international CONFERENCE

#123 – Not on My Watch

How Executives Can Influence Secure Behavior

presentation excerpts

Jennifer Bayuk
Principal
Jennifer L. Bayuk, LLC

Common CSO Perspective on CEOs

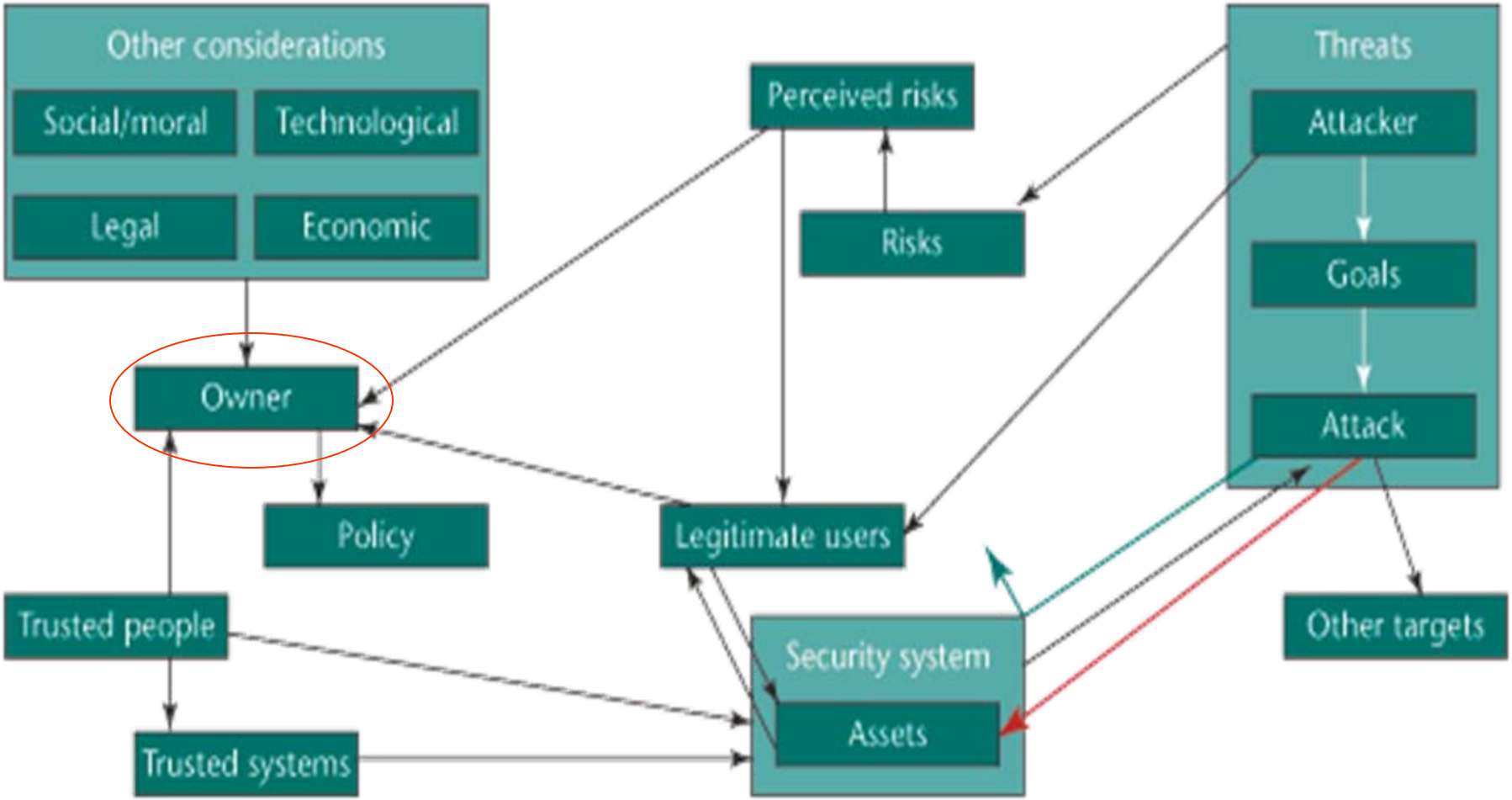
"I believe CEOs typically view the security operation as an internal insurance policy."

"Many CEOs undoubtedly view their organization's security operation as a necessary evil - as an unavoidable source of expense.

"In some instances, the only time security is considered by the C-Suite is when there is a projected expense impact or when an adverse event happens."

