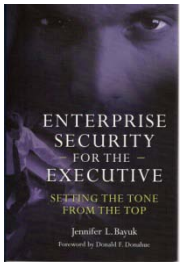
System-Level Security

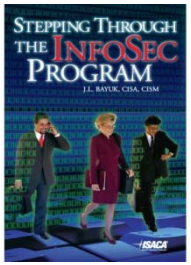
For CFI-CERT

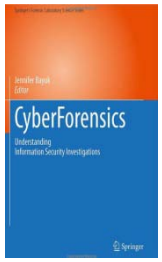
By:

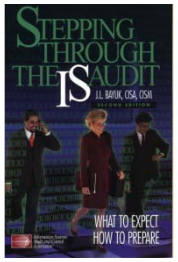
Jennifer Bayuk

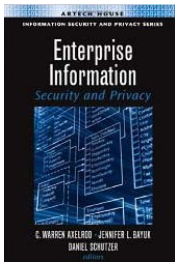
Jennifer Bayuk



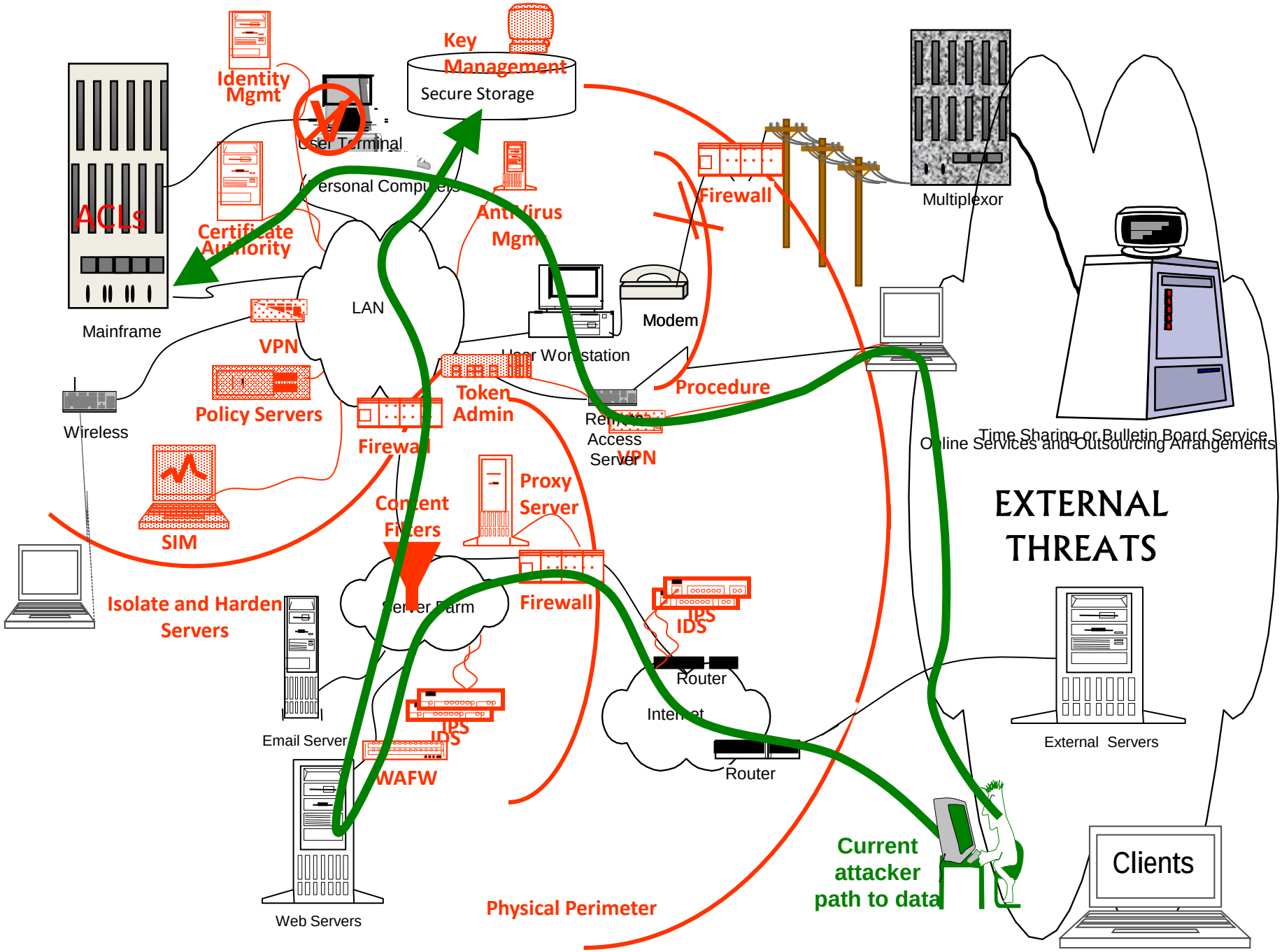


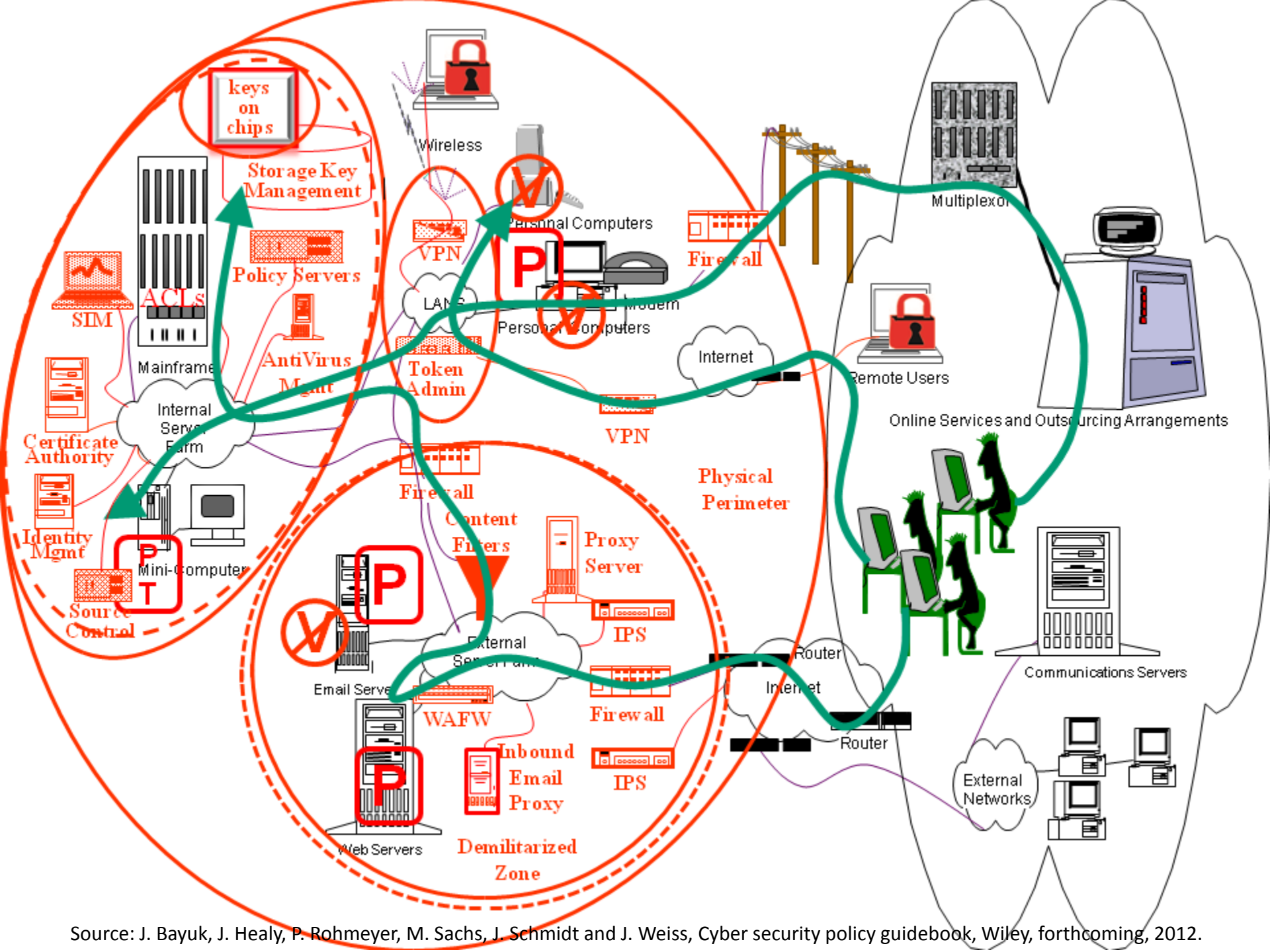






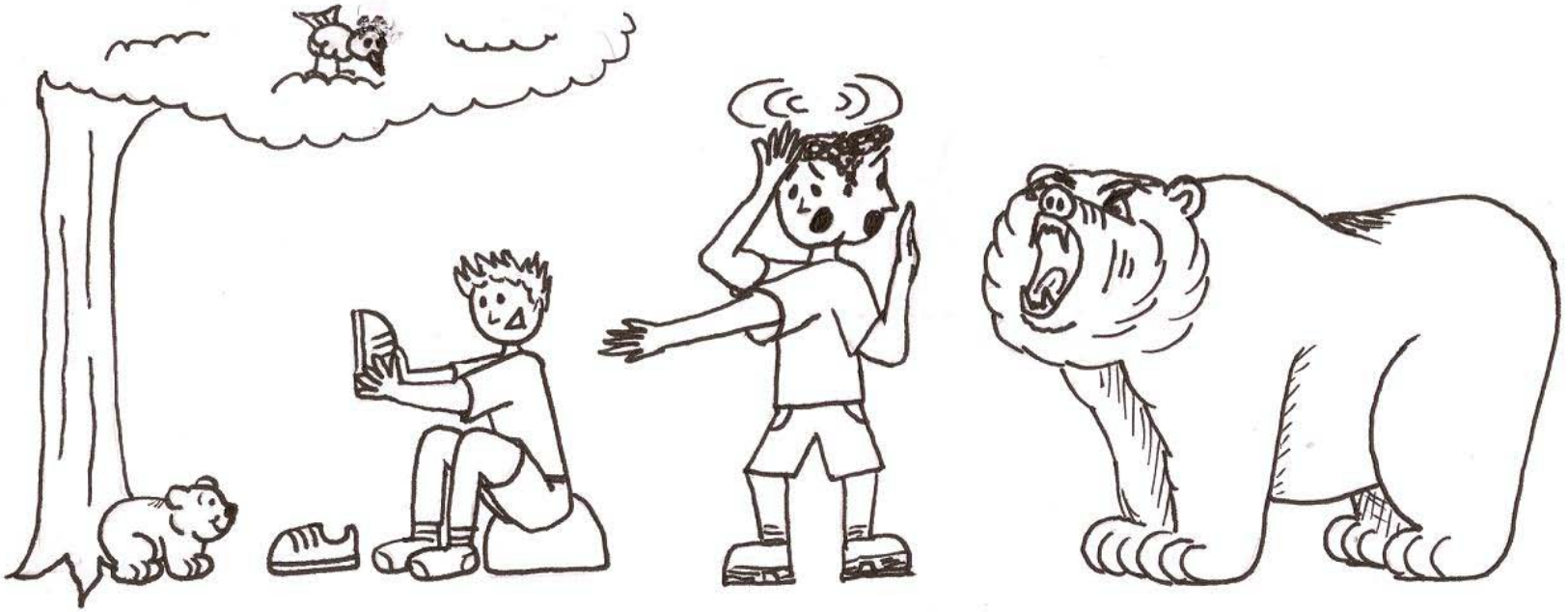
- Independent consultant experienced in a wide variety of private security positions including Chief Information Security Officer.
- Created Systems Security Curriculum for Stevens Institute of Technology
- Author of multiple textbooks on security management topics
- Chair and contributor to multiple public and private InfoSec Boards and Committees
- Systems Engineering PhD, Thesis in Security Metrics


Identity Mgmt
Key Management
Secure Storage
User Terminal
