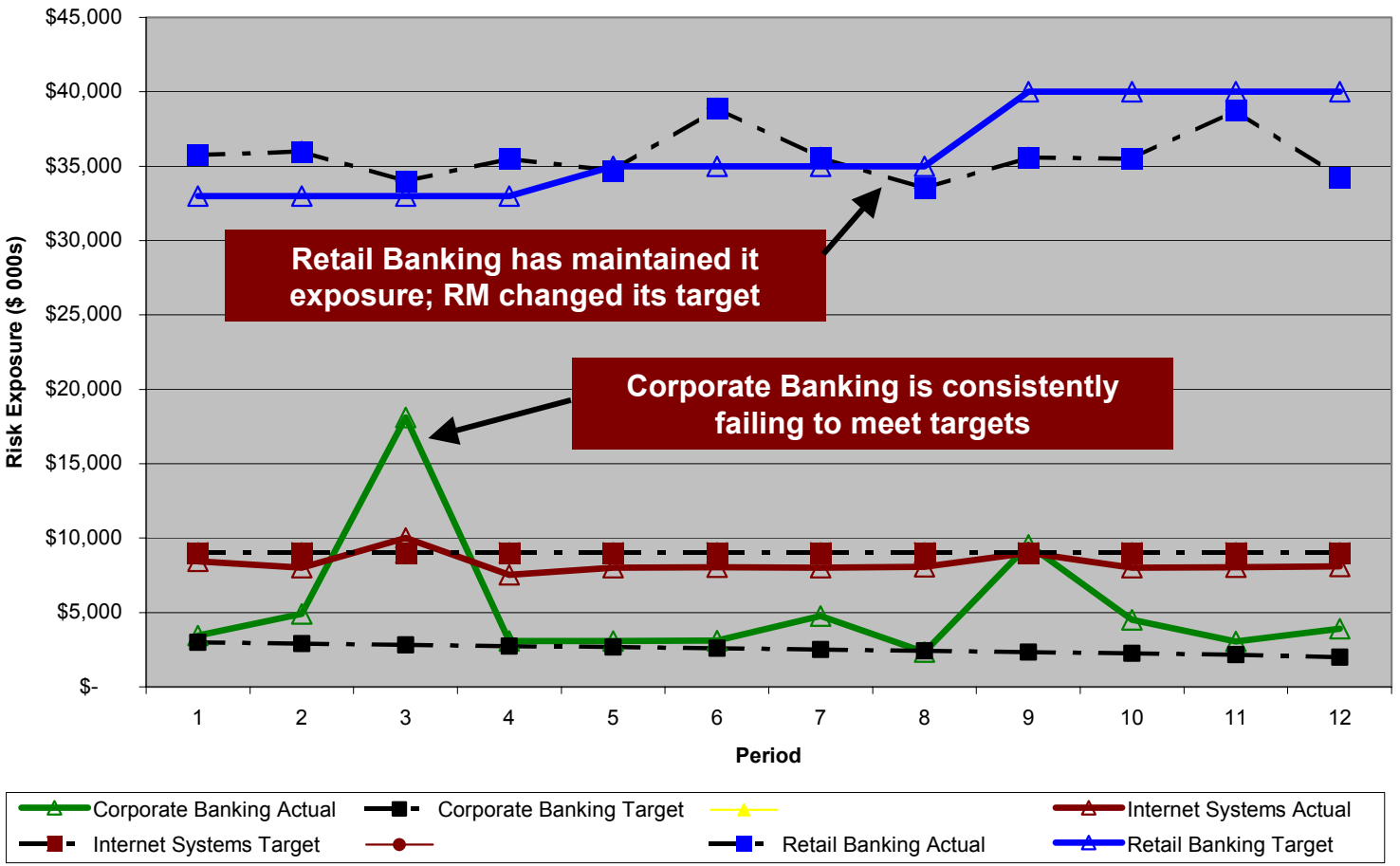
Asset	Type	Category	Maximum Loss Value	Number of Vulnerabilities	Total Exposure Metric	Current Exposure	Avg Cost/Exposure
AccountingData	File Server	4	\$ 8,000,000	22	1,245	\$ 5,998,719	\$ 272,669
kgorsak	ExecWorkstation	3	\$ 10,000,000	11	365	\$ 1,678,543	\$ 152,595
NY_Server	Email Server	3	\$ 2,000,000	11	567	\$ 598,934	\$ 54,449
NY_Sales	File Server	2	\$ 1,000,000	19	189	\$ 233,433	\$ 12,286
bney	ExecWorkstation	3	\$ 250,000	24	786	\$ 221,482	\$ 9,228
Chicago_Branch1	File Server	1	\$ 1,000,000	3	45	\$ 134,452	\$ 44,817
acoleman	ExecPortable	3	\$ 100,000	18	245	\$ 97,865	\$ 5,437
SF_Windows2003_MOM	MOM Server	1	\$ 50,000	3	33	\$ 17,689	\$ 5,896
Win2003LabServer	File Server	1	\$ 50,000	4	76	\$ 13,252	\$ 3,313
WebBastionHost	WebServer	2	\$ 75,000	5	165	\$ 10,678	\$ 2,136
rhendricks	Workstation	1	\$ 10,000	13	125	\$ 10,000	\$ 769
Cisco_VPN	VPN	1	\$ 7,500	4	120	\$ 7,500	\$ 1,875
Intranet_Server	Web Server	1	\$ 50,000	4	116	\$ 3,598	\$ 900
pstaubs	Portable	1	\$ 10,000	5	75	\$ 2,456	\$ 491
ramaini	Portable	1	\$ 10,000	7	90	\$ 2,432	\$ 347
ramaral	Workstation	1	\$ 10,000	6	85	\$ 1,345	\$ 224
kstone	Portable	1	\$ 10,000	1	75	\$ 150	\$ 150
MarketingServer	File Server	2	\$ 1,000,000	-	-	\$ -	\$ -
AccountingPrint	Print Server	1	\$ 25,000	-	-	\$ -	\$ -
Total Exposure				160	4,402	\$ 9,032,528	\$ 56,453

Step 7: Generate a Report



Step 7: Generate a Report

Summary of Risk Exposure By Department



Conclusions

- **IT Risk Analysis is in Its Infancy**
 - 3 generation: technology has gotten to Gen 2
 - Gen 3 is very hard: involves models that still need to be developed
- **Two ways to apply today**
 - Qualitative analysis
 - Quantitative analysis
- **Numerous methods**
 - Apply them carefully and in conjunction with each other
 - Software packages are beginning to implement Gen 2 approaches