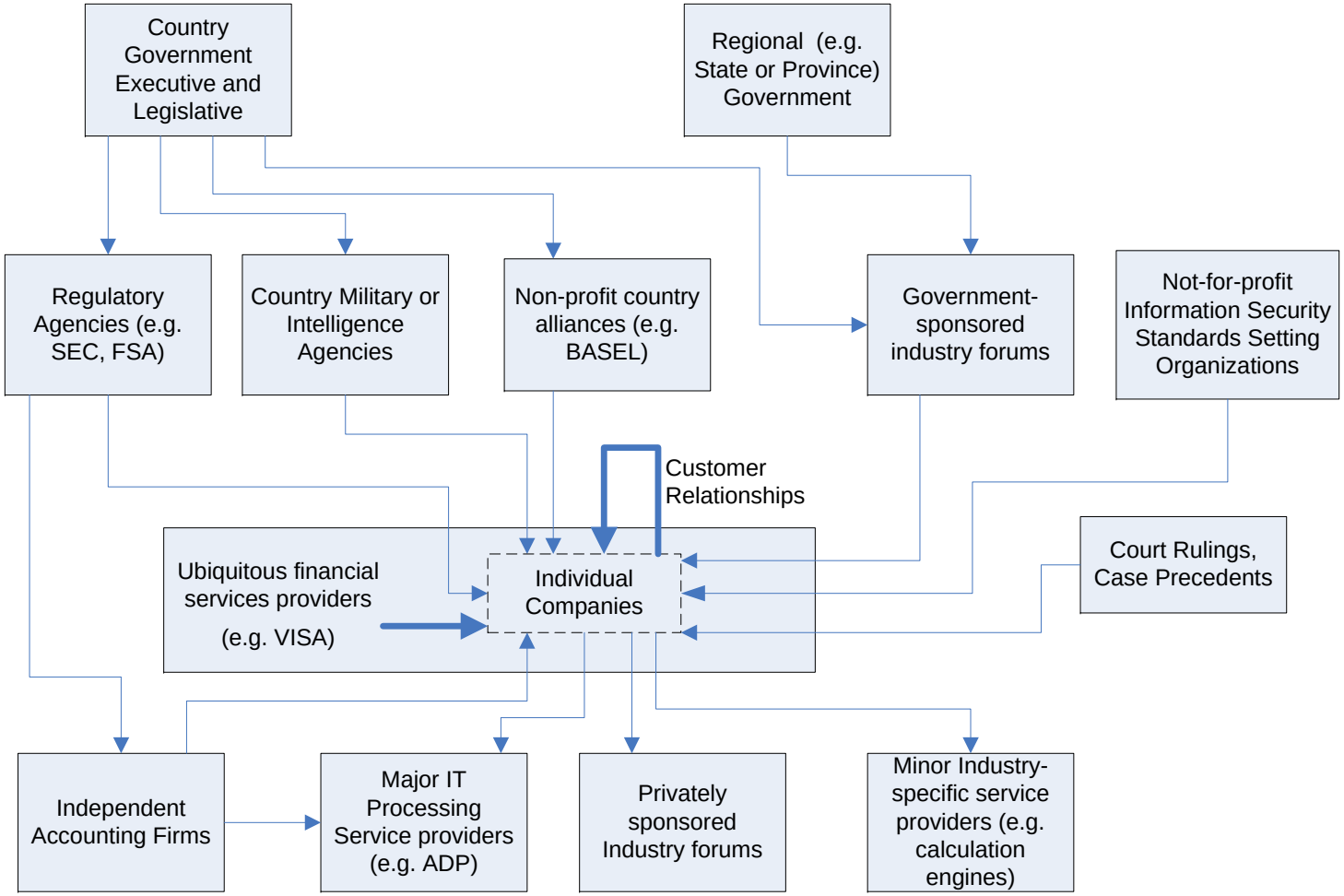
Source: Zalud, Bill, "A Strong Relationship…Except," *Security Magazine*, May 1, 2009

Example Root Cause Hypothesis



Source: Bruce Schneier, IEEE Computers and Security, May/June 2007

Business Perspective on Requirements



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

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

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

Typical Cost Justification

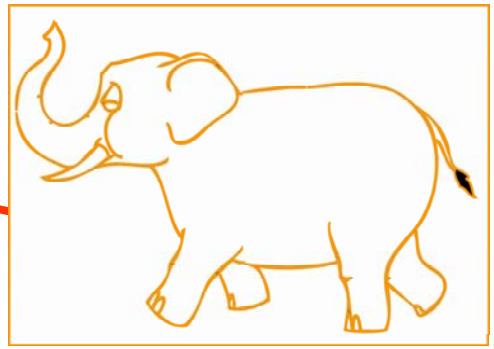
1. P = probability of event that causes harm

