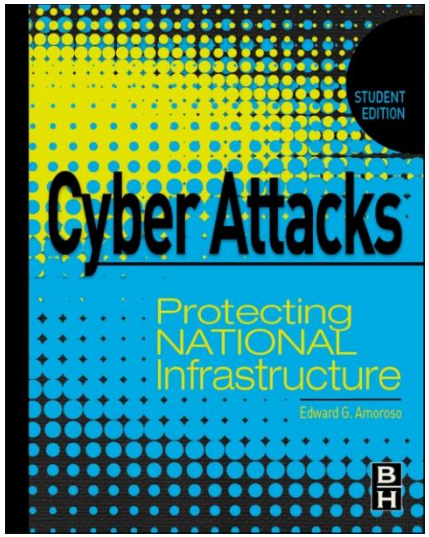


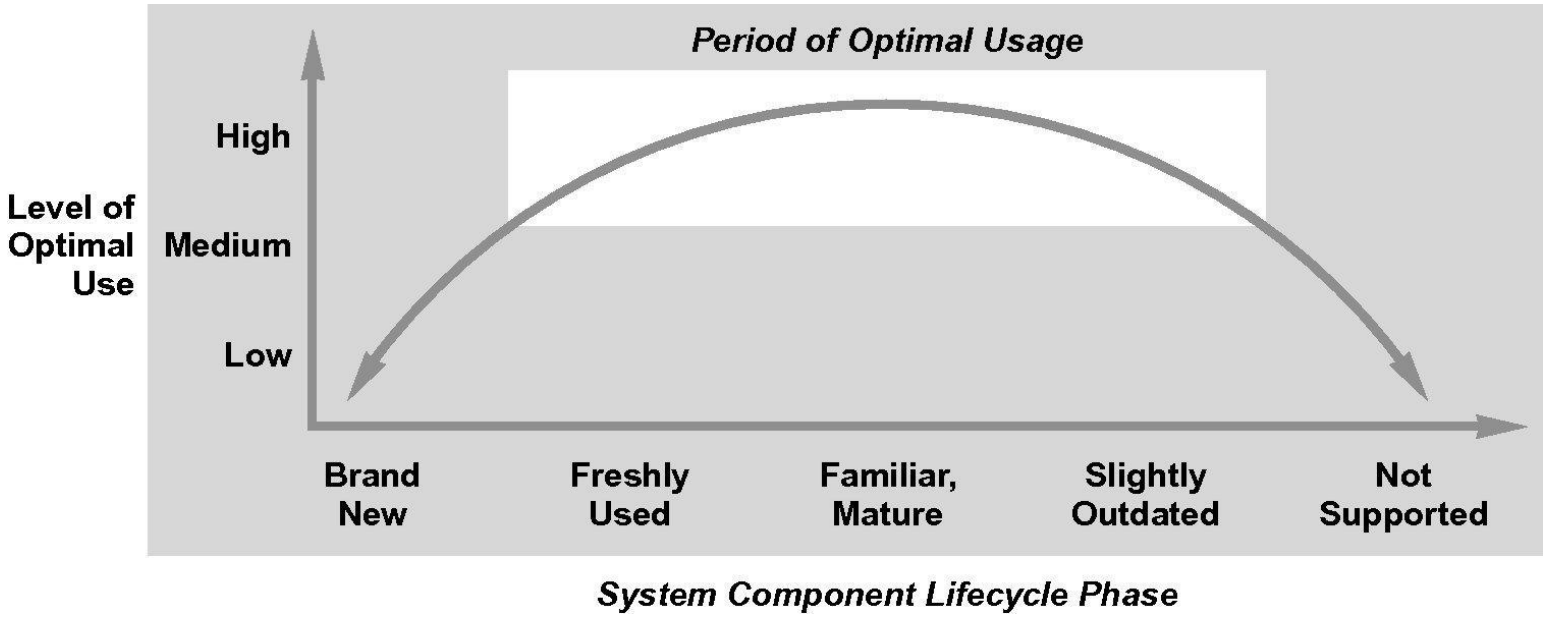
Chapter 10

Awareness

Introduction

- *Situational awareness* is the real-time understanding within an organization of its security risk posture
- Awareness of security posture requires consideration of the following
  - Known vulnerabilities
  - Security infrastructure
  - Network and computing architecture
  - Business environment
  - Global threats
  - Hardware and software profiles