Personal Computers
Anti Virus Mgmt
Certificate Authority
ACLs
Mainframe
LAN
Firewall
Multiplexor
Modem
User Workstation
VPN
Policy Servers
Token Admin
Wireless
Firewall
Remote Access Server
VPN
Procedure
Time Sharing or Bulletin Board Service
Online Services and Outsourcing Arrangements
SIM
Content Filters
Proxy Server
EXTERNAL THREATS
Isolate and Harden Servers
Server Farm
Firewall
IDS
Router
Internet
Email Server
IDS
WAFW
Router
External Servers
Current attacker path to data
Clients
Web Servers
Physical Perimeter



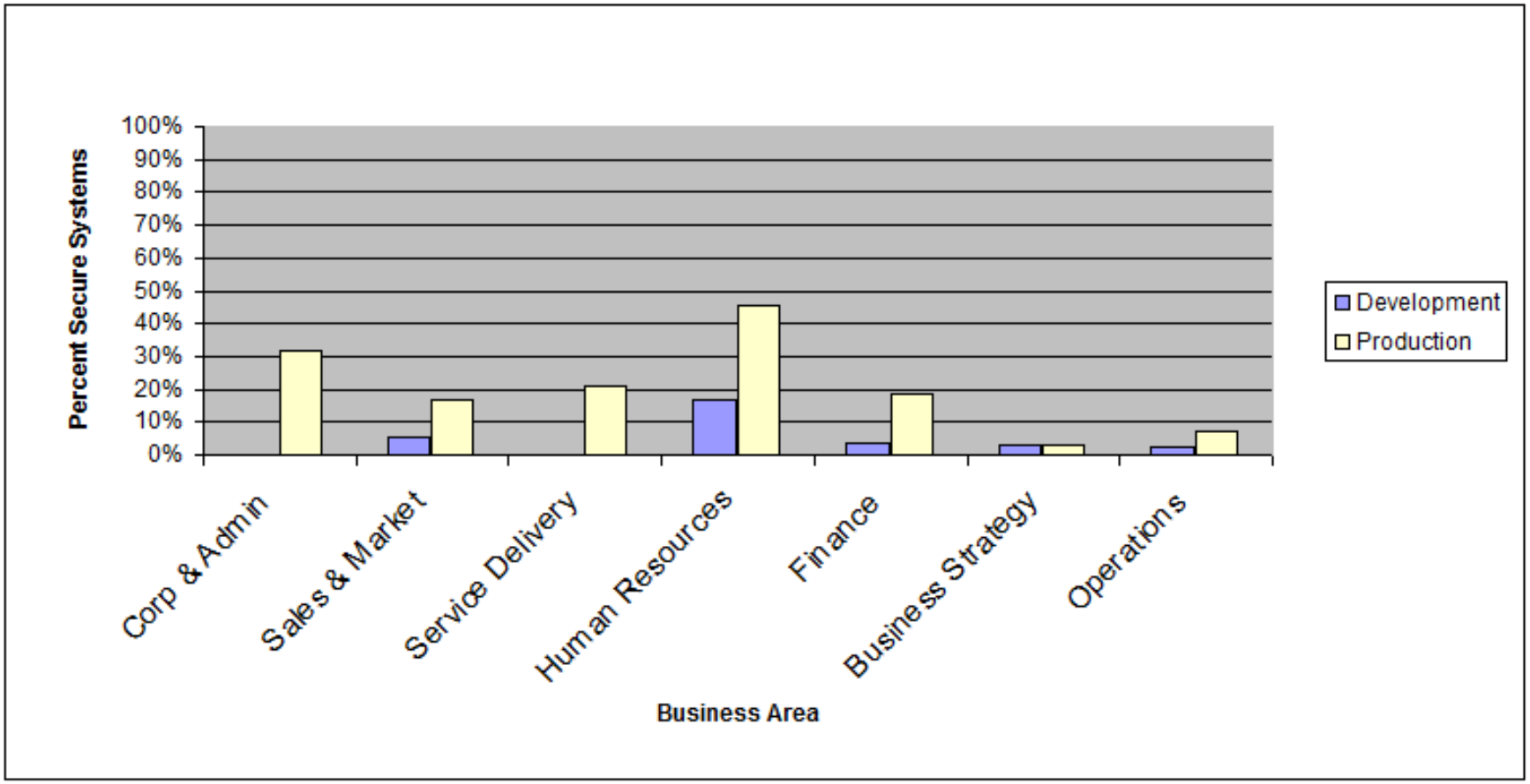
Source: J. Bayuk, J. Healy, P. Rohmeyer, M. Sachs, J. Schmidt and J. Weiss, Cyber security policy guidebook, Wiley, forthcoming, 2012.

Bear Analogy



Source: Bayuk, Jennifer, *Enterprise Security for the Executive, Setting the Tone from the Top*, Praeger, Fall 2009
http://www.praeger.com/catalog/C37660.aspx