   C = cost of damage from the event

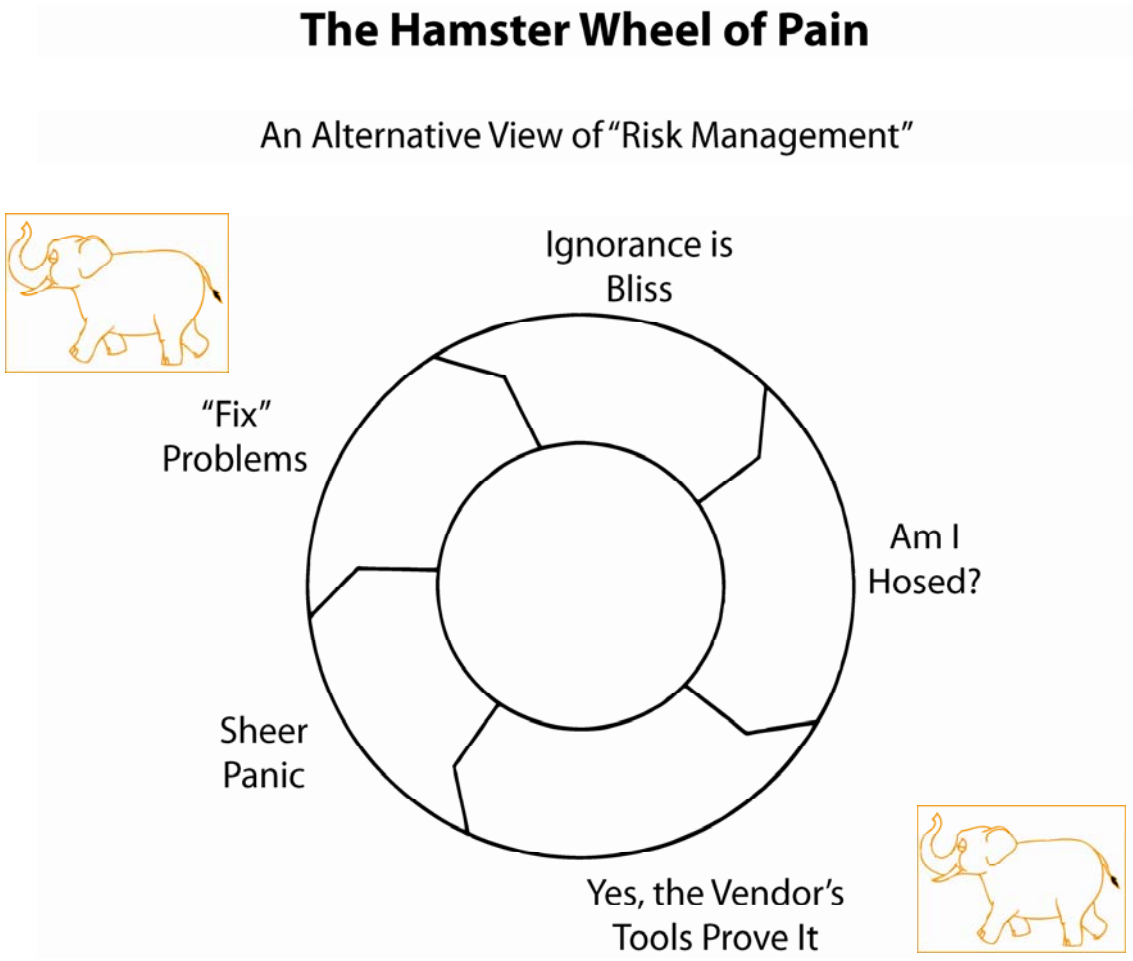
   T = cost of technology to prevent harm

