Pairing Organizational Strategy with Security Solutions

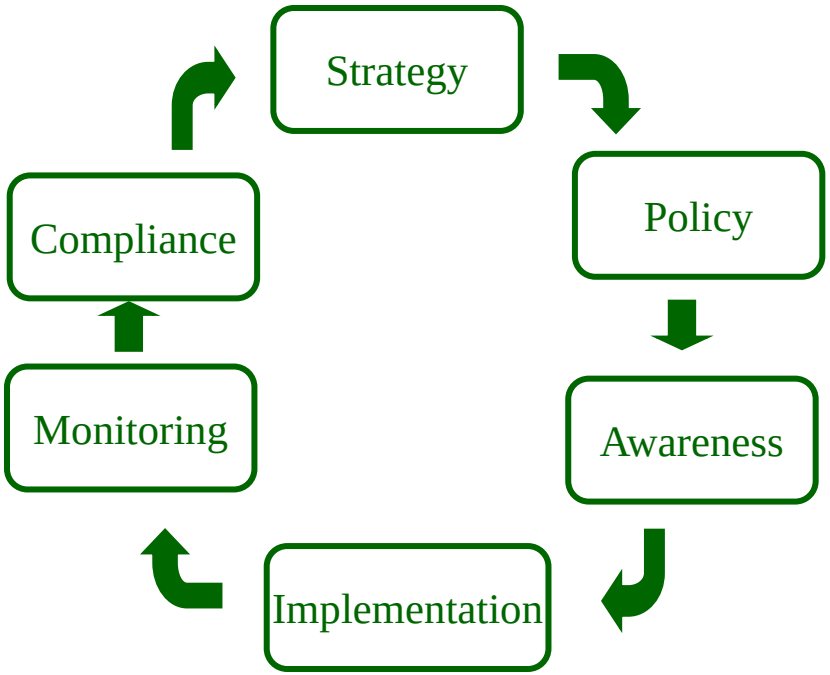
Jennifer Bayuk, CISA, CISM, CGEIT

www.bayuk.com

June 9, 2010
The Roosevelt Hotel
New York City

Security Strategy

- Tone at the top
- Strategy
- Organization
- Process
- Risk
- Metrics



Tone at the Top

- Is reflected in decisions
- Is observed, not communicated
- Exists whether cultivated or not
- Cannot be created via documents

Tone-setting Activities

- Memos to staff
- Training Videos
- Awareness activities
- Program visibility
- Process integration
- Documentation availability