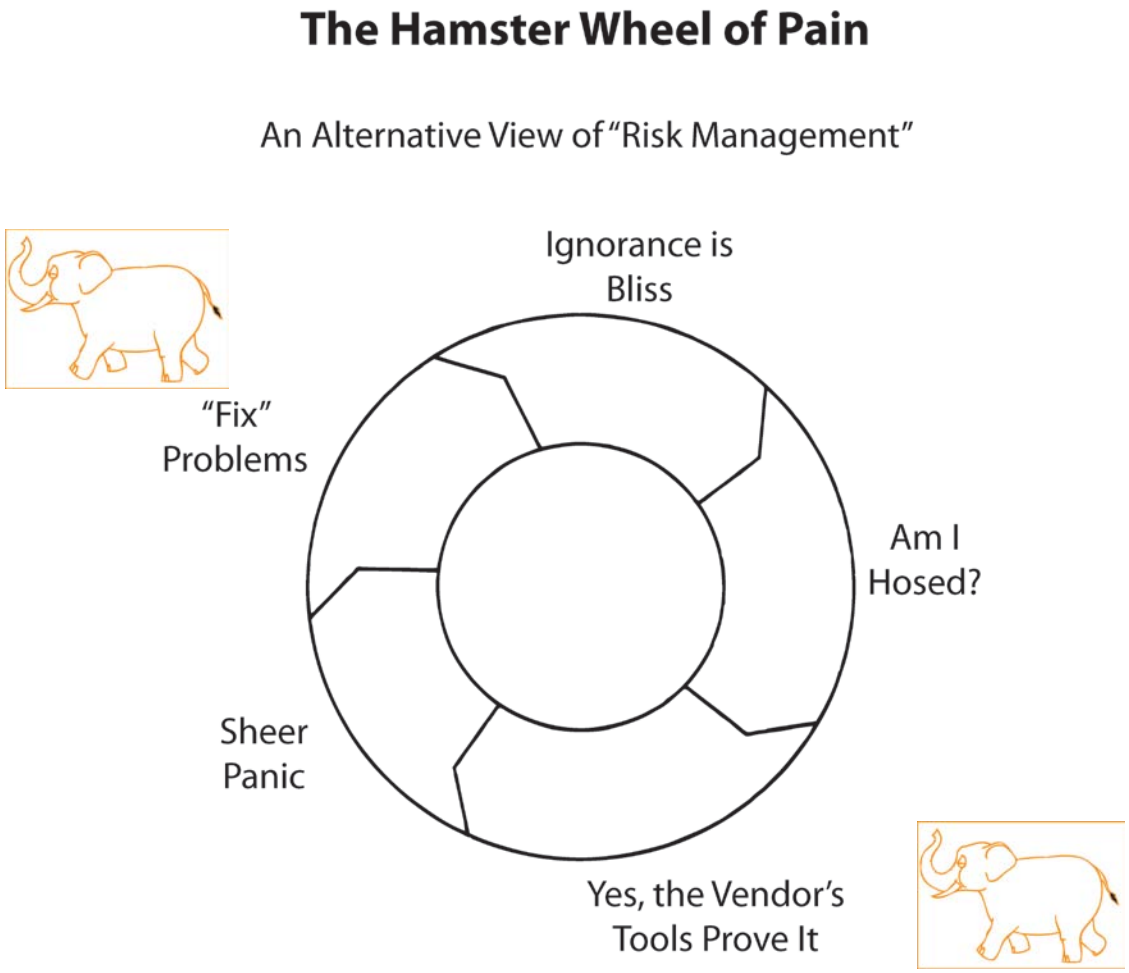
Example Excerpt from Scare Deck



Security Horror Stories

- tales of organizations that did not pay attention to security, and thus fell victim to some criminal, who exploited an obvious vulnerability to steal or destroy something so valuable that the company had to disclose its inadequacy
- variations on the definition replace the criminal with an auditor
- designed to produce fear, uncertainty, and doubt
- by definition *preventable*

How *not* to judge the value of security



Source: Jaquith, Andrew, Security Metrics, Pearson Education, 2007.

Typical Cost Justification

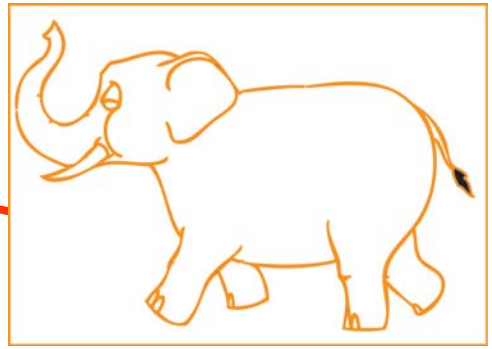
1. P = probability of event that causes harm

   C = cost of damage from the event

   T = cost of technology to prevent harm

2. P x C = amount it is reasonable to spend to prevent the event

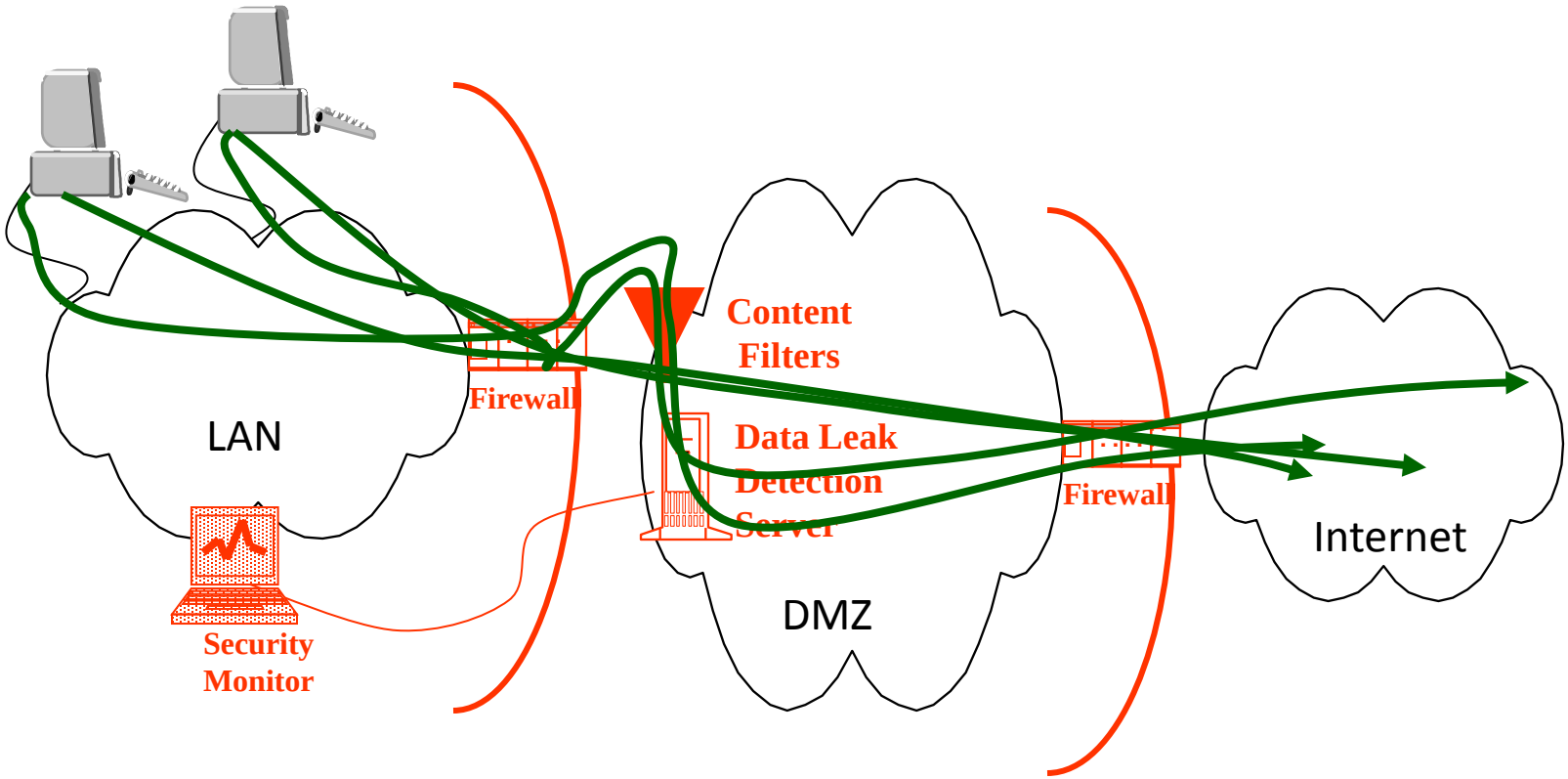
3. If (T < P x C), Buy T



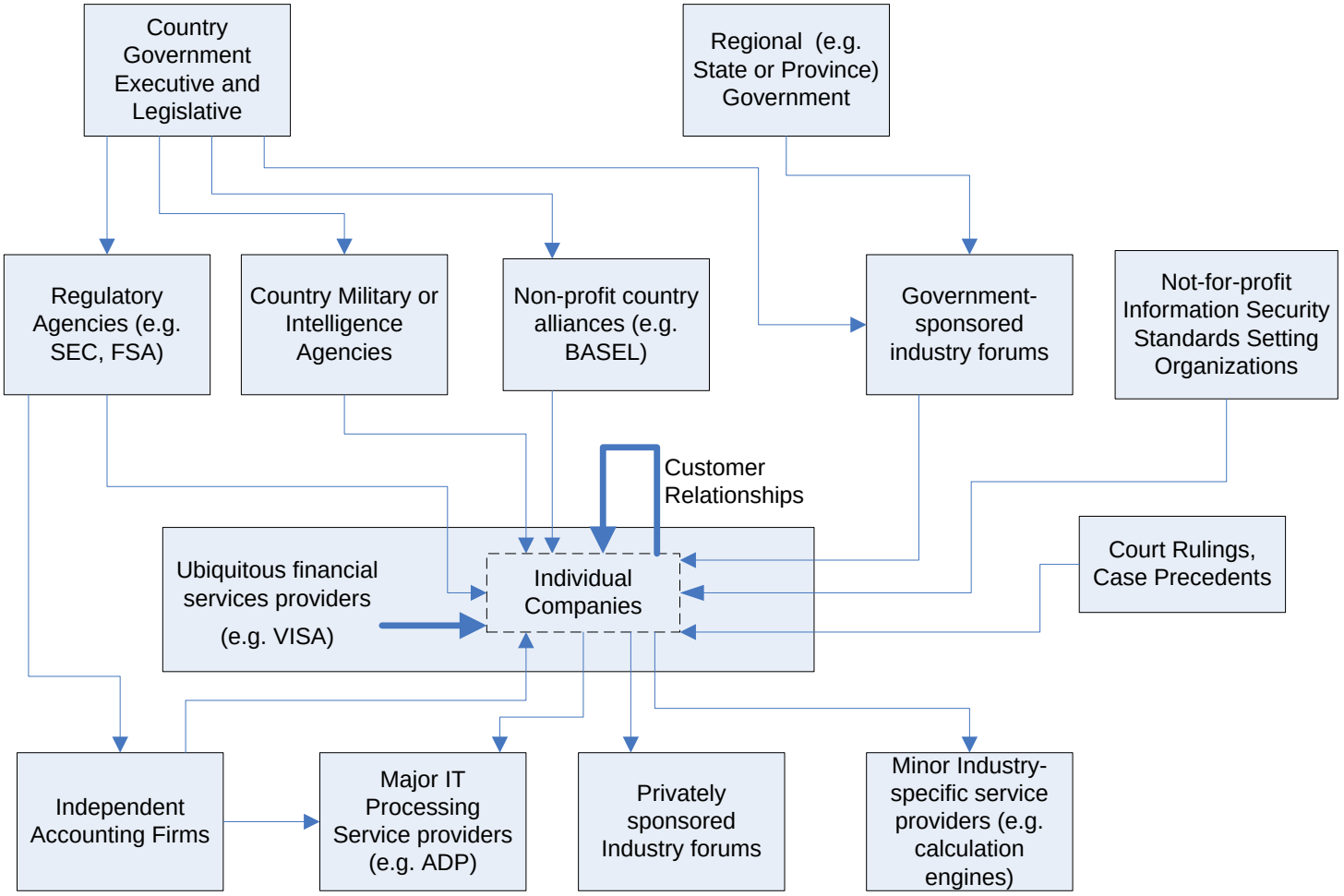
CXOs are….

