

Class 2 EMTM 604

Gregg Vesonder

University of Pennsylvania

Penn Engineering - Computer & Information Science

©2009 Gregg Vesonder

Roadmap

- Schedule
- Logbook
- Dave Kormann:
 - Network Security
 - Firewalls
 - IPsec
 - Internet Key Exchange
 - VPNs
 - Security Policy
- Current readings: Dhillon, chapters 5-9; Schneier, chapters 10 through 14
- Readings next class: Dhillon, chapters 13-14, Canon, chapters 1-8 and Schneier, chapters 1-5

Schedule

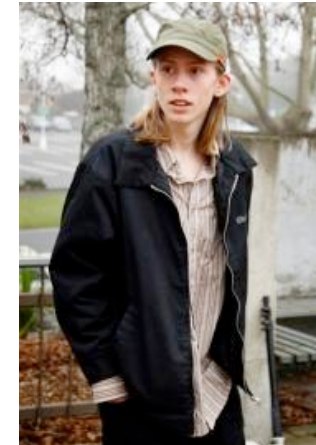
- Dave Kormann Lecture - March 27th
- Patrick McDaniel Lecture - April 24th
- Home Audit due April 10th
- Logbooks due April 24th
- Team generated security and privacy policy - May 8th
- Still five lectures from me too!
- **Note 5 long lectures!**
- Missing schedules will result in grade deduction unless a prior arrangement has been made - I am flexible but ...
- If you email me material do not assume I received it unless I confirm it

Clarifications

- Destroy that disk!
 - Although there are numerous bit wiping products on the market most security experts I polled favored physical destruction in addition to bit wiping
 - Residual magnetism
 - Disk head positioning
 - "If you erase the data by whatever means, you should see a surface devoid of any specific pattern or periodicity," Knotts explained. "Our goal was to see a random distribution of magnetization that would indicate a clean disk." <http://www.gatech.edu/newsroom/release.html?id=1010>