Fig. 10.1 – Optimal period of system usage for cyber security



Introduction

- Factoring in all elements of situational awareness should create an overview of current security risk
- Descriptors such as *high, medium,* and *low* are too vague to be helpful
- Security risk levels should be linked with actionable items

Fig. 10.2 – Rough dashboard estimate of cyber security posture

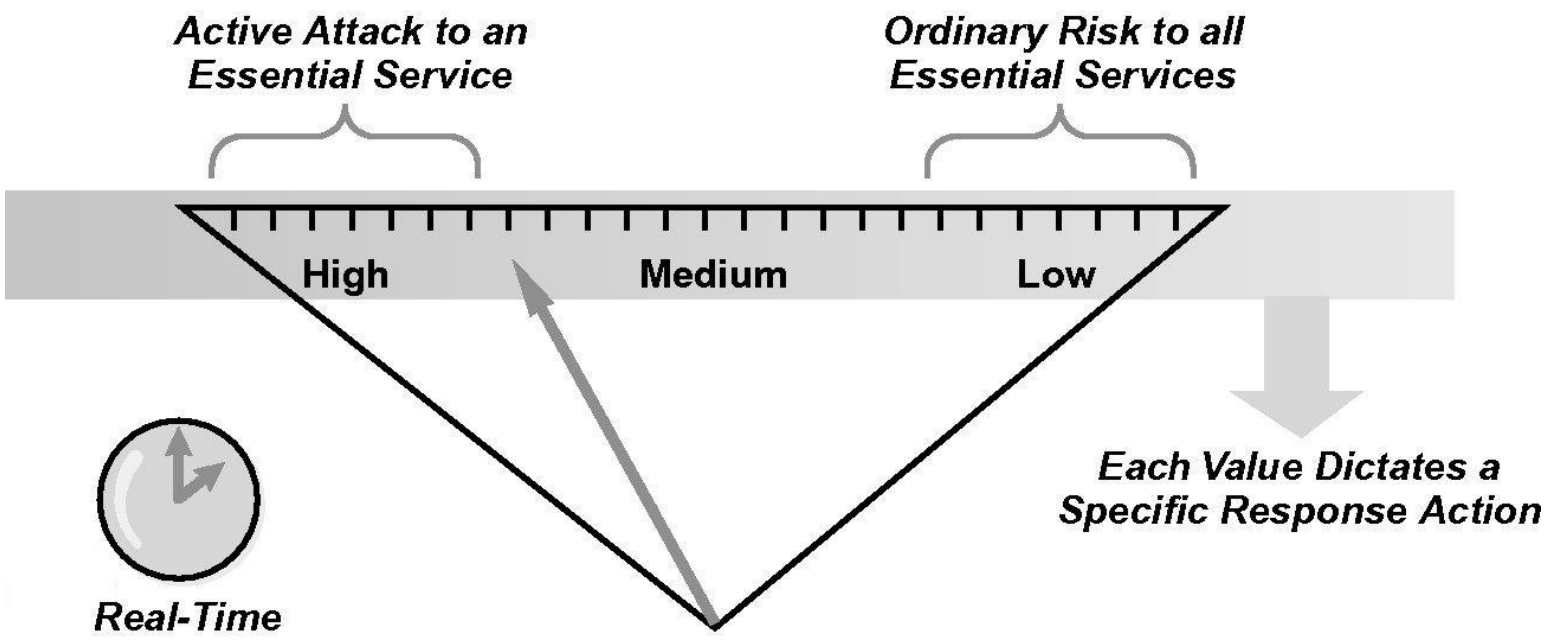
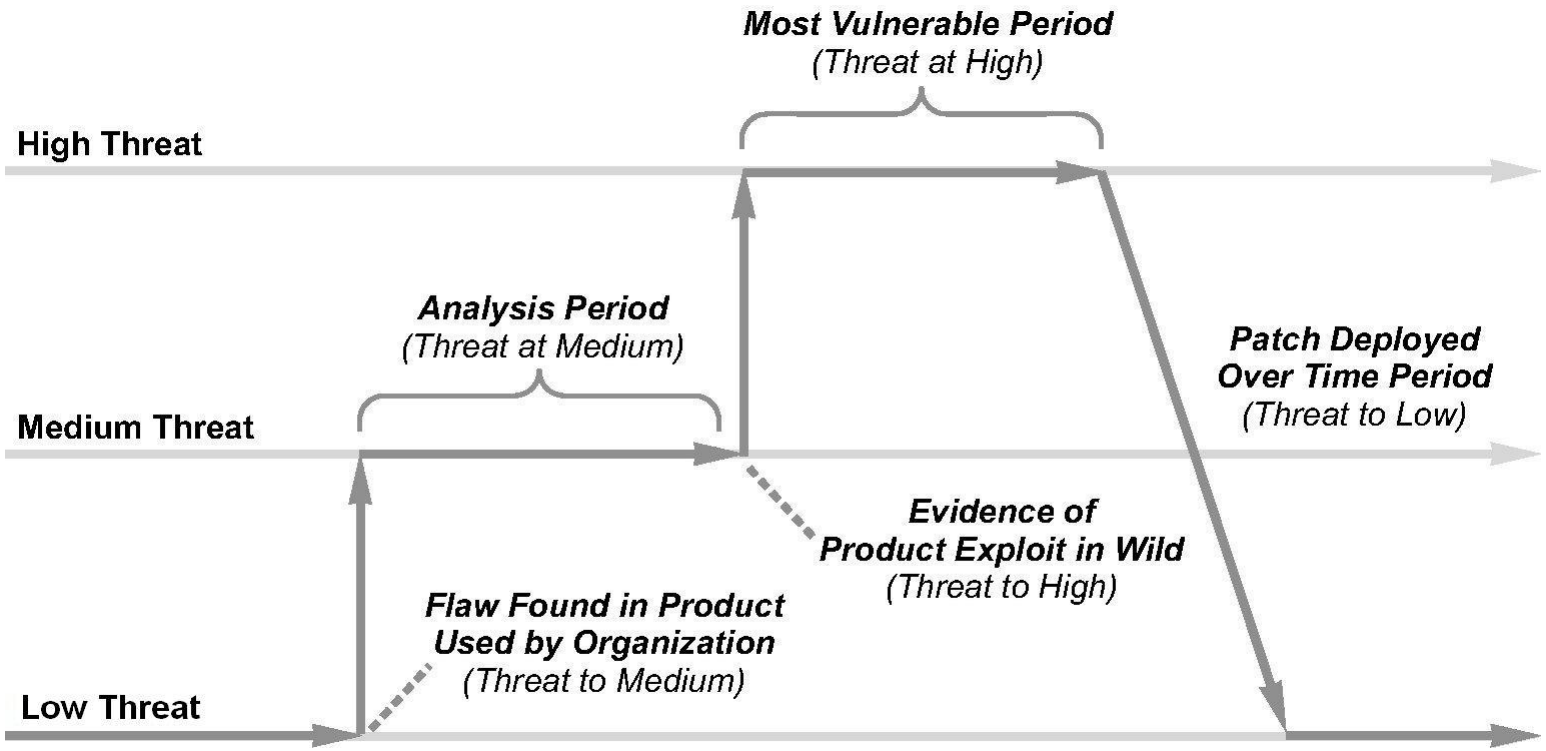