- the highest ranking manager with sole responsibility for risk-based decisions within some domain
- generally comfortable with risk
- ***assumed to make decisions based on FUD?***

Example Security Project



Enterprise Security Influences



Source: C. Warren Axelrod, Jennifer Bayuk, and Daniel Schutzer, Editors, Enterprise Information Security and Privacy, Artech House, 2009

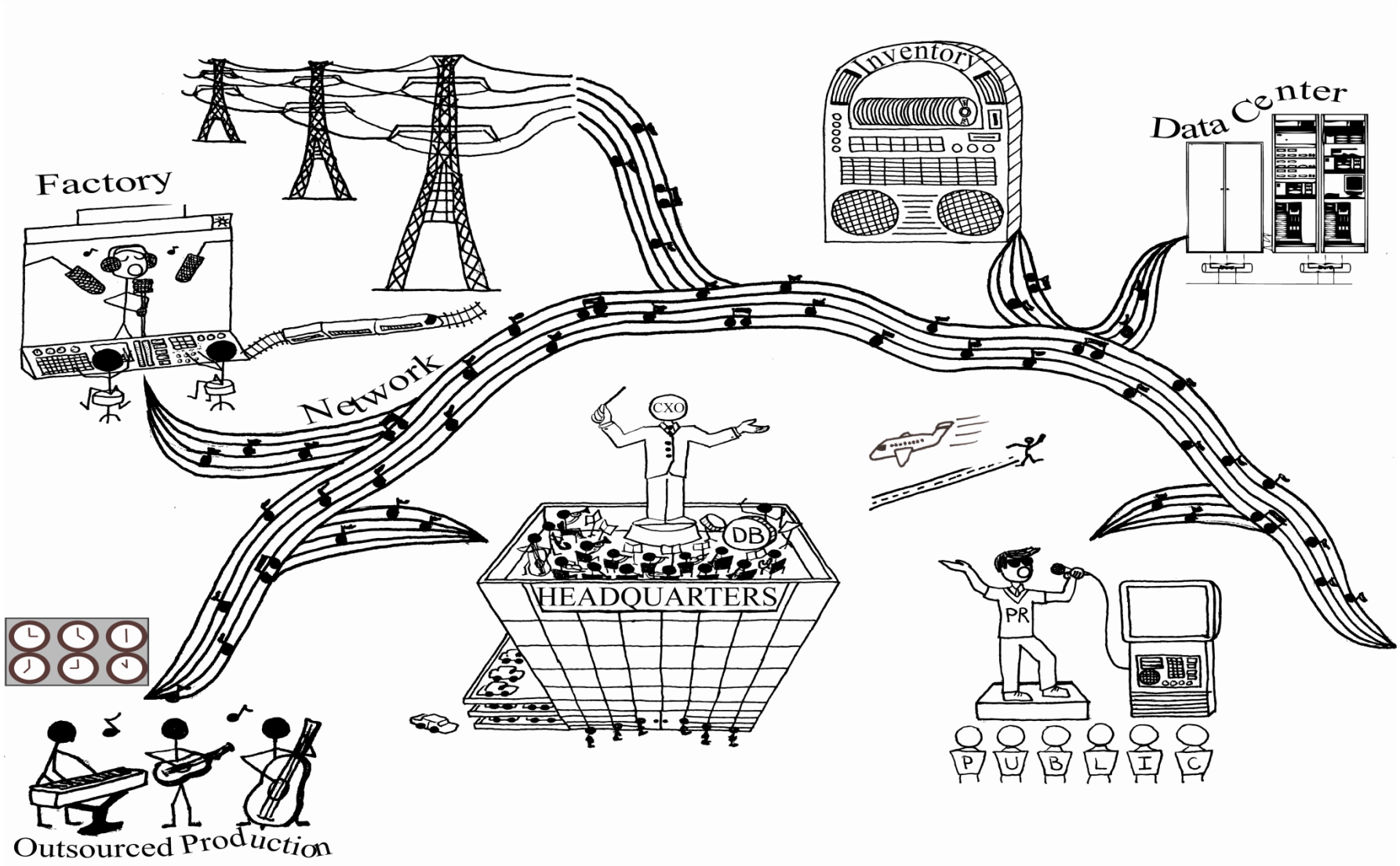
A CXO is like a Pilot

- CXOs are comfortable at the helm
  - Rulebooks provide comfort level for safe decisions
  - Risk Managers provide checkpoints

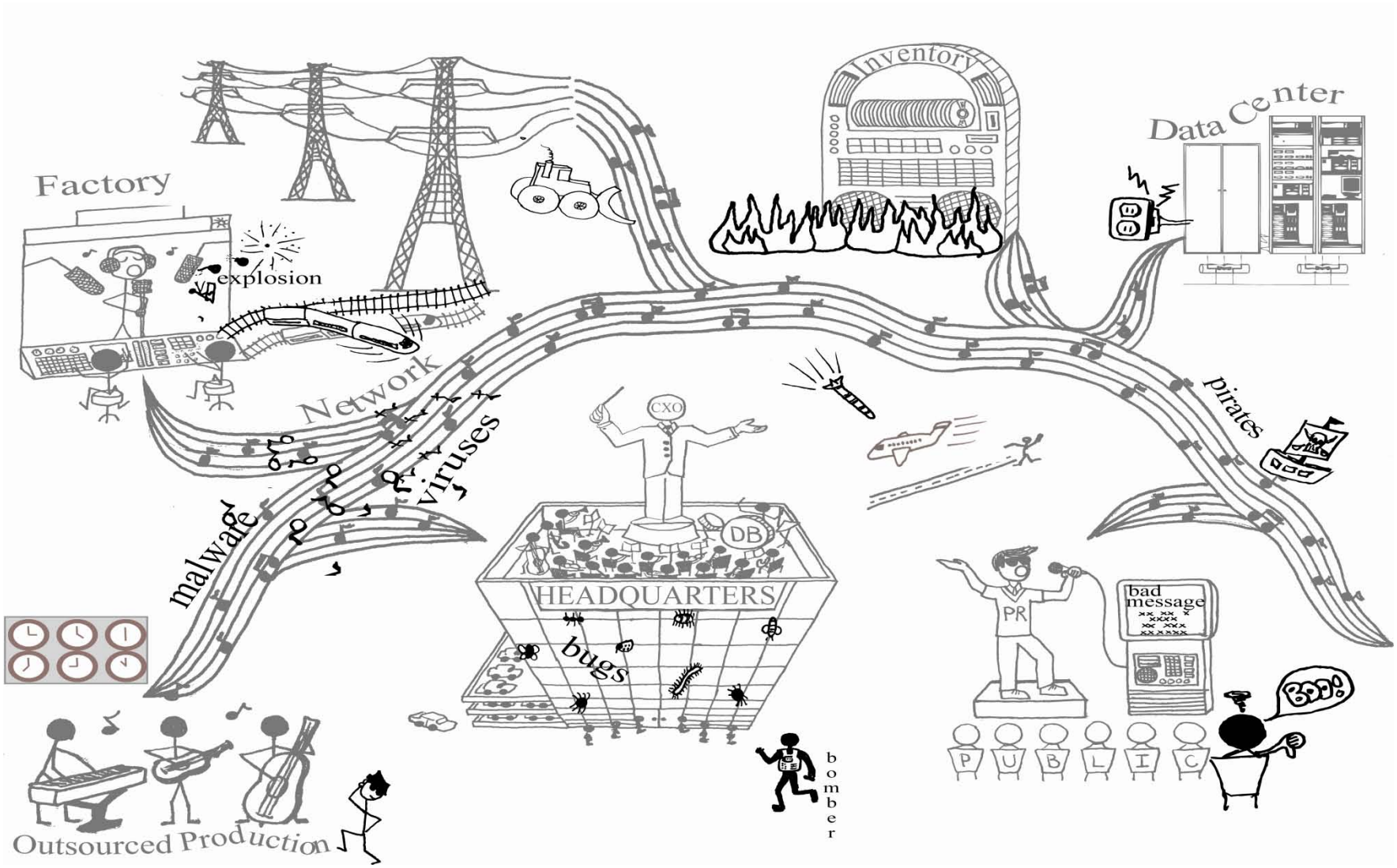
The plane has to stay in the air and get to the destination.