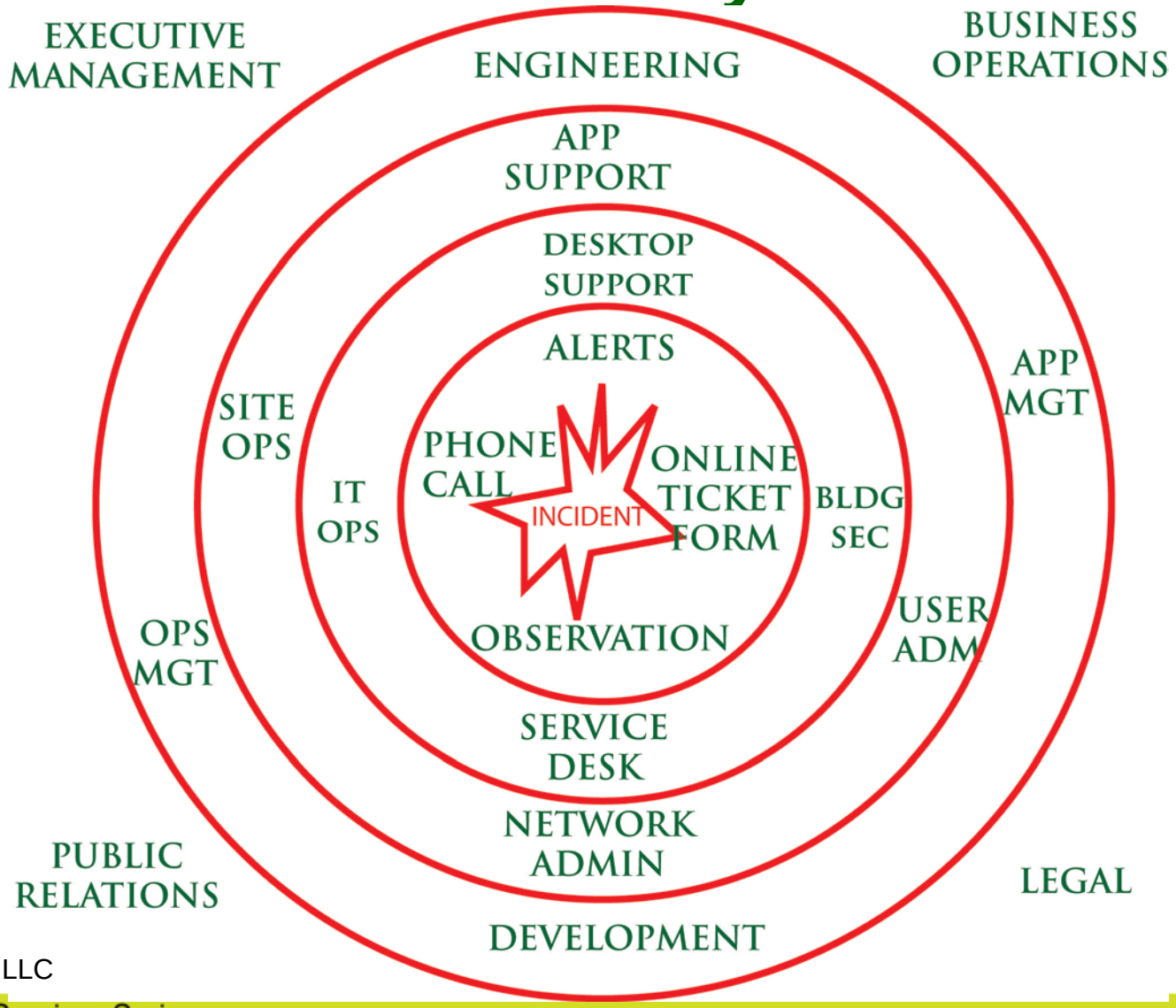
Security Program Strategy

Observe-Orient-Decide-Act	*– Original Military version*
Plan-Do-Check-Correct	*– The ISACA COBIT version*
Plan-Secure-Confirm-Remediate	*– A popular Software Vulnerability guide version*
Prepare-Detect-Respond-Improve	*– Carnegie Mellon's CERT version*
Restrict-Run-Recover	*– A Big 4 consultant's version*

Tone ➔ Strategy

- How involved is management in the program?
  - Policy?
  - Process?
  - Job function?

Information Security Process



InfoSec Resources

- Executive Management Steering Committee
- Chief Risk Officer
- Chief Privacy Officer
- Information Security Manager
- Director of IT Operations
- IT Site Operations Manager
- IT Implementation Management
- IT Subject Matter Experts
- Application Architects
- IT Project Managers
- IT Product Owners
- Security Administrators
- Business Application Owner
- Business Data Owner
- Procurement Manager
- Compliance Manager
- Physical Security Organization

InfoSec Roles and Responsibilities

Given "realms" of business operation, resource identification involves not only specifying areas of responsibilities, but also making use of existing business and operational process.

Where a person performs this role:	An associated InfoSec process responsibility is:	A sample key performance indicator is:
Manages the lifecycle of IT **applications** and platforms	Security Review Participation	Security-policy-compliant systems configuration
	Security Requirements Capture	Business requirements for confidentiality, integrity, and availability are documented
	Application Security Design	Technical implementation plans for meeting business process security requirements
	Change Control	Secure archive, retrieval, and compilation of organization-maintained source code and product customizations
	Security Upgrade Management	Testing and application of security software fixes
Procures IT services	Security Requirements Capture	Formal requirements for security in all Requests for Product Information and Proposals
	Contract Requirements	Business requirements for confidentiality, integrity, and availability in information service provider and technology maintenance contracts