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

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



How *not* to judge the value of security



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

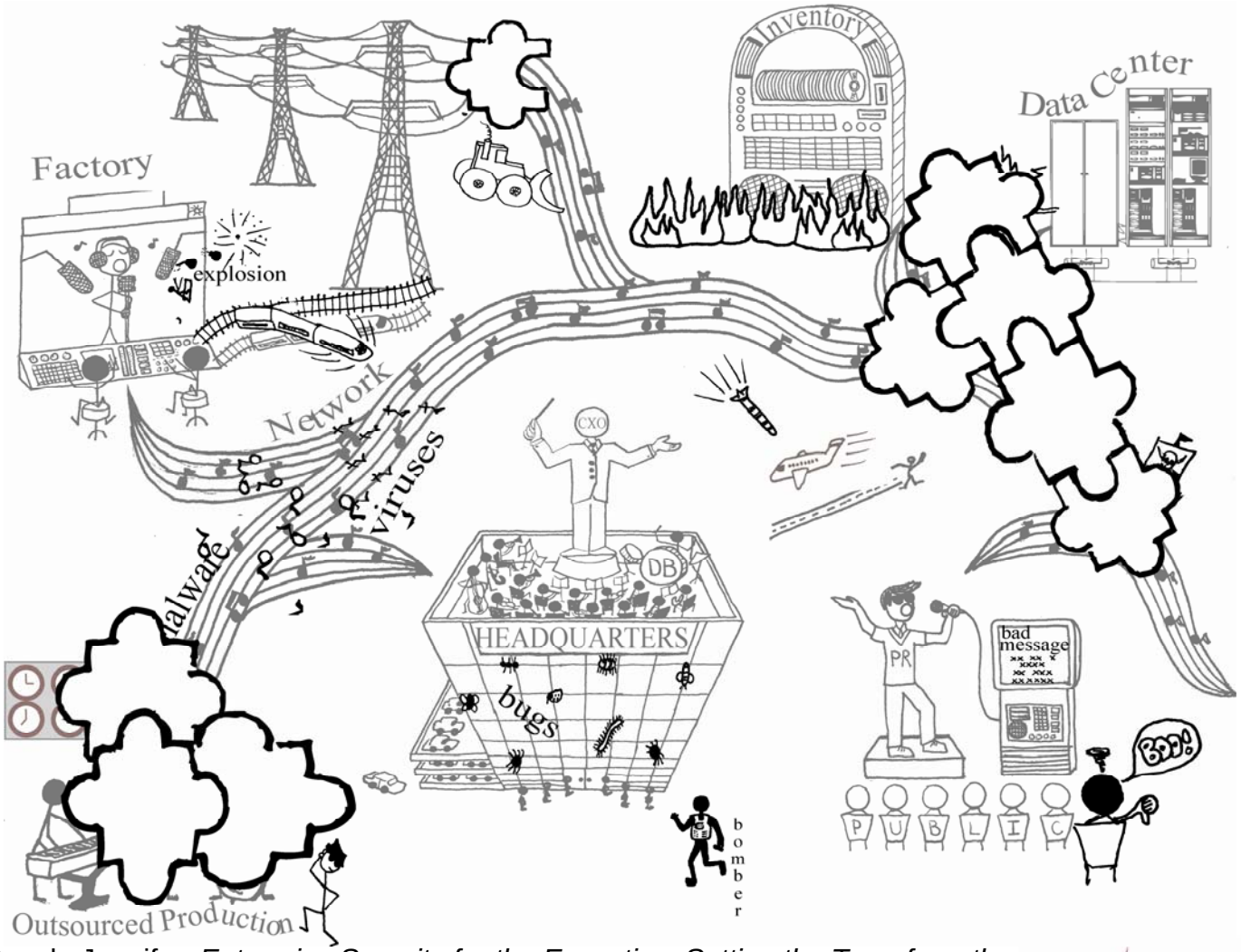
A CIO is like a Corporate Pilot

- Money Makers exert pressure
- Rulebooks provide comfort level for safe decisions
- Risk Managers provide much needed checkpoints

Similarly, *all* CXO s have surroundings to preserve!