Source: Bayuk, Jennifer, Introducing Security at the Cradle SANS Security and Audit Controls that Work Conference. April 2003

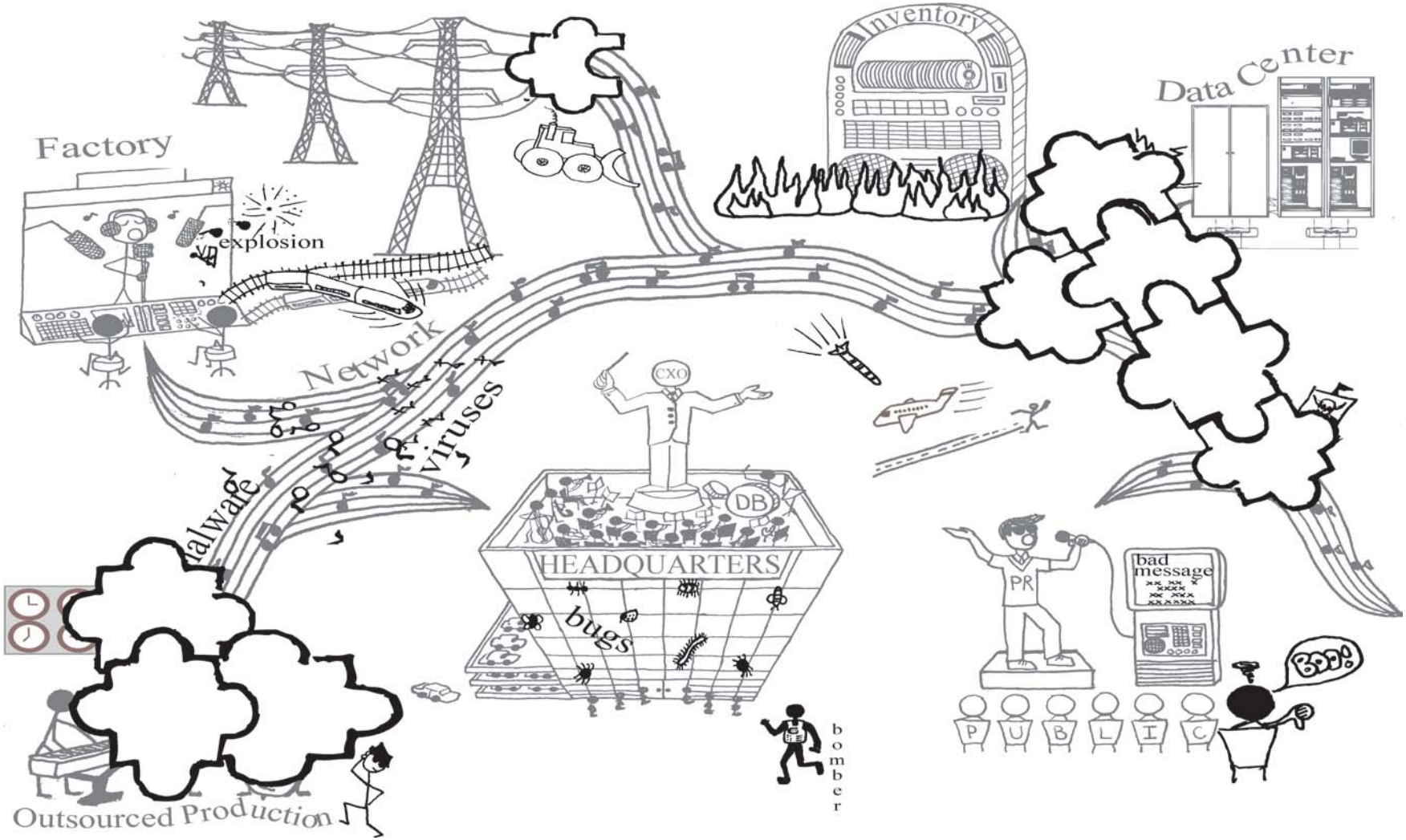
CXO Strategy



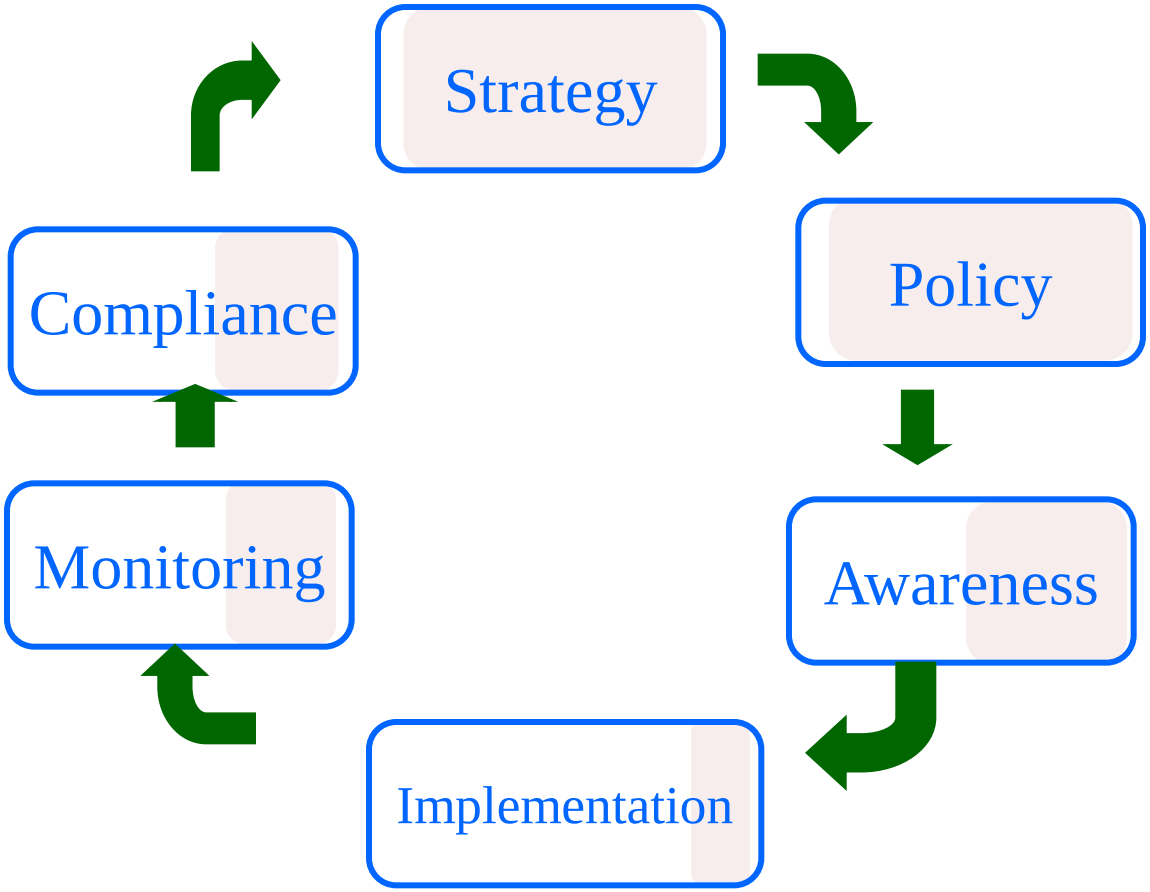
Threat Landscape Overlay



Hamster Wheel Approach



Holistic Security Program

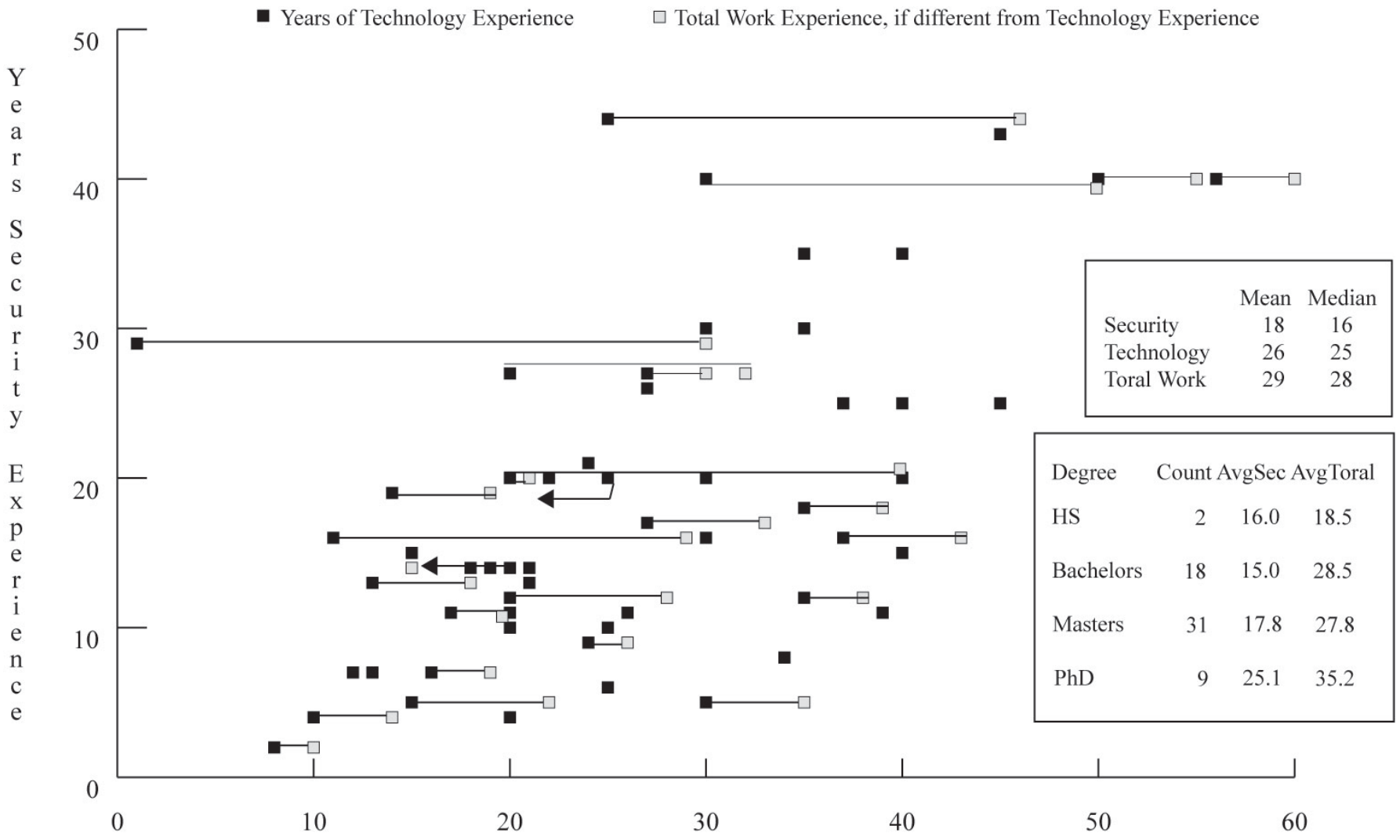


Source: Bayuk, Jennifer, *Stepping Through the InfoSec Program*, ISACA, 2007

Holistic System Security Architecture

- A system security architecture should have:
  - Security requirements corresponding to enterprise mission and threat environment
  - Major enhancements to currently available security metrics data generation, collection and analysis, as well as corresponding decision analysis and response options
  - Increases in security effectiveness of existing security architecture patterns and more cost efficient deployment of security resources