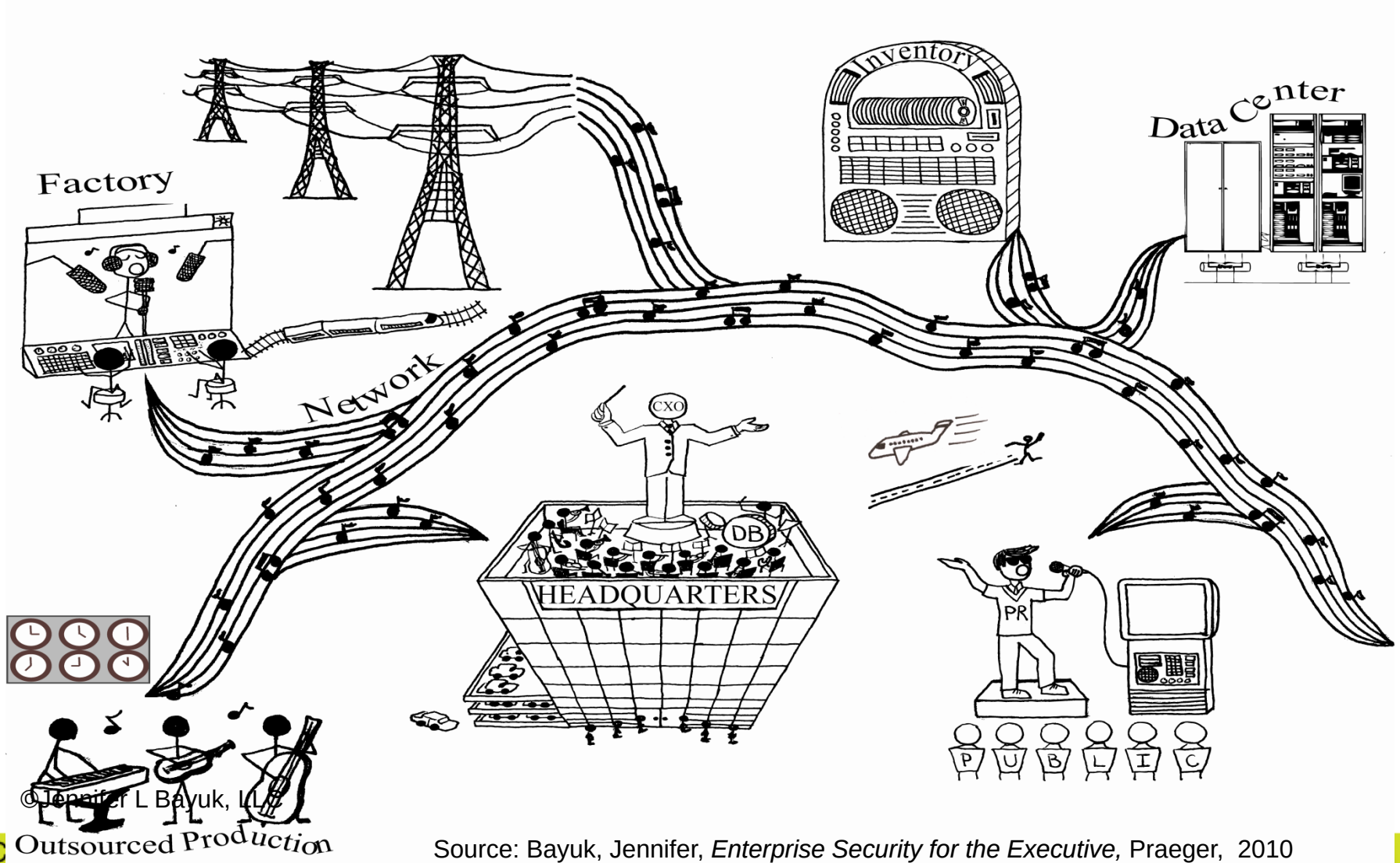
A CXO is like a Pilot

- 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.

