Identifying, Assessing, and Controlling Risk

Chapters 7 and 8, Management of Information Security Whitman and Mattord © 2004

THE EXPLOSION OF BOTNETS HAS MANDATED A NEW WARNING LABEL:

Risk Management

- Sun Tsu, The Art of War:

  If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Know your enemy

- Once the organization knows its own weaknesses, organizations can then focus on:
  - Identifying Risks
  - Examining Threats
  - Understanding Risks and Threats
  - Determine how to control or mitigate risks and threats
- Known as Risk Management, or a Risk Management Program

Know yourself

- All systems are vulnerable, from within and from outside
- Mitigate risk by understanding how data is processed, stored, and transmitted
- Risk management programs must be maintained and kept current
- 3 groups – Information Security, Information Technology, and Management/Users.

Risk Identification and Assessment Process

1. Plan and Organize Process
2. Create System Component Categories
3. Develop Inventory of Assets
4. Identify Threats
5. Specify Vulnerable Assets
6. Assign Value or Impact Rating to Assets
7. Assess Likelihood of Vulnerabilities
8. Calculate Relative Risk Factor for Assets
9. Preliminary Review of Possible Controls
10. Document Findings

Inventory of Assets

- People
  - Inside and outside organization
- Procedures; standard procedures and sensitive ones – those that introduce risk
- Data – transmitting, processing, and storing
- Software – applications, operating systems, & security
- Hardware – systems, peripherals, and security devices
- Network – often focus of attacks, and as such, separate from software and hardware. Internal and external

Classifying and Categorizing Assets

- Once assets are identified, they must be analyzed against organization's risk management program, developing an inventory of assets
- Inventory should reflect sensitivity and security priority of each asset
  - Consider Confidential, Internal, and Public
- Classification should be comprehensive and mutually exclusive.

Assign Values for Information Assets

- As assets are identified, categorized, and classified, a relative value must also be assigned.
- Value can be based on:
  - Most critical to the success of the organization
  - Generates most revenue
  - Generates the highest profitability
  - Most expensive to replace
  - Most expensive to protect
  - Most embarrassing/liable if compromised

Data Classification

- Data classification model needs to fit your organization.
- Consider security clearances if level of security warrants it.
- Periodical reviews
- Management of classified information assets
  - Includes storing, distribution, portability, and destruction.
  - Extreme examples include military – requires discipline.
  - “Clean Desk” policy
  - Dumpster Diving

Sample Asset Classification

Information Asset	Data Classified	Impact to Profitability
Information Transmitted:		
EDI Document Set 1 - Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 - Supplier Orders (outbound)	Confidential	High
EDI Document Set 2 - Supplier Fulfillment Advise (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer Service Request via e-mail (inbound)	Private	Medium

Order of Importance

- Once asset values are determined, prioritize them
- Use a weighted factor analysis worksheet to ensure accuracy of analysis
  - Helpful in determining most critical and least critical assets
  - Consider using different criteria to help define overall asset value

Potential Loss or Value

- Use information documented during risk identification to assign weighted scores to information assets
- Could again use 1 – 100 range, with 100 being reserved for assets so critical their loss would immediately stop company operations

Example Weighted Factor

Information Asset	Criteria 1; Impact on Revenue	Criteria 2: impact on Profitability	Criteria 3: Impact on Public Image	Weighted Score
Criterion Weight (1 - 100); Must total 100	30	40	30	
EDI Document Set 1 - Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2 - Supplier Orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2 - Supplier Fulfillment Advise (inbound)	0.4	0.5	0.3	41
Customer Order via SSL (inbound)	1	1	1	100
Customer Service Request via e-mail (inbound)	0.4	0.4	0.9	55