Security SME Survey Demographics



	Mean	Median
Security	18	16
Technology	26	25
Toral Work	29	28

Degree	Count	AvgSec	AvgToral
HS	2	16.0	18.5
Bachelors	18	15.0	28.5
Masters	31	17.8	27.8
PhD	9	25.1	35.2

Security SME Survey Results

Winners

User identification and authentication
Withstand targeted penetration attacks by skilled attack teams
Incident detection and response
System interfaces accept only valid input
Articulate, maintain, and monitor system mission
Security awareness
Evaluate the extent to which systems are protected from known threats
Physical and environmental protection
Personnel screening and supervision

More Important

Segregate users into groups or roles for access control
Software integrity preservation
Due diligence in system and services acquisition
Infrastructure risk assessment
Security features that correspond to system functions
Control over removable media
Logs that verify that process designed to secure system is followed
Certification, accreditation, and security assessments
Quantify the value of assets at risk in system operation

Very Important

System recovery planning
Security features required to maintain integrity over system interfaces
System and software change control
System output conforms to well-defined specifications
Pass internal security review
Maintain audit trails on use of system functions
System-level risk assessment

Still Important

Progress in a management plan to secure system
Use security standards as system requirements
Successful execution of business continuity procedures
Fail in denial of service mode
Maintain integrity of interfaces through system development lifecycle
Pass security audit
System follows a commonly used architecture pattern
Percentage of systems or components that have passed security configuration tests
Pass regulatory audit
Oversight of vendor maintenance
Maintain values of standard security variables in system technical configuration
Number of resources consumed in system security tasks

Security SME Survey Summary Results

Winners – System-level security functionality

Very Important – System maintenance processes

More Important – Component level controls

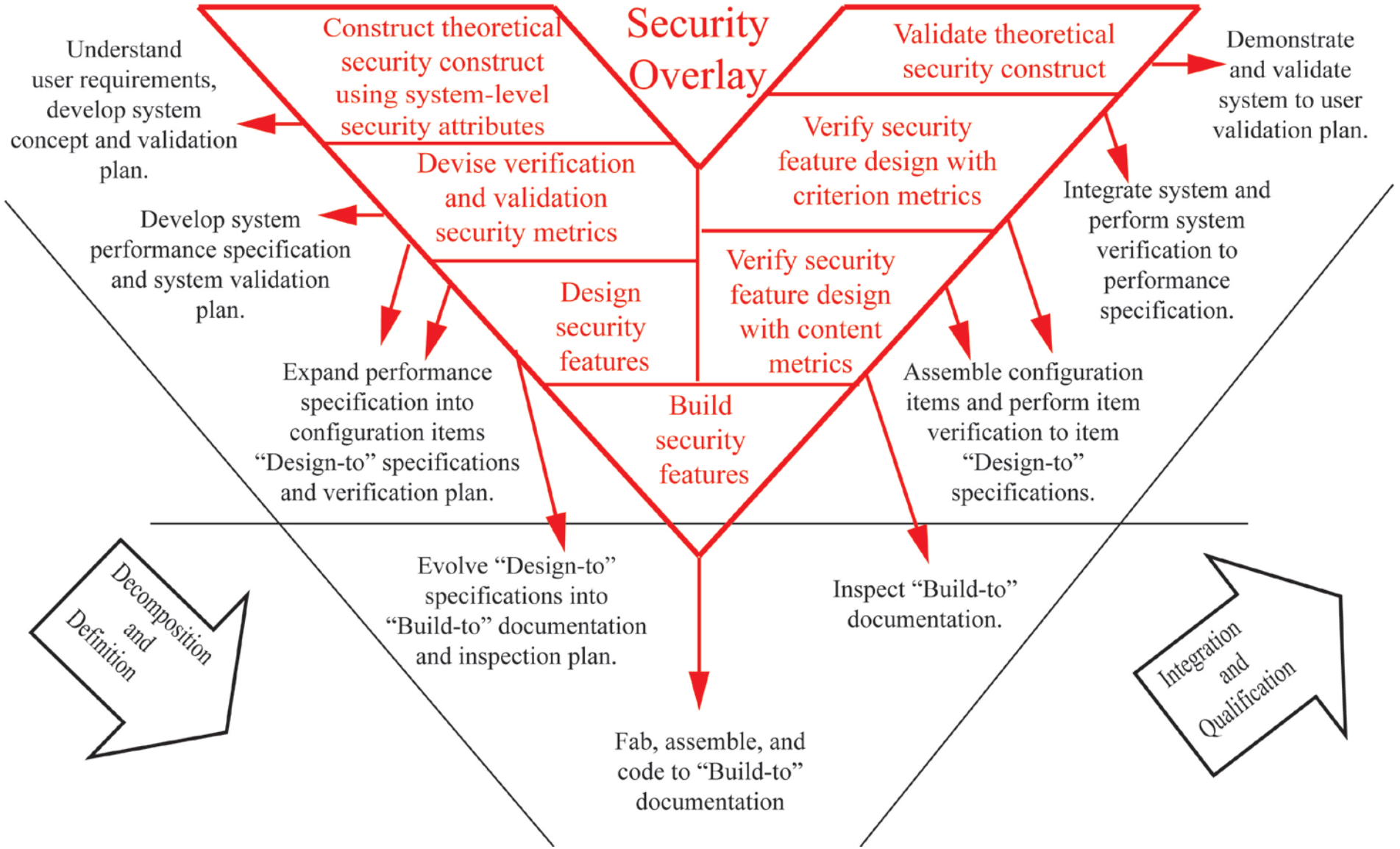
Still Important – Checklists and audit

All data available at: http://www.bayuk.com/thesis/

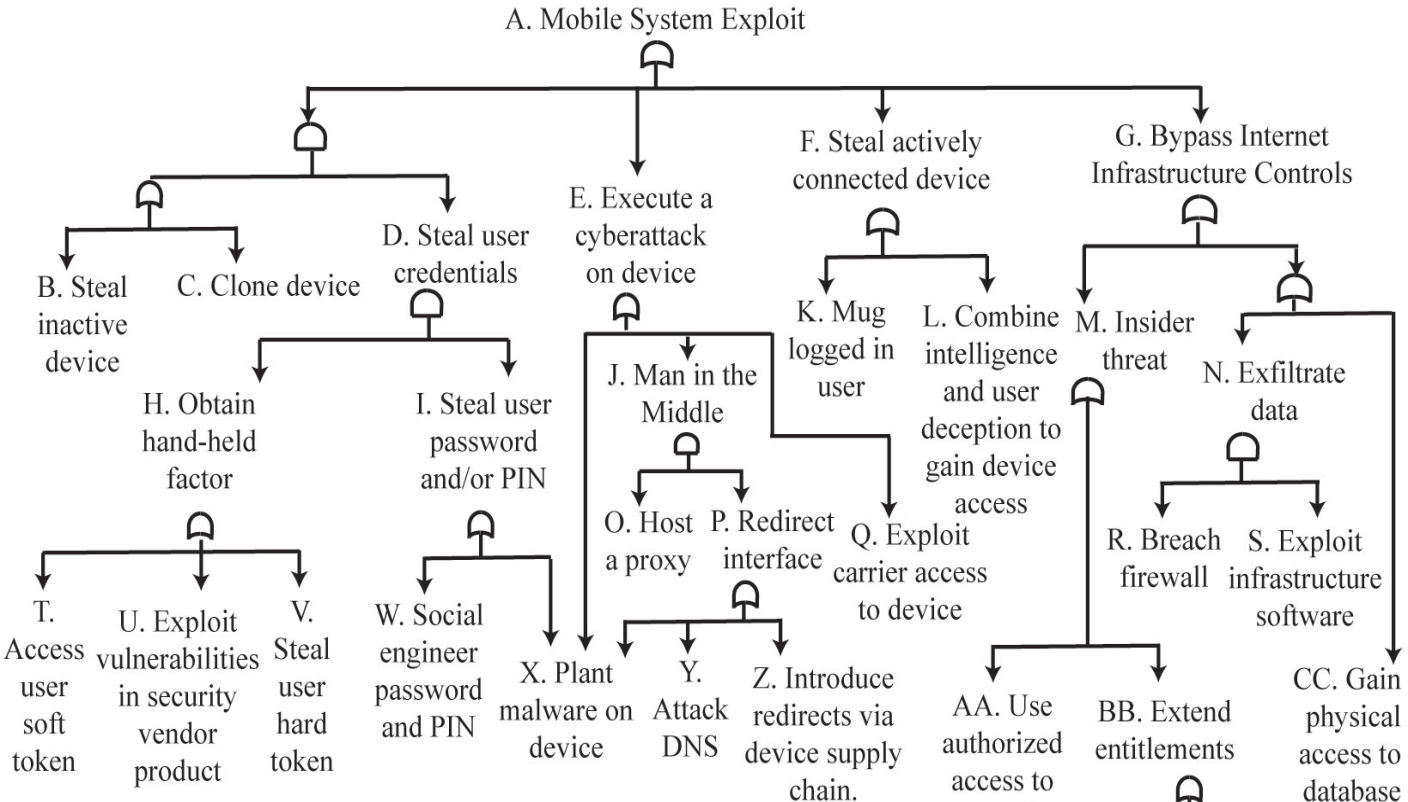
Why System-Level Security?