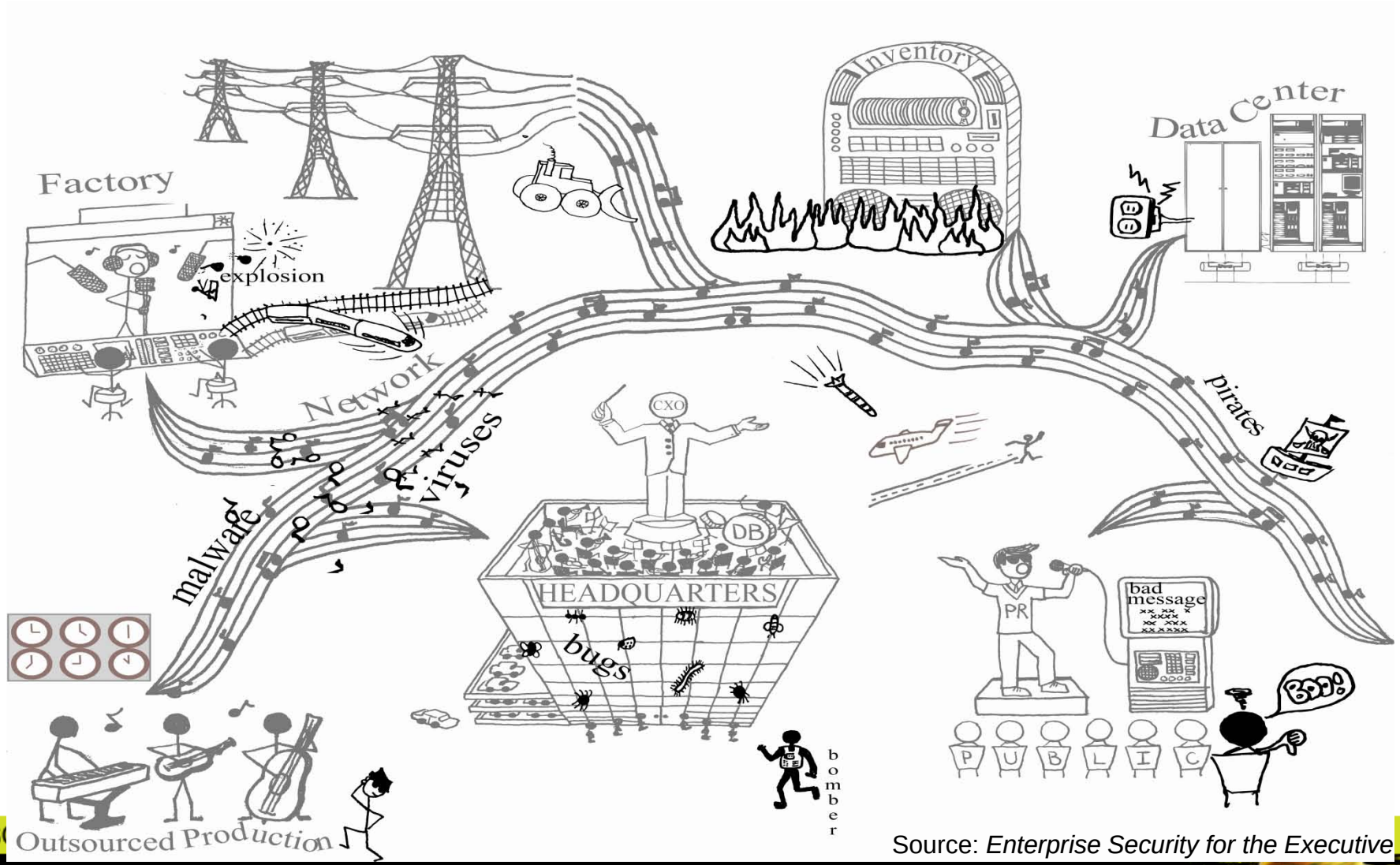
Source: Bayuk, Jennifer, Introducing Security at the Cradle SANS Security and Audit Controls that Work Conference. April 2003