Threat Identification

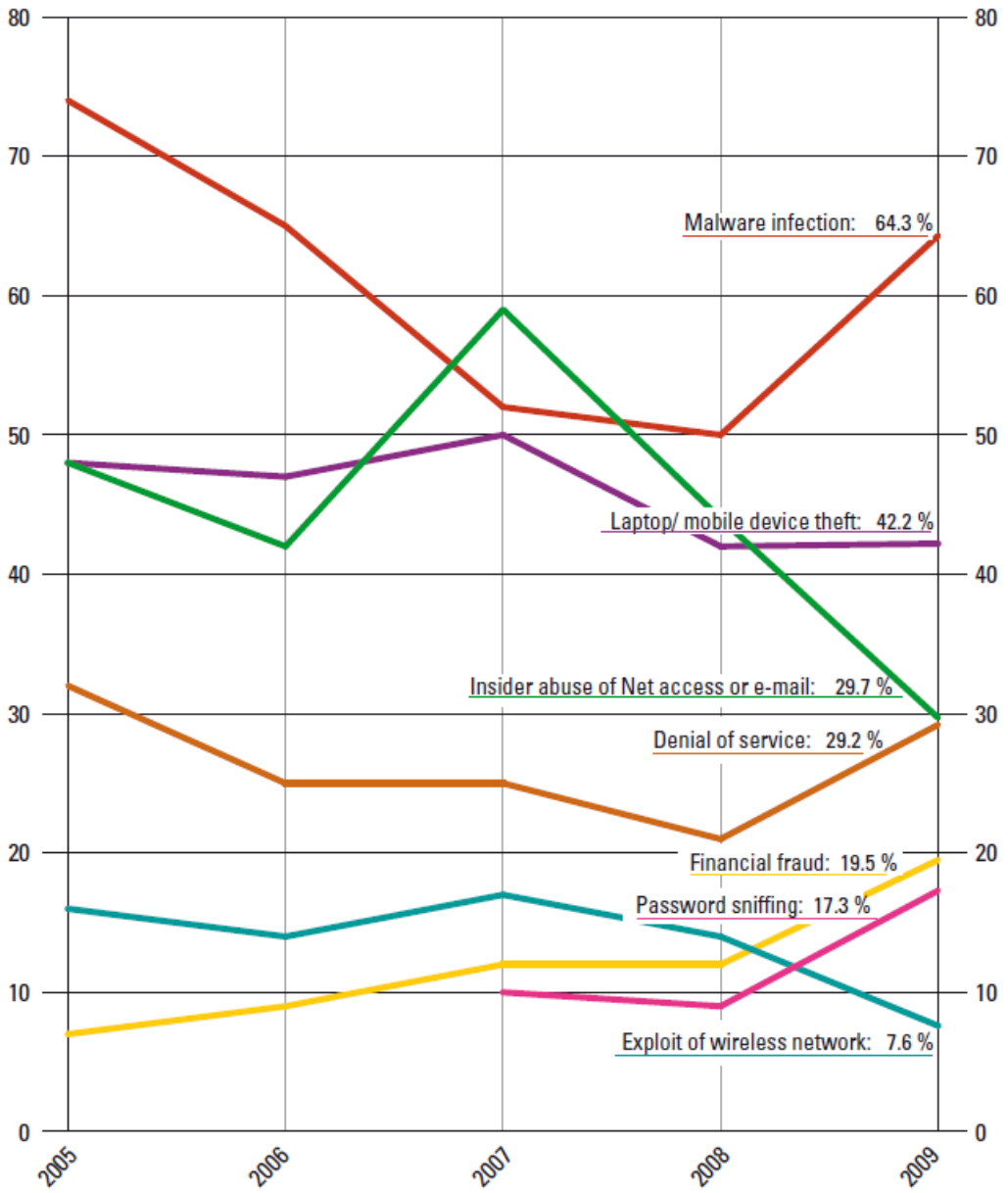
- All systems are subject to a range of threats.
- If you assume every threat is a threat to every asset, the project scope of your asset and threat identification, and risk management program, become too complex
- Threats need to be identified and prioritized

Identify and Prioritize Threats

- Human error or failure
- Compromises to intellectual property
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attacks
- Forces of nature
- 3rd party QOS variations
- Technical hardware failures or errors
- Technical software failures or errors
- Technical obsolesce