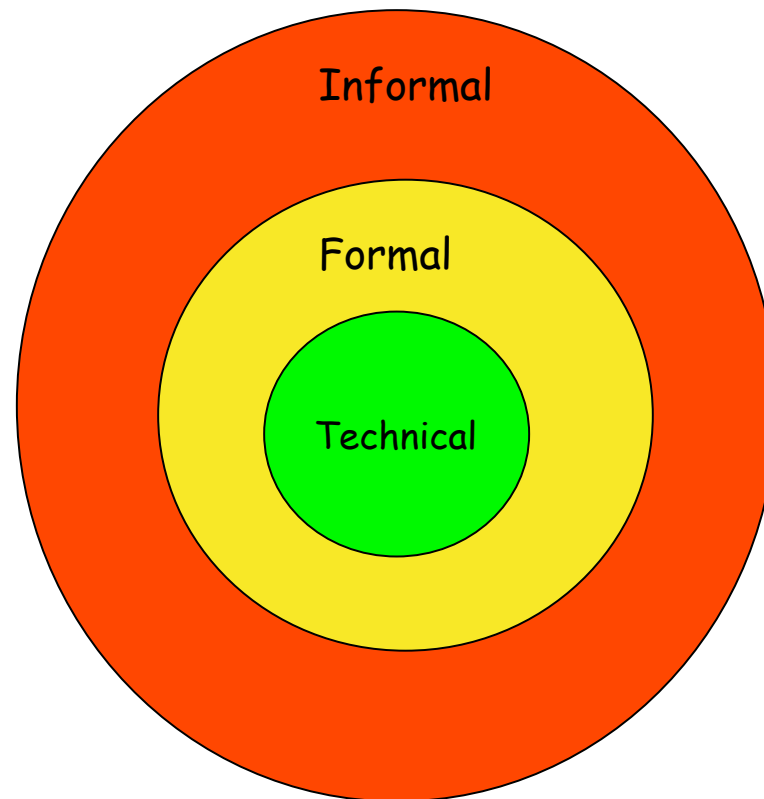
Today's Log

- Employees put their business' security at risk News Article - Wednesday, March 19, 2008 11:34
- Filed under: IT Security & Business Continuity
- Most business computers are at risk from attack due to out-of-date antivirus software and disabled firewalls. New research by security vendor Sophos has shown that two-thirds of business computers are not fully secure, leaving companies open to risk, reports IT Pro. Missing security patches are another reason that businesses are left unprotected.
- John Shaw, group product manager at Sophos, told the computing website: "I suspect these findings are going to be quite shocking to IT managers. "It's a lot to do with how difficult it is for IT managers to keep control of what end users are doing with their computers," he added. IT managers must ensure that end users do not turn off or disable features, or install other software, potentially putting the company at risk. By restricting network access and managing end-point security Sophos says managers can limit the risk, reports the website. A recent report showed that remote workers increase the risk to a company's computer security.
- Yours?



AP- Owen Thor Walker
Walker pleaded guilty last July — when he was 18 — to a raft of charges connected to his work for an international network that the FBI estimated infiltrated 1.3 million computers and skimmed bank accounts or damaged computer systems to the tune of more than \$20 million. Hired by TelestraClear

Coordination in 3's



Home Security Survey Advice

- Remember that I am looking for survey wisdom as much as the survey itself - I hope to make a synthesis available as a product of this course - I will also vet with security experts I know.
- The next slide provides some points to consider

Home Security Audit Pointers

(from CERT)

- If used for work has your network configuration been vetted by corporate security?
- Do you use regularly updated virus protection software?
- Do you use a home firewall?
- Do you have a home "policy" on unknown or suspicious email attachments?
- Do you have a home policy on unknown or new software?
- How do you retire old hardware? (Byers not CERT)
- Are hidden filename extensions disabled?
- Are all applications (browsers, office) and OS kept up to date with patches?
- Do you turn off computer or disconnect when not in use?
- Do you disable Java, JavaScript and ActiveX at some level?
- Do you make regular backups of important files
- Do you have a boot or emergency disk?

These are suggestions - I expect novel extensions!

Software Risk Management

- (much of this adapted from <http://www.eas.asu.edu/~riskmgmt/intro.html> and the SEI)
- Risk is defined as exposure to harm or loss, not only probability but effect as well.
- NOT RISK AVOIDANCE
- The SEI (and others) phases of risk analysis are:
 - Identify
 - Analyze
 - Plan
 - Track
 - Control

C
O
M
M
U
N
I
C
A
T
I
O
N

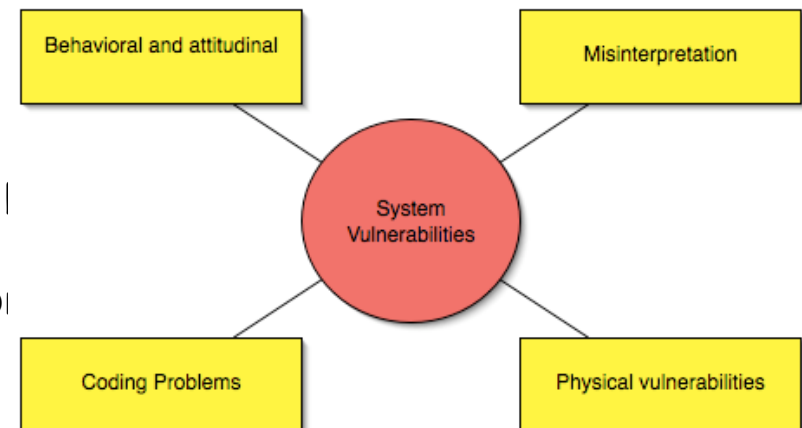
NIST Security Risk Assessment

- System Characterization
- Threat Identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendation
- Results documentation

Risk is a function of the likelihood of a given threat resulting in certain vulnerabilities

Identify Risk

- Risks can be known, unknown and unknowable or known knowns, known unknowns (apply to this project), unknown unknowns :-)!
- SEI method of risk identification (and management) based on following assumptions:
 - Risks are often known by tech staff | poorly communicated
 - A repeatable method is necessary for risk management
 - Must cover all areas
 - Attitude must be non-judgmental and supportive so that controversial views can be heard
 - Success or failure of the project can not be based solely on risk assessment