What CXOs Want



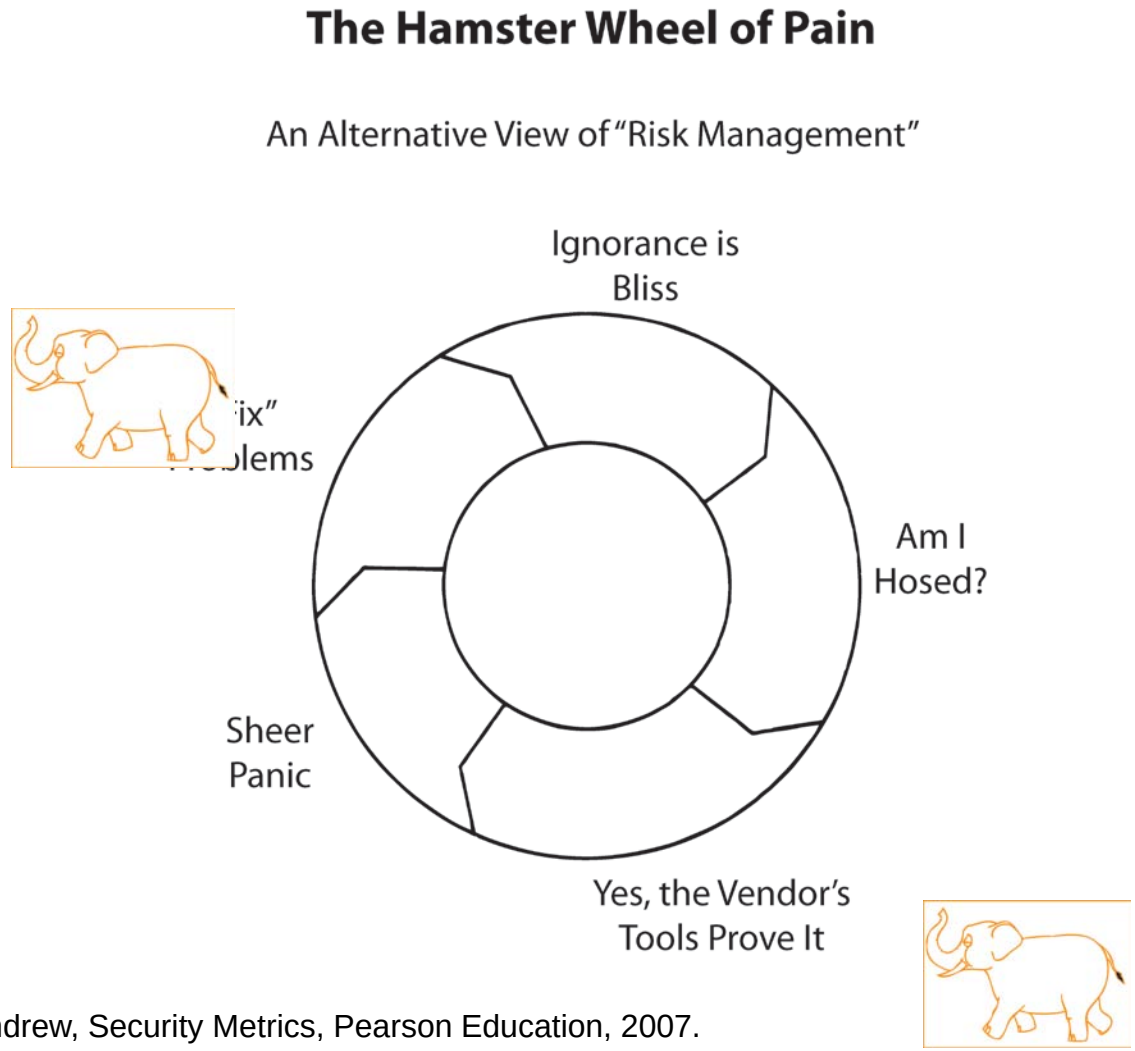
Source: Bayuk, Jennifer, *Enterprise Security for the Executive,* Praeger, 2010