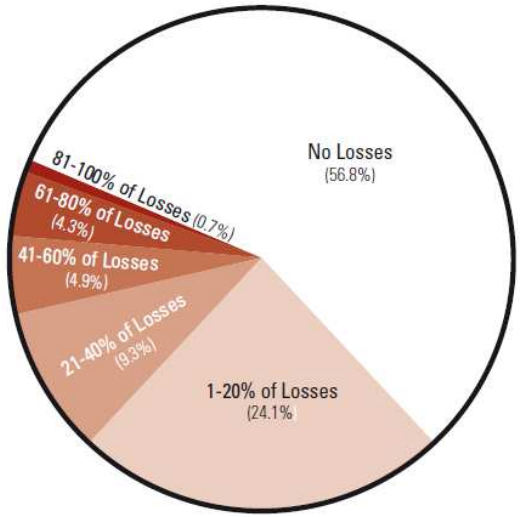
Types of Attacks Experienced

By Percent of Respondents

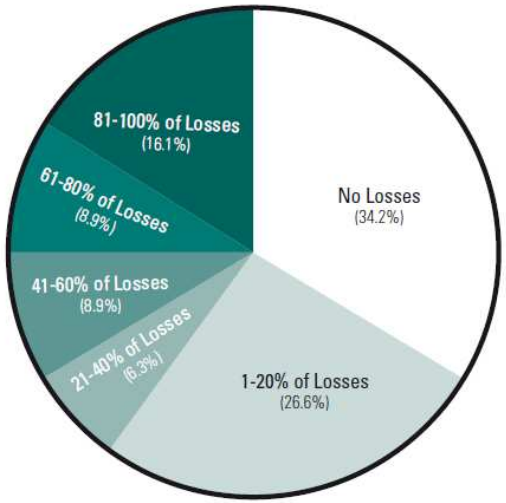


Losses due to Insiders

Malicious



Non-Malicious



Source: 2009 C

Vulnerability Assessment

- Vulnerabilities are specific avenues that threat agents can exploit to attack information assets
- Once the information assets have been identified and threat assessment criteria have been documented, review information assets for each threat.
- This produces a list of vulnerabilities

Risk Assessment

- Assigning a risk rating or score to each specific vulnerability. Not a specific score, but a method to gauge relative risk associated with each vulnerability.
- Risk = Likelihood of the occurrence of vulnerability * value of asset – percent of risk mitigated by current controls + uncertainty of current knowledge of vulnerability

Likelihood

- Overall rating – a numeric value from 0.1 to 1.0
  - Likelihood of meteor strike would be 0.1
  - Likelihood of receiving an email virus would be 1.0
- Could use 1 – 100 or whatever range
- Probably shouldn’t use 0, as nothing is impossible
- Use professionalism, experience, and judgment to assign likelihood; be consistant

Risk Currently Mitigated

- Determine how much of the risk is currently covered; percentage of likelihood * value

Uncertainty

- As it is impossible to know everything about every vulnerability; frequency, likelihood, impact, etc… This uncertainty should be added to the overall risk assessment
- Again; percent of likelihood * value

Ranked Vulnerability Example

Asset	Asset Impact	Vulnerability	Vulnerability Likelihood	Risk Rating Factor
Customer service request via email (inbound)	55	Disruption due to hardware failure	0.2	11
Customer service request via email (inbound)	55	Disruption due to software failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web Server failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server ISP service failure	0.1	10
Customer service request via email (inbound)	55	E-mail disruptions due to SMTP mail relay attack	0.1	5.5
Customer service request via email (inbound)	55	E-mail disruptions due to ISP service failure	0.1	5.5
Customer service request via email (inbound)	55	E-mail disruptions due to power failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web Server DOS attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web Server software failure	0.01	1
Customer order via SSL (inbound)	100	Lost orders due to Web Server buffer overrun attack	0.01	1