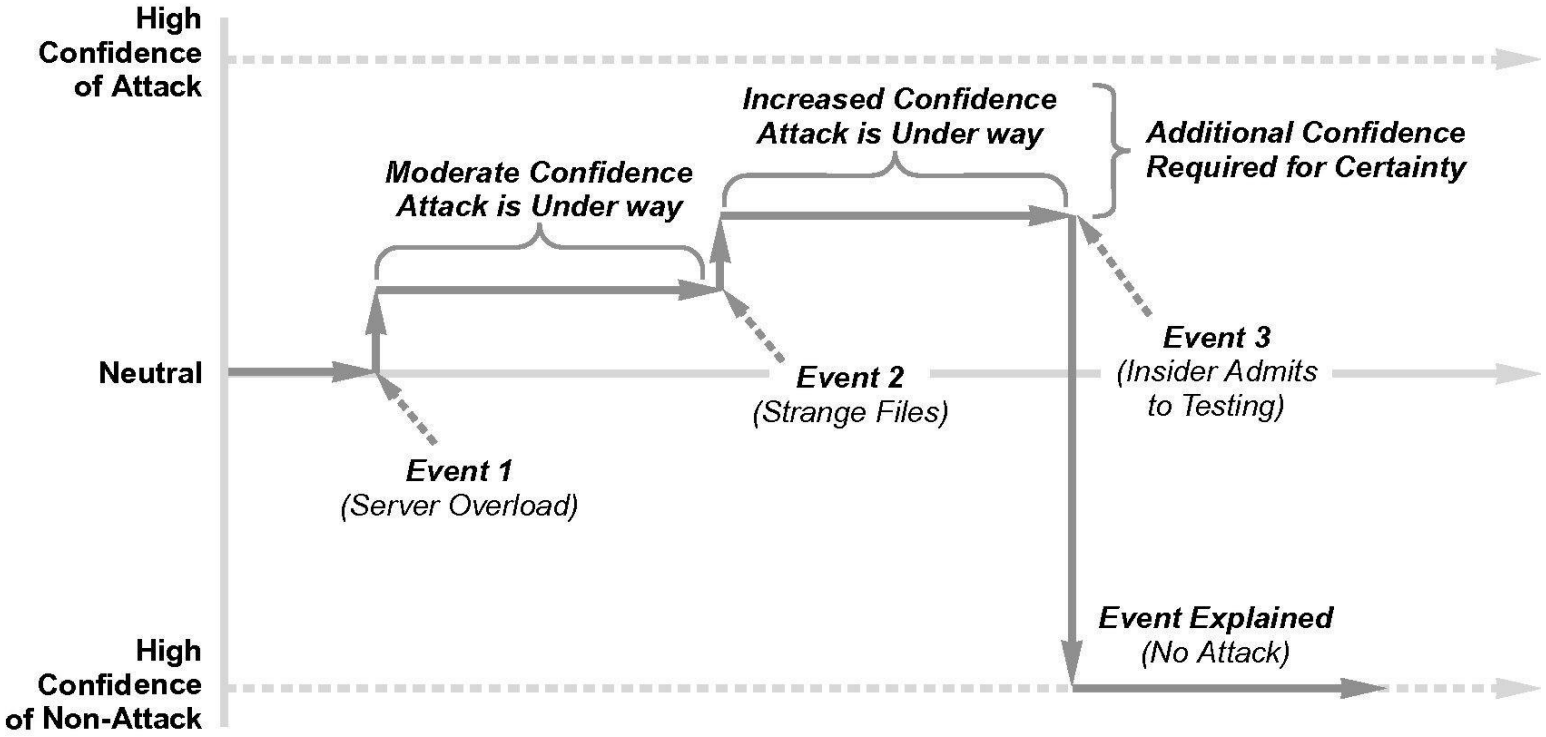
Fig. 10.3 – Security posture changes based on activity and response



Detecting Infrastructure Attacks

- No security task is more difficult and complex than the detection of an ongoing attack
- Many tools for detecting attack, yet none comprehensive or foolproof
- Determination of risk level is a fluid process