Threat Landscape Overlay



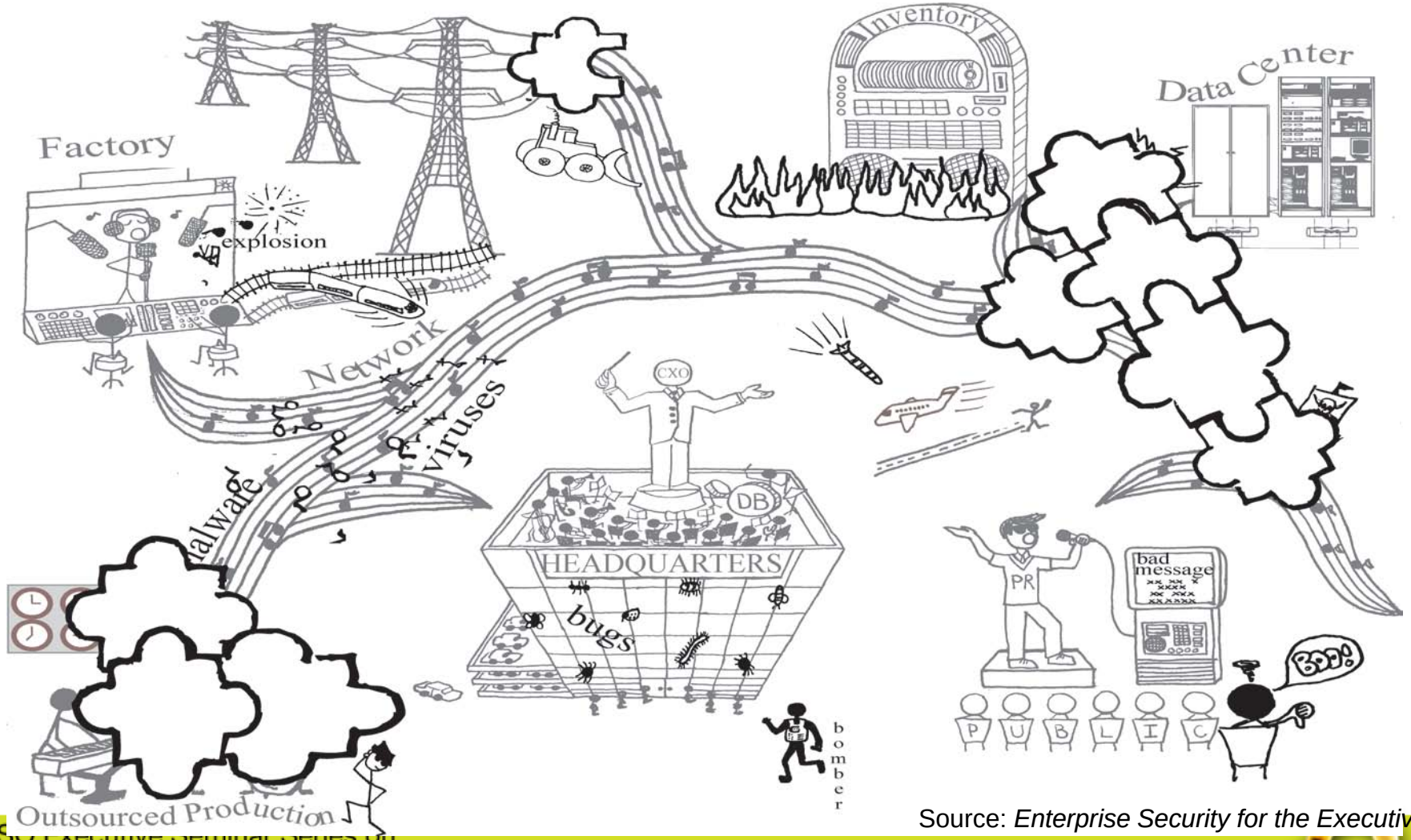
Source: *Enterprise Security for the Executive*