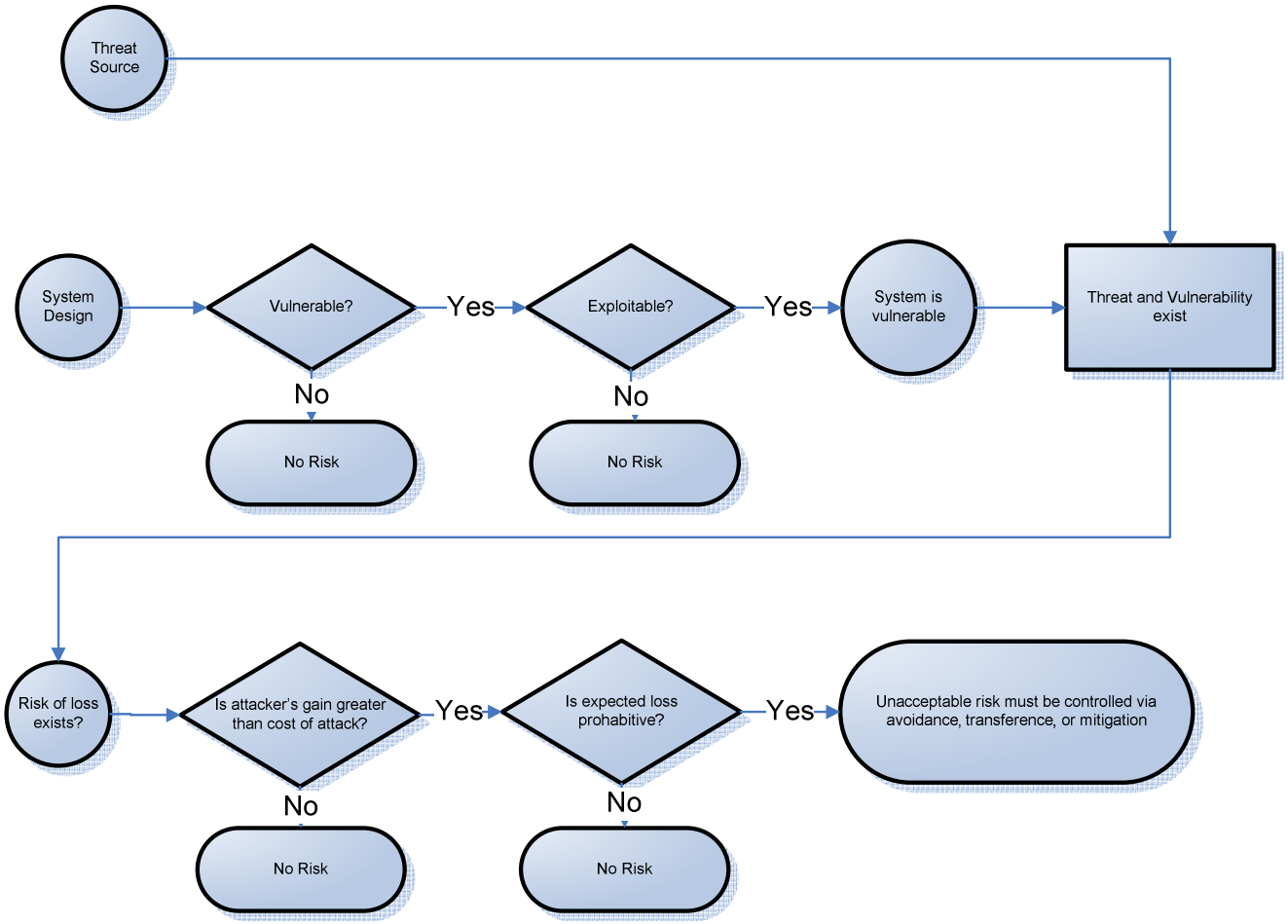
Follow up Review and Documentation

- The goal overall thus far is to identify information assets and their vulnerabilities and to rank them according to their need for protection. Much information about the assets, their threats, and existing controls will be gathered to achieve this.
- The final summarized document is the ranked vulnerability risk worksheet.

Risk Control Strategies

- Once risk vulnerability worksheet has been created, security and IT teams must choose a strategy top control the risks
  - Avoidance – safeguards to eliminate or reduce risks of the vulnerability
  - Transference – shifting the risk to other areas or outside the organization
  - Mitigation – reduce impact should vulnerability be exploited
  - Acceptance – accepting risk without trying to control or attempts to mitigate

Risk-Handling Action Points



Categories of Control

- Controlling risks by means of avoidance, mitigation, or transference can be defined through these four control categories or layers;
  - Control Function – preventative or detective controls to defend vulnerability
  - Architectural Layer – controls that apply to more than one layer; firewalls, policies, security apps
  - Strategy Layer – avoidance, mitigation, or transference
  - Information Security Principal – commonly accepted information security principals

Information Security Principals

- Confidentiality – when control provides assurance of the confidentiality of asset
- Integrity – when control ensures asset is correct
- Availability – ensures asset is available as expected
- Authentication – users of asset are who they claim to be
- Authorization – users of asset are allowed to use it
- Accountability – activities taken can be traced to user
- Privacy – access, update, and removal of asset complies with legislation

Feasibility Studies and CBA

- Before implementing strategy, an understanding of economic and non-economic consequences must be understood
- Number of ways, very much organizational specific
- Deliverable can be a cost avoidance by implementing strategy

Recommended Risk Control Practices

- Once risk assessment has determined cost of protecting valuable and vulnerable assets, and the potential cost, there is often a battle within organizations to justify or lower that cost.
  - Important to develop/document strong justification
- The Operationally Critical Threat, Asset, and Vulnerability Evaluation method (OCTAVE)
- http://www.cert.org/octave/

OCTAVE Method

- Preparing For OCTAVE
- Phase 1 Build Asset-based Threat Profiles
  - Process 1: Identify Senior Management Knowledge
  - Process 2: Identify Operational Area Management Knowledge
  - Process 3: Identify Staff Knowledge
  - Process 4: Create Threat Profiles

OCTAVE Method (cont)

- Phase 2 Identify Infrastructure Vulnerabilities
  - Process 5: Identify Key Components
  - Process 6: Evaluate Selected Components
- Phase 3 Develop Security Strategy And Plans
  - Process 7: Conduct Risk Analysis
  - Process 8: Develop Protection Strategy