- System security may comply with security standards, yet still not serve the mission of a given enterprise
  - Security professionals call this: correct versus effectiveness (C&E)
  - Certification authorities call this: security testing and evaluation (T&E)
  - Engineers instead use: verification and validation (V&V)
- Current approaches to security engineering:
  - Apply standard criteria to an enterprise security program to determine its security strength
  - Measure process rather than results
  - Concentrates on security risk, the cost of controls, and the expected benefit of return on a single security investment
  - Pass C&E, T&E, and Verification, but fail on Validation

System Security Modeling



Example Mobile Communications: Attack Tree



List of attack paths:

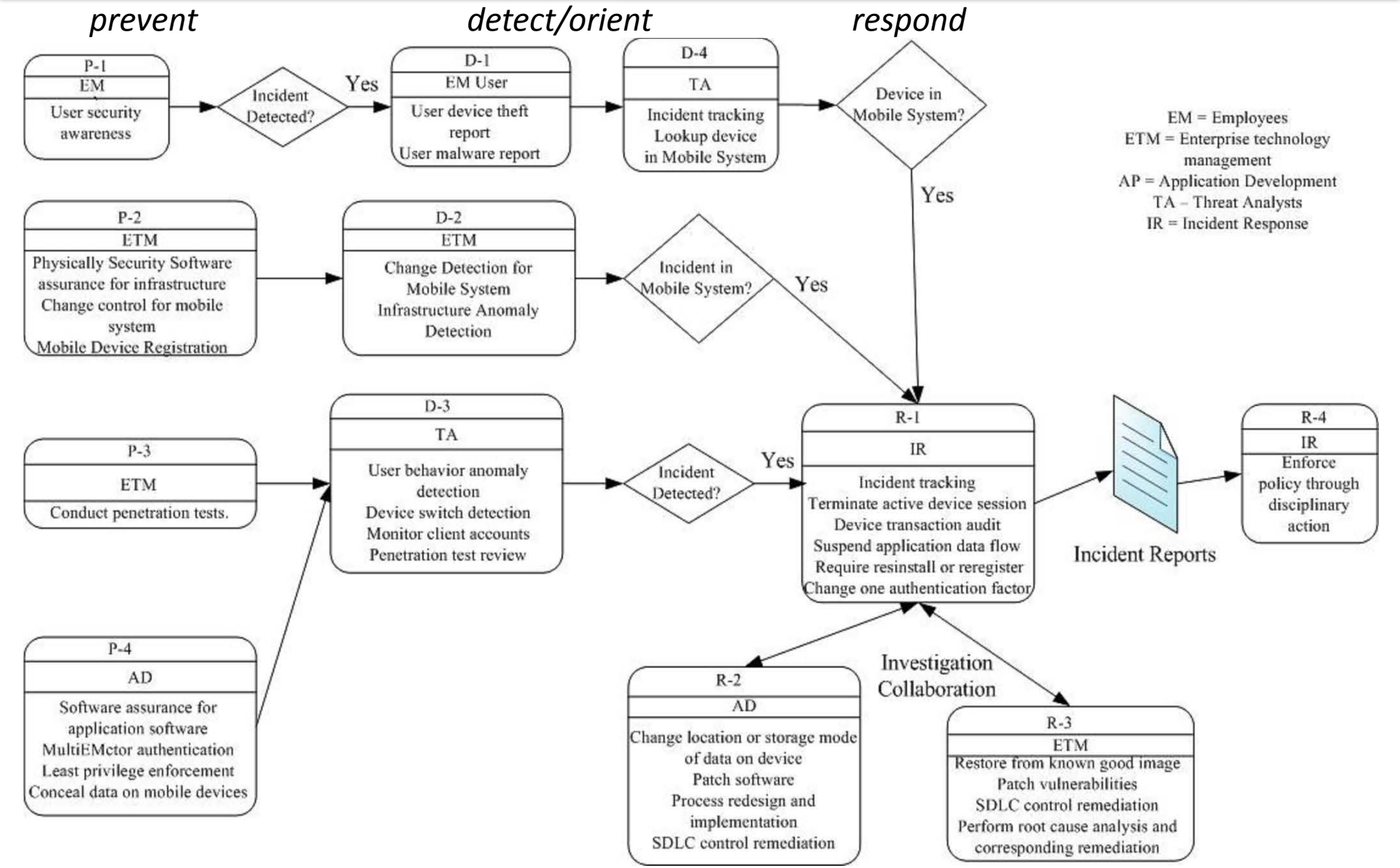
1. A,**B**,D,H,**T**,I,**W**
2. A,**B**,D,H,**T**,I,**X**
3. A,**B**,D,H,**U**,I,**W**
4. A,**B**,D,H,**U**,I,**X**
5. A,**B**,D,H,**V**,I,**W**
6. A,**B**,D,H,**V**,I,**X**
7. A,**C**,D,H,**T**,I,**W**
8. A,**C**,D,H,**T**,I,**X**
9. A,**C**,D,H,**U**,I,**W**
10. A,**C**,D,H,**U**,I,**X**
11. A,**C**,D,H,**V**,I,**U**
12. A,**C**,D,H,**V**,I,**W**
13. A,E,**X**
14. A,E,J,**O**,P,**X**
15. A,E,**O**
16. A,E,J,**O**,P,**Y**
17. A,E,J,**O**,P,**Z**
18. A,F,**K**
19. A,F,**L**
20. G,M,**AA**
21. G,M,BB,**DD**
22. G,M,BB,**EE**
23. G,N,**R**,**S**
24. G,**CC**

KEY: and / or

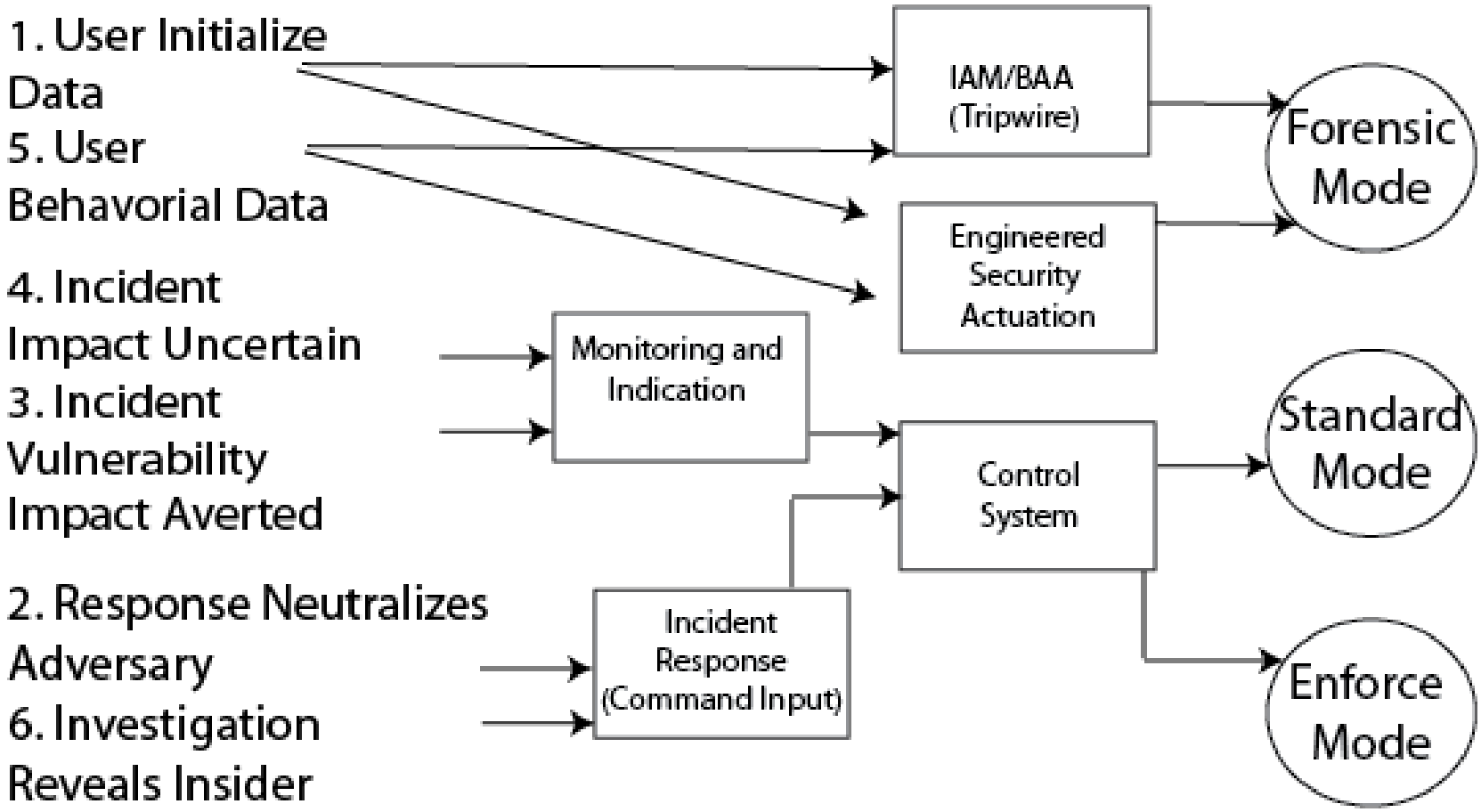
Mobile Communications: OODA/PDR Loop Feature List