Analyze Risk

- Probability of risk, USAF Handbook categories are very low, low, medium, high and very high
- Impact of risk, USAF Handbook categories are negligible, marginal, critical and catastrophic
- Risks are rarely independent
- A matrix is used to determine overall risk for different categories (e.g., effort, performance, schedule, cost, support)

Sample Impact/Probability Matrix (used to calculate overall risk)

Impact/Probability	V. High	High	Medium	Low	V. Low
Catastrophic	H	H	M	M	L
Critical	H	H	M	L	0
Marginal	M	M	L	0	0
Negligible	M	L	L	0	0

Plan for the Risks

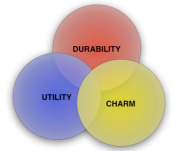
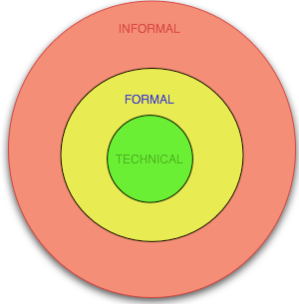
- What can you do:
 - Mitigate impact by developing a contingency plan should risk occur and identify the trigger to initiate the contingency plan
 - Avoid the risk by changing something
 - Accept the risks and the consequences if it occurs, "do nothing"
 - Limit the risk by using controls
 - Transfer the risk, for example purchase insurance
 - Study the risk further so that you can decide on one of the above
- In addition:
 - Specify why risk is important
 - What info is need to track status of risk
 - Who is responsible for Risk Management and what is the cost, by identifying and managing the controls

Risk Control Implementation (NIST)

- Assign priorities to actions, based on level of risk assigned during risk assessment
- Recommended control alternatives are evaluated
- Cost benefit analysis is conducted
- Controls selected based on cost benefit analysis
- Responsibilities are allocated (assigned)
- Safeguard implementation plan is developed
- Controls are implemented and assessment of residual risk is made
- Do this again at frequent intervals or when warranted (my worry beads)

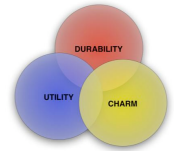
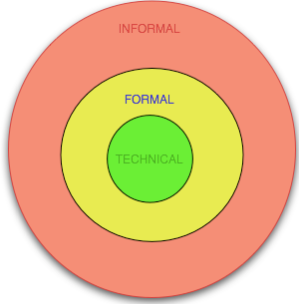
Risk Tracking and Control

- Track like everything else in the project monitoring status of risks and actions taken to address them. Appropriate risk metrics should be in place.
- Control, the risk process should be in place in the beginning, deviations to the plan should be corrected, triggering events should be handled and the process should be assessed for effectiveness.



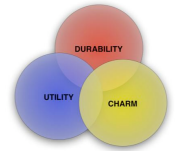
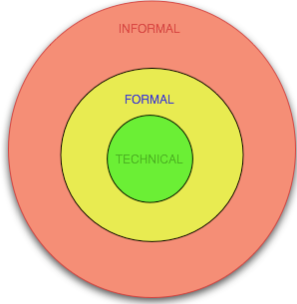
More on Security Controls

- Technical:
 - Supportive: identification, crypto key management
 - Preventive: authentication, authorization, access control enforcement
 - Detection and Recovery: audit, intrusion detection and containment



More on Security Controls - 2

- Formal:
 - Preventive: security responsibility assignment, security plans and policies, security awareness training
 - Detection management controls: personnel controls (background checks, clearances, rotation of duties), audits, **ongoing risk management**
 - Recovery management controls: contingency and disaster recovery plans, incident response capability



More on Security Controls - 3

- Informal:
 - Preventive: security awareness program, security training in both technical and managerial issues, develop a security subculture
 - Detection: informal feedback mechanisms (COMMUNICATION!), reward structures, formal reporting structures \approx informal social groupings
 - Recovery: ownership of activities, encourage stewardship

References

- <http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf>
- S. Singh, The Code Book, Doubleday, 1999, ISBN 0-385-49531-5