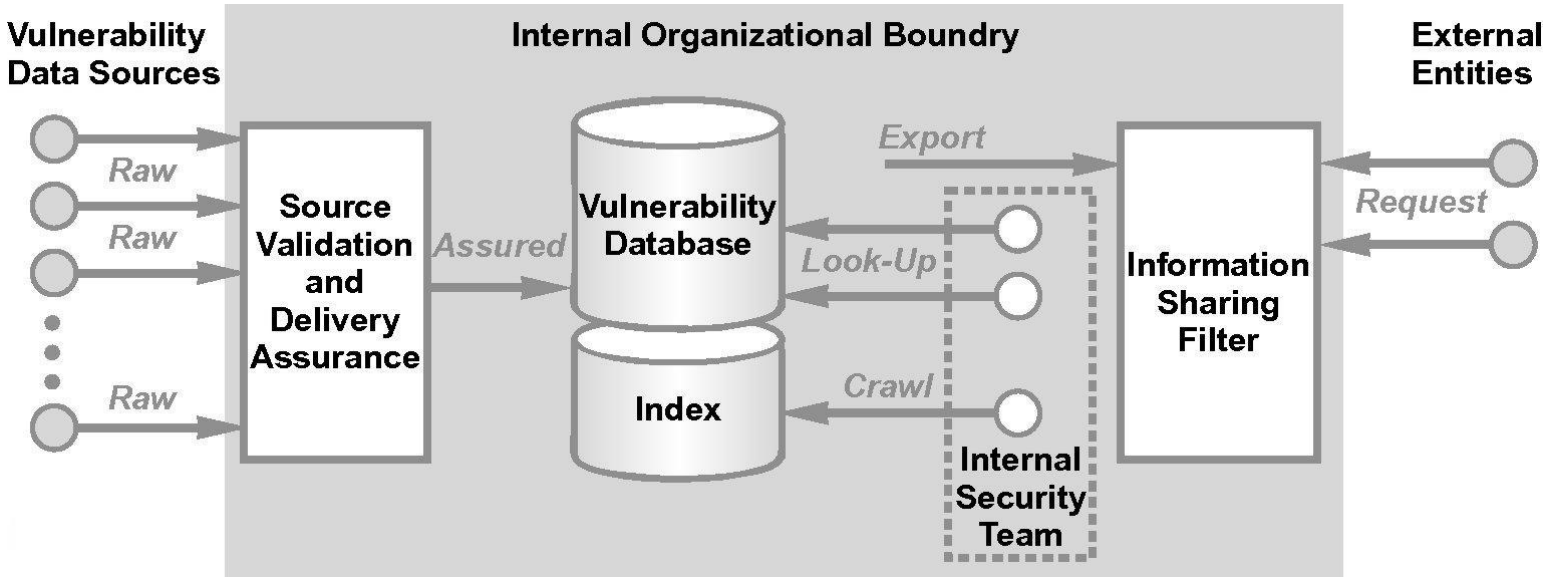
Fig. 10.4 – Attack confidence changes based on events



Managing Vulnerability Information

- Situational awareness for national infrastructure protection requires a degree of attention to daily trivia around vulnerability information
- Practical heuristics for managing vulnerability information
  - Structured collection
  - Worst case assumptions
  - Nondefinitive conclusions
  - Connection to all sources

Fig. 10.5 – Vulnerability management structure



Managing Vulnerability Information

- Three basic rules for managers
  - Always assume adversary knows as much or more about your infrastructure
  - Assume the adversary is always keeping vulnerability-related secrets from you
  - Never assume you know everything relevant to the security of your infrastructure