Security Feature Requirements Map to Model			
#	**Expected failure in:**	**Requires a response such as:**	
Preventive Controls			
P1	Physical security (3)	R1	Suspend application information flow (8-m-5)
P2	User security awareness (6)	R2	Terminate active device session (8-m-5)
P3	Multifactor authentication (5)	R3	Change one authentication factor (8-m-5)
P4	Conceal data on mobile devices (10)	R4	Change location or storage mode of data on device (6-k-10-e)
P5	Software assurance (4-j-6-k)	R5	Patch software and require reinstall (6-i-10-s)
P6	Least privilege (9h-5-1)	R6	Process redesign and implementation (9-q-h-5,9-9-h-3)
P7	Mobile system change control (3)	R7	Restore from a known good image (3)
Detective Controls			
D1	User theft report (r-9)	(R1)	Suspend application information flow
D2	User behavior anomaly detection (2-b-5-g-7-l-n-8)	(R2)	Terminate active device session
D3	Device switch detection (2-b-5-g-7-n-8)	R8	Incident tracking (9)
D4	Device tamper detection (2-b-5-g-7-n-8)	R9	Device transaction audit (2)
D5	Penetration tests (4)	R10	Patch vulnerable software and/or infrastructure (3, j-6-k-10)
D6	Monitor client accounts (8-f-2)	R11	Enforce policy through disciplinary action (8-p-9-q)
D7	Mobile system change detection (8-f-2)	R12	Systems development lifecycle control remediation (8-p-9-q,3)
D8	Mobile system anomaly detection (8-f-2)	R13	Root cause analysis and corresponding remediation (8-p-9-q,3)

Mobile Process Support Requirements

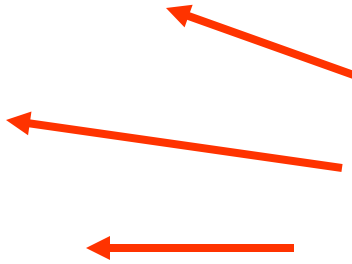


Design for Redundancy and Functional Block Partitioning



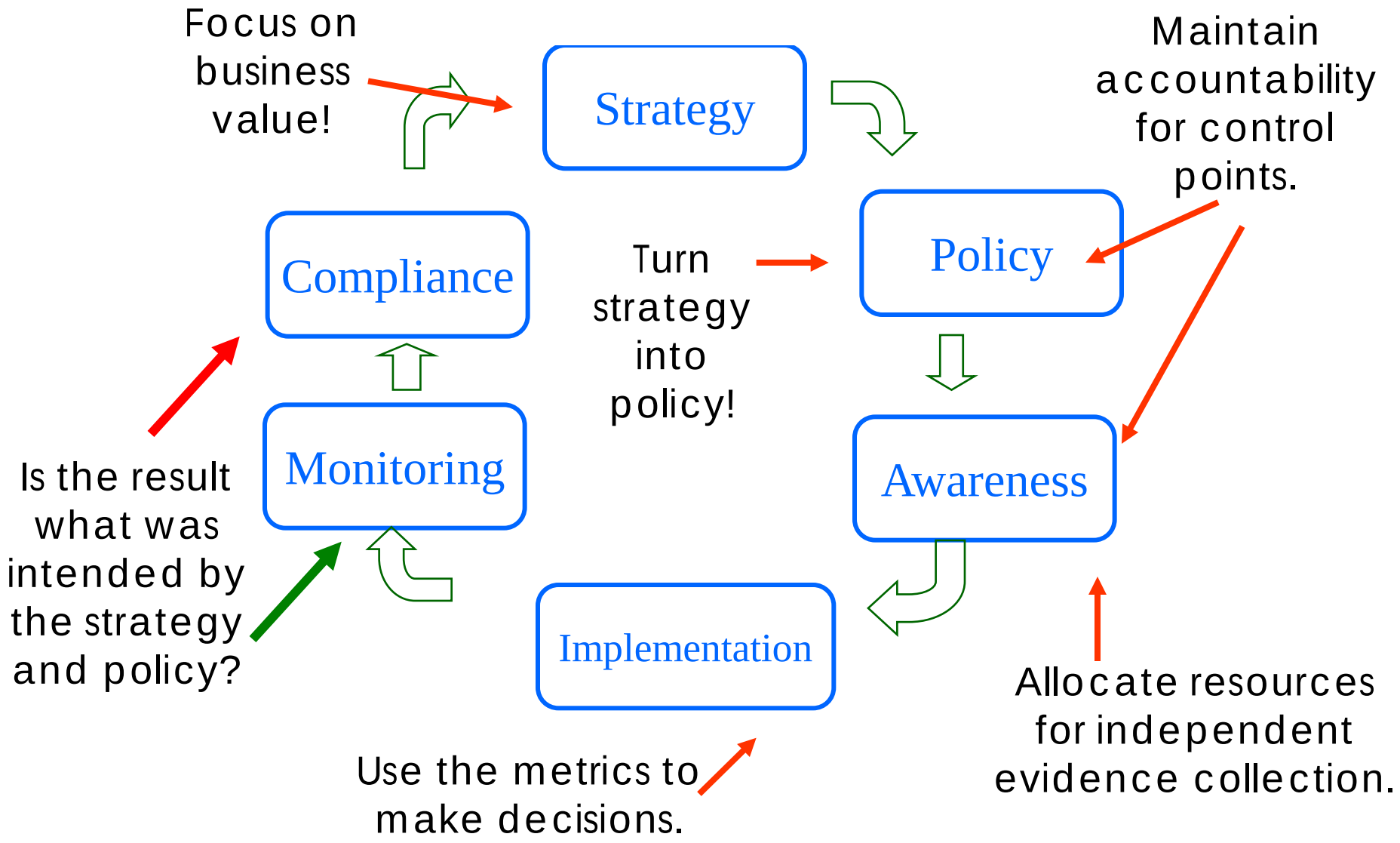
Triad and True

- Prevent, Detect, Respond
- Confidentiality, Integrity, Availability
- People, Process, Technology
- Audit, Review, Assess
- Monitor, Measure, Manage

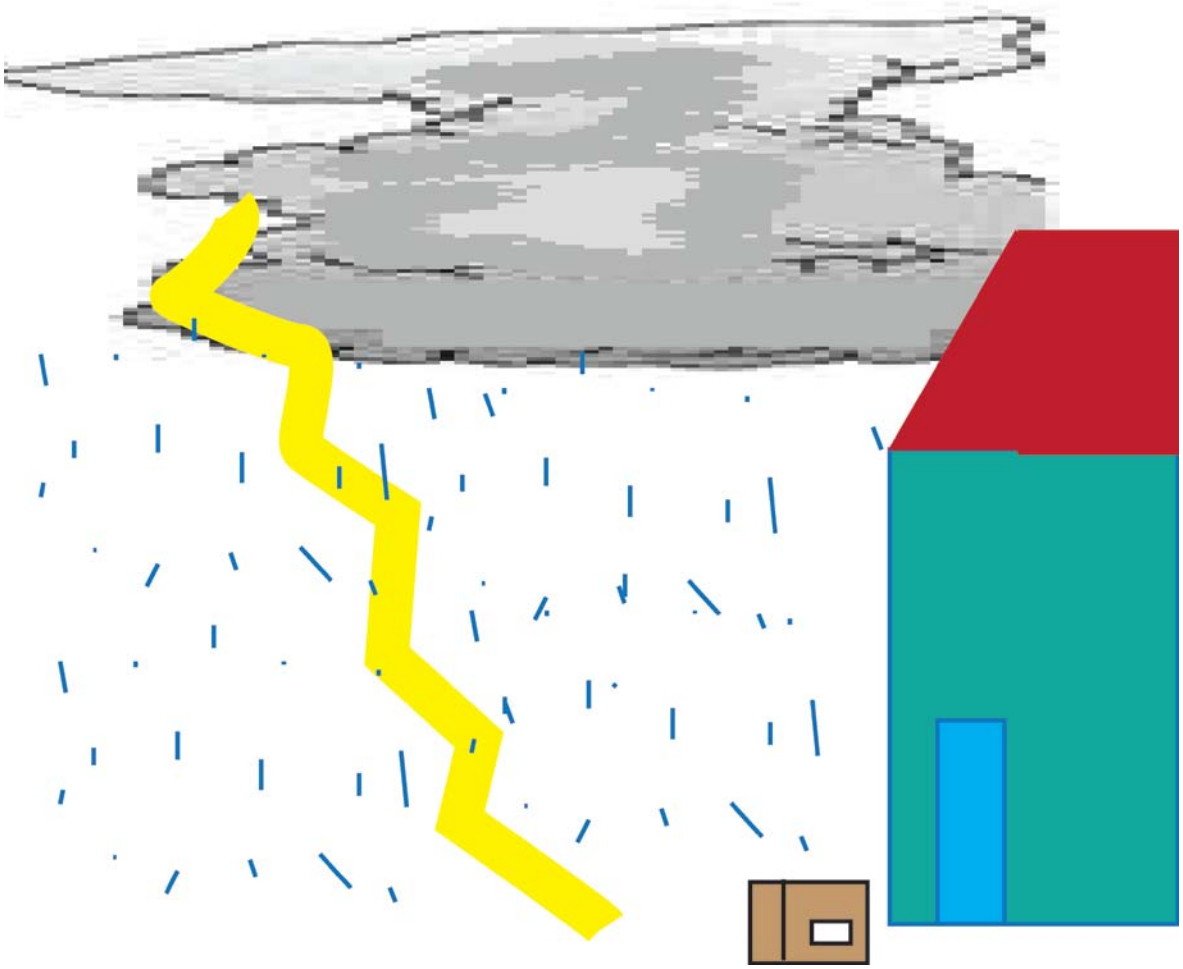


CXOs already do this.

CXO Security Support Strategy



Design Basis Threat



Questions, Discussion?

jennifer@bayuk.com

www.bayuk.com