How *not* to view Security Risk



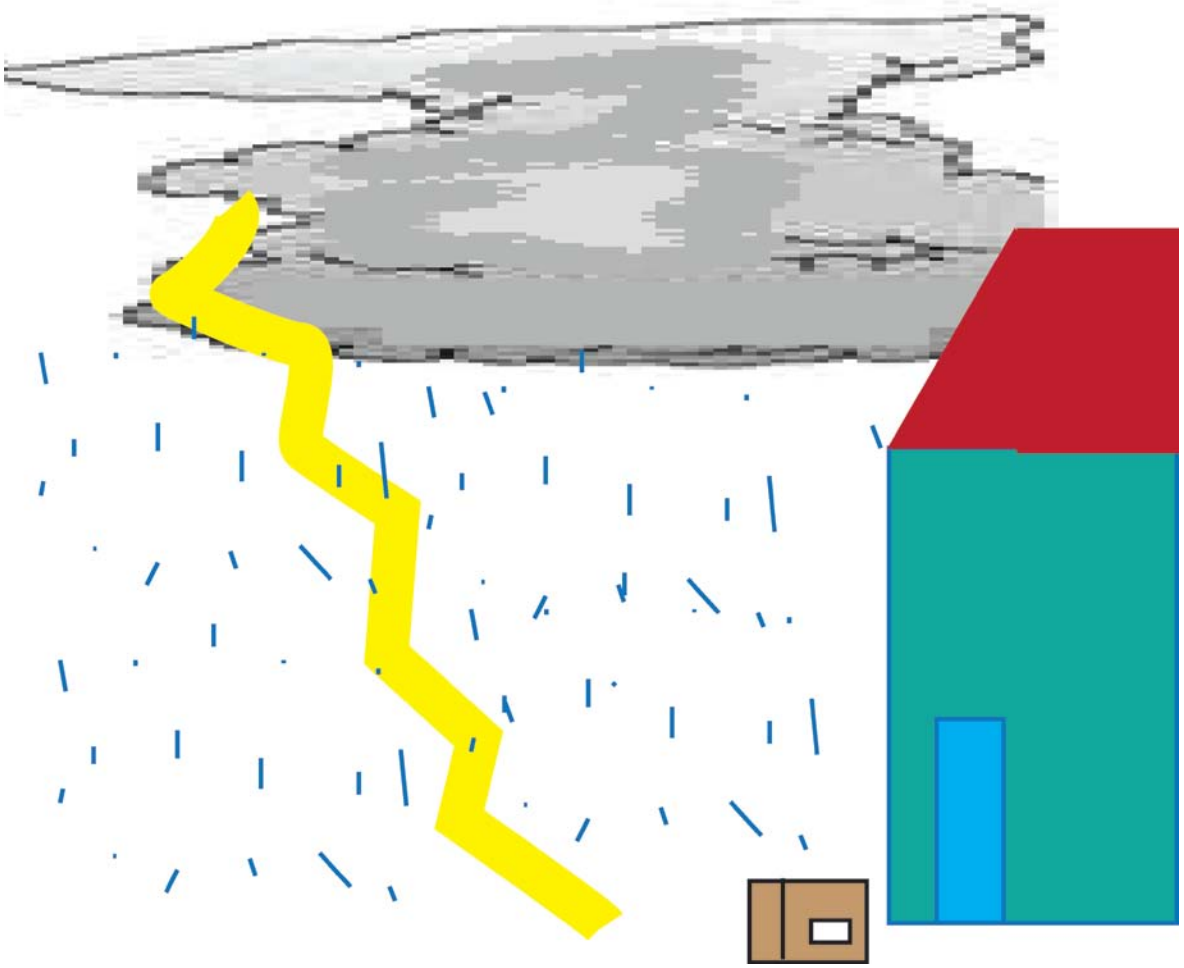
Source: Jaquith, Andrew, Security Metrics, Pearson Education, 2007.

Hamster Wheel Approach



Source: *Enterprise Security for the Executive*

Weatherproofing Analogy



Policy at CXO Level

- “All data used to run the physical plant should never leave the plant unless through a process controlled by information technology, and then, only for the purpose of archiving recovery data.”
- “All information concerning our customers will not be shared with anyone who does not have an immediate need to know to accomplish a service or task on the customer’s behalf.”
- “All product inventory will be stored only in company warehouses unless it is in the process of being shipped under a customer purchase order.”