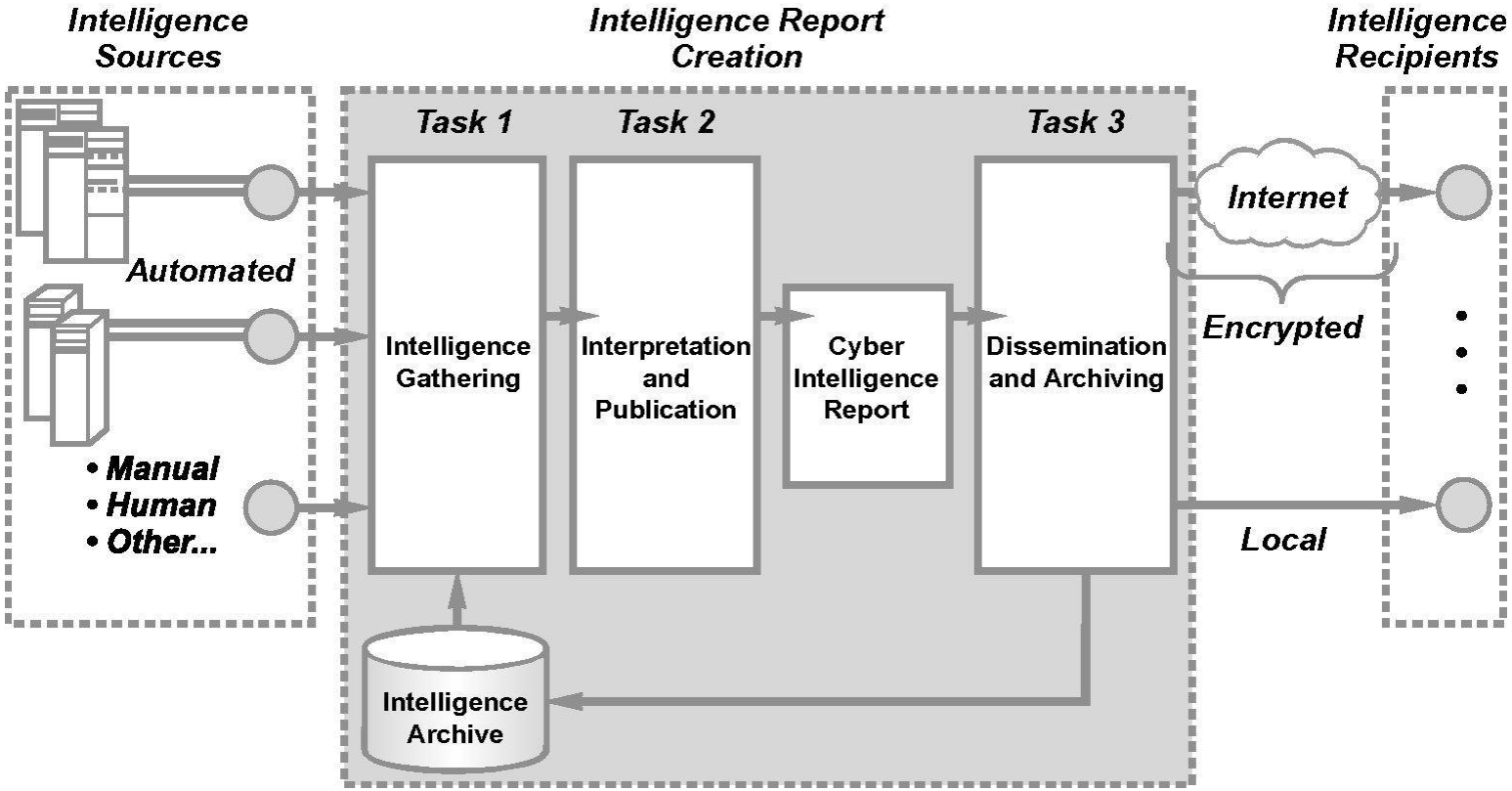
Cyber Security Intelligence Reports

- Daily cyber security intelligence reports are standard in government agencies
- They would be useful in enterprise settings
- A cyber security intelligence report would include
  - Current security posture
  - Top and new security risks
  - Automated metrics
  - Human interpretation

Cyber Security Intelligence Reports

- Tasks for creating a cyber security intelligence report
  - Intelligence gathering
  - Interpretation and publication
  - Dissemination and archiving

