Managing Security
Perspective of the Business Executive

Eric Hartwell

Department of Electrical Engineering & Computer Science
EECS 711 Chapter 1 Paper Presentation

eah@kc.rr.com
Managing Security

Abstract

Business executives typically do not understand the details regarding IT services and equipment, so when it comes down to the security aspects of these systems, most are clueless. This presentation looks at IT security from the perspective of a non-technical executive manager. The key here is to not look the the low-level details, but to understand the general security functions so that an executive can understand how it pertains to the operations of the business. The three key areas to look at are how to balance security and productivity, employing the extended risk analysis model to show threats and vulnerabilities, and using the CIA model for alternatives.
Managing Security

Outline

• Introduction
• Security vs. Productivity
• Extended Risk Analysis
• CIA Model
• Summary
• Conclusion
Managing Security

Introduction

• Introduction
• Security vs. Productivity
• Extended Risk Analysis
• CIA Model
• Summary
• Conclusion
Managing Security

Introduction

• It’s true—most executives don’t know IT specifics
• “It is more important to know the questions to ask than the answer to those questions”
• The role of IT personnel is to answer security questions and to implement solutions
• Finding balance between security & productivity
• Find risk from vulnerabilities and threats
• CIA model used to identify security control function
Managing Security

Introduction

- Introduction
- Security vs. Productivity
- Extended Risk Analysis
- CIA Model
- Summary
- Conclusion
Managing Security

Security vs. Productivity

- Do losses outweigh cost of security?
  - Remember, security isn’t free
  - Increases cost of operations, but doesn’t increase revenue
  - A security system should cost less than losses prevented

- Privacy is also important
  - It can’t be achieved without security

- Legal requirements
  - GLB, HIPAA, SOX
Managing Security

Security vs. Productivity

• Security and productivity should be balanced
  – Security increase = productivity decrease
  – Security decrease = productivity increase (initially)

• Less security = greater chance of negative activity
  – Risk is management’s responsibility to weigh appropriately

• Don’t be deceived by “positives” from lower security!
  – Productivity plummets once a significant breach occurs
  – Not to mention reputation, trust; trade secrets, liability
  – Losses can easily exceed costs of security solutions
Managing Security

Security vs. Productivity

- Security can be too strict...
  - Employees may not be able to access equipment or data
  - Expenses may not be justified
  - Some employees may attempt to circumvent
    - Expensive, difficult to use, and compromised

- Management should look to two teams
  - Security personal for technical detail
  - Function/process area managers
Managing Security

Security vs. Productivity

• Security personnel likely to increase security to max
  – The infrastructure belongs to the organization, but...
  – Security admin likely views as a reflection of competence
    o When network is attacked, it’s personal
    o Not rewarded for repelling; responsible for attack if it happens
  – Creates bias that will likely result in productivity loss

• Function managers evaluated on productivity
  – Reject anything that causes inefficiencies
    o Even if it is beneficial long-term!

• Security manager paradox: a useable network is insecure, a secure network is unusable
Managing Security
Extended Risk Analysis

- Introduction
- Security vs. Productivity
- Extended Risk Analysis
- CIA Model
- Summary
- Conclusion
Managing Security
Extended Risk Analysis

- Risk is the probability of an adverse event occurring
  - Interaction between threats and vulnerabilities
- Threats exist outside; little control over these
- Vulnerabilities result from choices
  - Example: threat of hurricane in FL, locate elsewhere
- Some threats can be controlled
  - If vulnerable to theft, conduct background checks
  - Most threat counters rely on external entities
Managing Security
Extended Risk Analysis

• The manager must determine vulnerabilities
  – Organization can choose features implemented or location

• Threat with no vulnerabilities means no risk
  – Example: hacker attacks network not connected to Internet

• Two options once risk is determined...
  – Make attack difficult through controls
    o Lowering probability of successful attack
  – Transfer economic consequences to external entity
Managing Security
Extended Risk Analysis

• Controls are put into place to deter attacks and/or limit damage when adverse affects occur
  – Deter by making things more difficult
  – Deflect by making another target attractive
  – Detect immediately or soon after

• Controls are technical
  – Need competent personnel to install or implement
  – If not done right, it could be worse than no controls

• Best for high frequency attacks
Managing Security
Extended Risk Analysis

- Market insurance is for transferring adverse consequences to other entity for a premium
  - Insurance traditionally for accidents or disasters, but is plenty viable for risk
- It obviously does not change the probability of attack
- Best used for rare, high economic impact situations
- Cost of controls and insurance should not be more than the expected loss resulting from said risk
Managing Security
Extended Risk Analysis

- It is almost impossible to remove all risk
  - Remaining portion is residual risk
  - When risk declines, costs of further risk reduction can soar
- The goal is to get to a point when it is not economically practical to continue reducing
- At some point it is likely that some attack will be successful
  - Establishing a recovery plan is essential for these situations
Managing Security
Extended Risk Analysis

Figure 1: Extended Risk Analysis Model [Reid 2007]
Managing Security

CIA Model

- Introduction
- Security vs. Productivity
- Extended Risk Analysis
- CIA Model
- Summary
- Conclusion
Managing Security

CIA Model

- Once risks have been identified, a manager must be able to manage these risks
- The CIA model can be used as a model
  - Confidentiality: ensures information on a need-to-know basis and that unauthorized access is prevented
  - Integrity: ensures that data is not deleted for corrupted either accidentally or deliberately
  - Availability: ensures that information is available when it is required and that it will supported the organization’s ability to operated and accomplish its objectives
Managing Security

CIA Model

• Confidentiality doesn’t stop at electronic access
  – Physical information should also be safeguarded
• Integrity can be extended to reliability of people, procedures, and networks
  – Measure of trust you have in a system or function
• Availability includes status of equipment, available support, and anything else preventing a user from accessing data they should be able to access
Managing Security
CIA Model

- The triangle is designed to help a manager visualize the trade-offs between the three points
  - Manager should focus on desired functions and not the technical details
- When a manager signs off on what they want to see percentage wise, security personnel can figure out the technical implementation
- Different technology implementations will result in trade-offs between the three points
Managing Security

CIA Model

Figure 2: CIA Triangle with Security Technologies [Reid 2007]
Managing Security

Summary

- Introduction
- Security vs. Productivity
- Extended Risk Analysis
- CIA Model
- Summary
- Conclusion
Managing Security

Summary

• It is imperative to find the appropriate balance between security and productivity

• Extended Risk Analysis is very helpful in determining the risk from threats/vulnerabilities and what steps to take until the risks are acceptable

• The CIA model is useful for visualizing where the organization should be and what technologies the security personnel should implement
Managing Security

Conclusion

• Introduction
• Security vs. Productivity
• Extended Risk Analysis
• CIA Model
• Summary
• Conclusion
Managing Security

Conclusion

• Securing assets can be very challenging, but it is extremely important for an organization
• Even though threats are generally outside the control of managers, they still have control over location, tools used, and functionality implemented
• Risk is manageable via controls and/or insurance
• Secure the organization while allowing users to do what they need to do
• CIA triangle helps bridge the gap between non-technical managers and IT security staff
Reference

Questions?