Awareness promotes Accountability

Think holistically

Program should be unavoidable

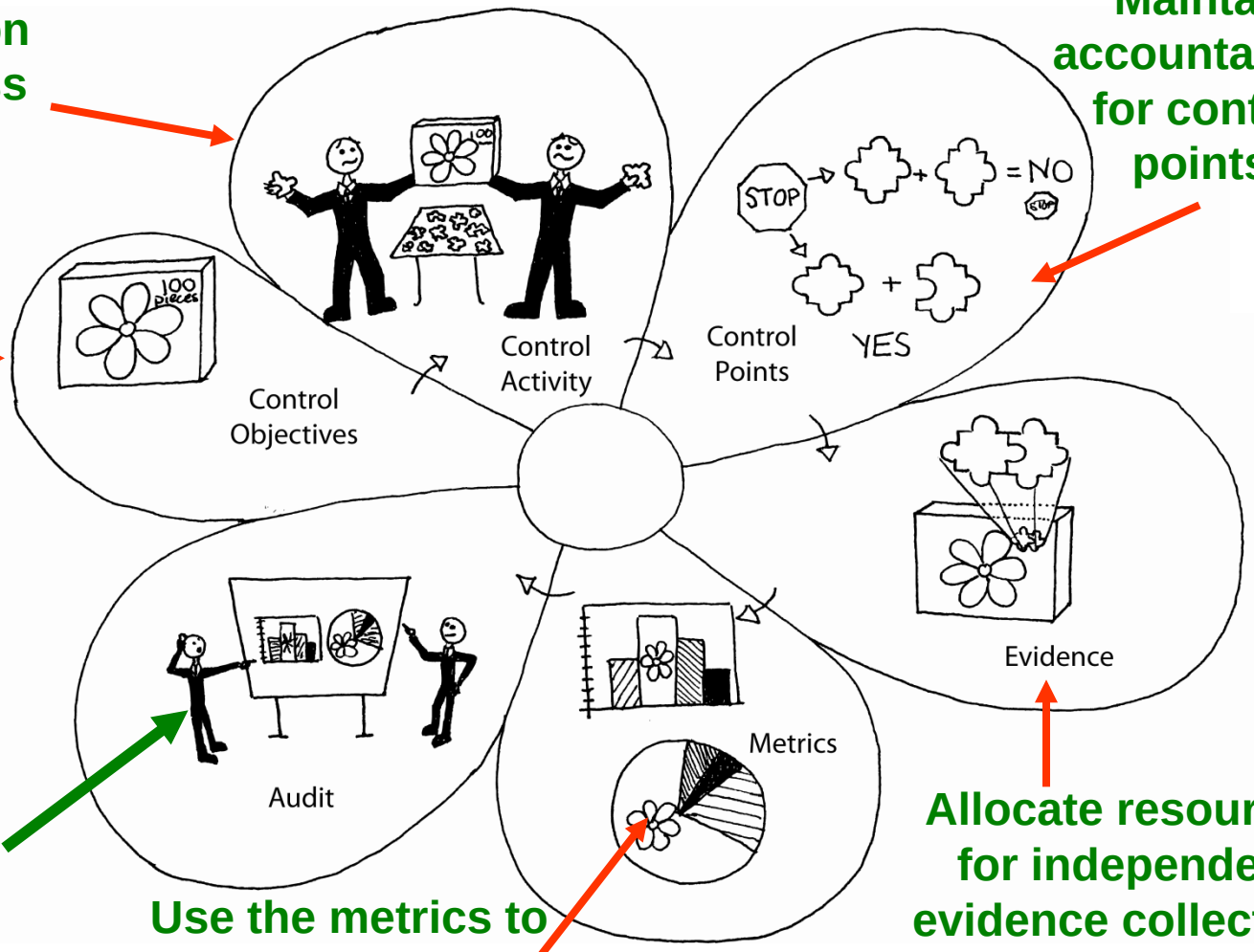
- Tone at the Top
  - Documentation
    - Roles and Responsibilities
      - Process Creation
        - Corresponding Training
          - Metrics

CXO Support Strategy

Focus on business value!

Maintain accountability for control points.

Turn strategy into policy!



Is the result what was intended by the strategy and policy?

Use the metrics to make decisions.

Allocate resources for independent evidence collection.

Questions, Discussion?

Jennifer Bayuk, CISA, CISM, CGEIT

www.bayuk.com

jennifer@bayuk.com

Presentation based on the book:

Enterprise Security for the Business Executive

Setting the Tone at the Top, Praeger, 2010