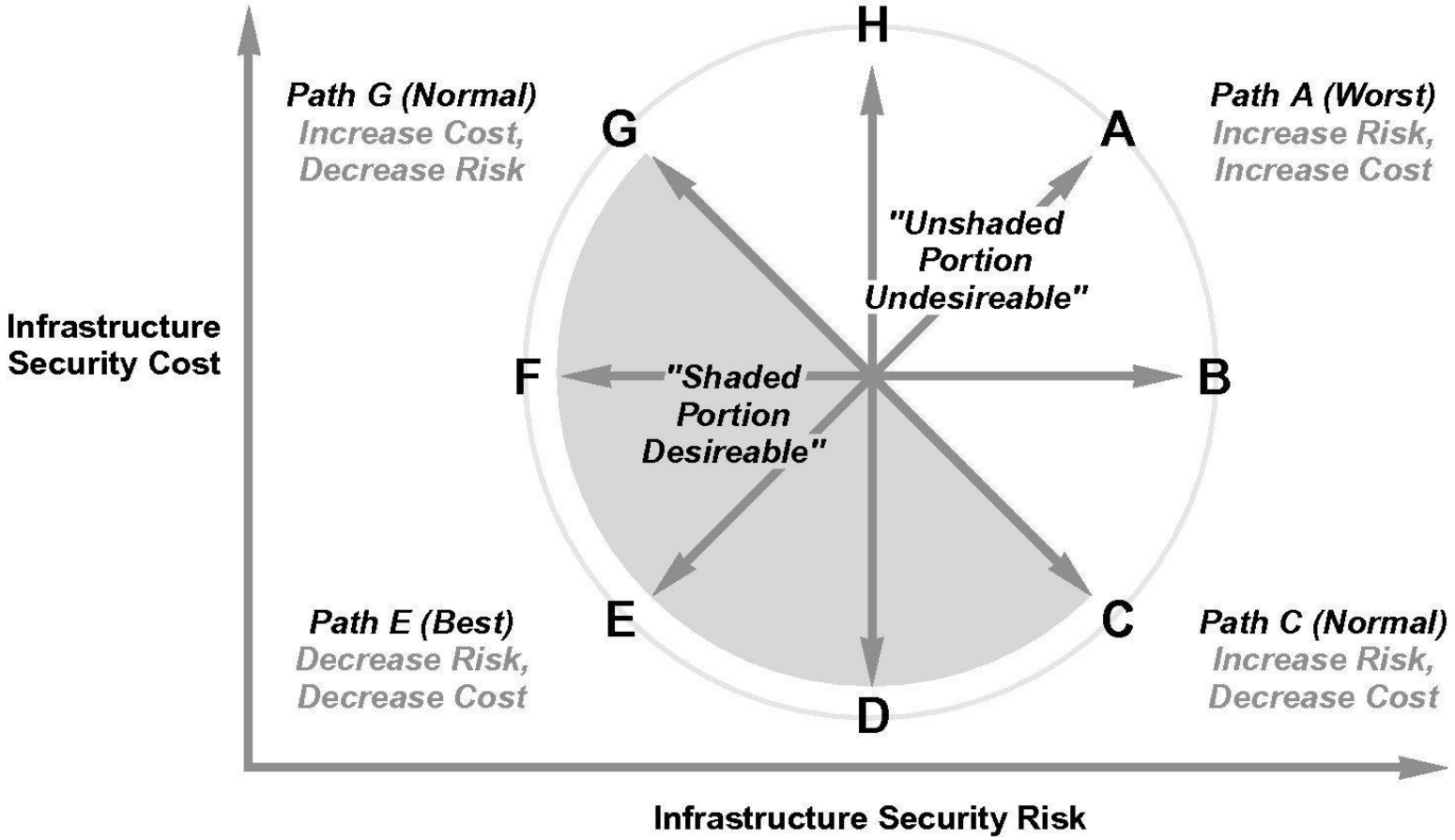
Fig. 10.6 – Cyber security intelligence report creation and dissemination



Risk Management Process

- Security risks must be tracked and prioritized
- Generally agreed upon approach to measuring risk associated with specific components begins with two estimations
  - Liklihood
  - Consequences
- Actual numeric value of risk less important than overall relative risk
- A useful construct compares security risk against cost of recommended action

Fig. 10.7 – Risk versus cost decision path structure



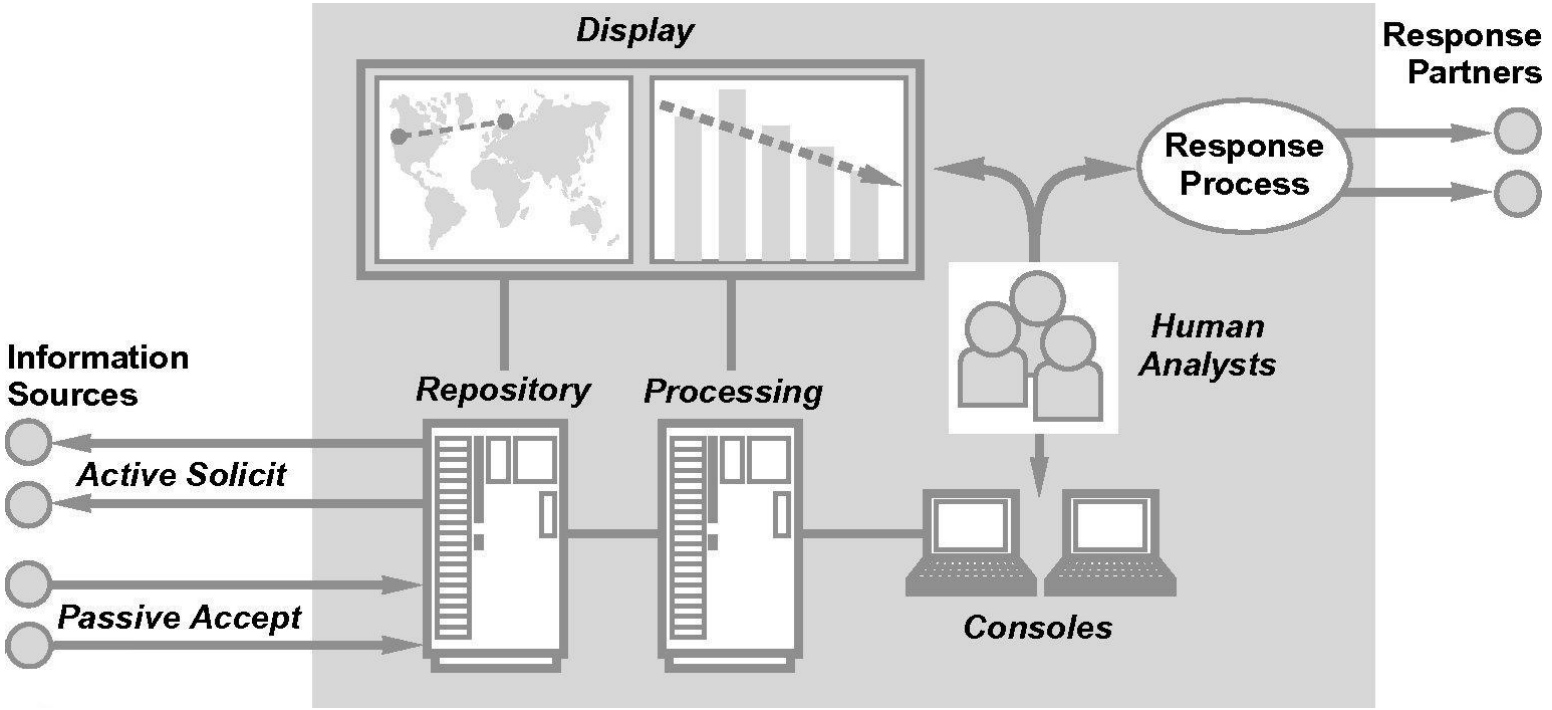
Risk Management Process

- Increasing risks likely incur increased costs
- Summary of management considerations
  - Maintaining a prioritized list of security risks
  - Justifying all decisions

Security Operations Centers

- The *security operations center* (SOC) is the most visible realization of real-time security situational awareness
- Most SOC designs begin with centralized model – a facility tied closely to operation
- A global dispersal of SOC resources is an around-the-clock real-time analysis of security threats

Fig. 10.8 – Security operations center (SOC) high-level design



National Awareness Program

- A national-level view of security posture will require consideration of the following
  - Commercial versus government information
  - Information classification
  - Agency politics
  - SOC responsibility