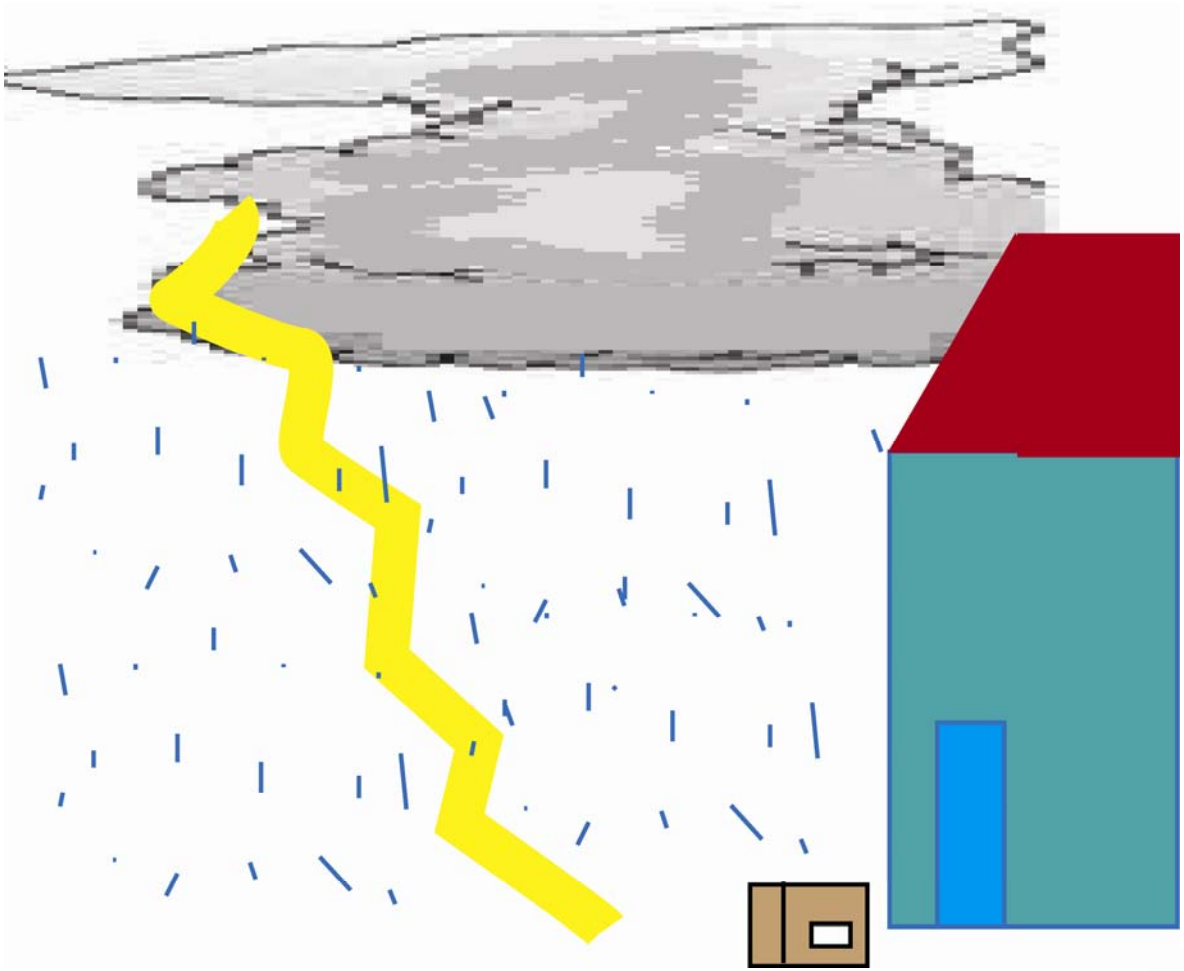
Source: Bayuk, Jennifer, “Introducing Security at the Cradle,” *SANS Security and Audit Controls that Work Conferenc,*. April 2003

Absence of systemic security

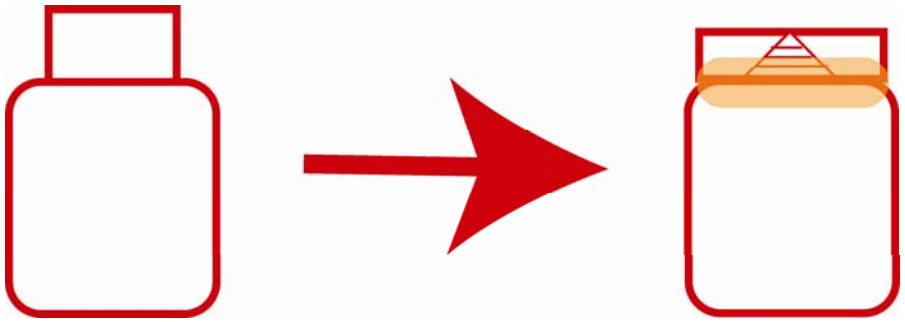


Source: Bayuk, Jennifer, *Enterprise Security for the Executive, Setting the Tone from the Top*, Praeger, Fall 2009 http://www.praeger.com/catalog/C37660.aspx

Weatherproofing Analogy



Industry Standards

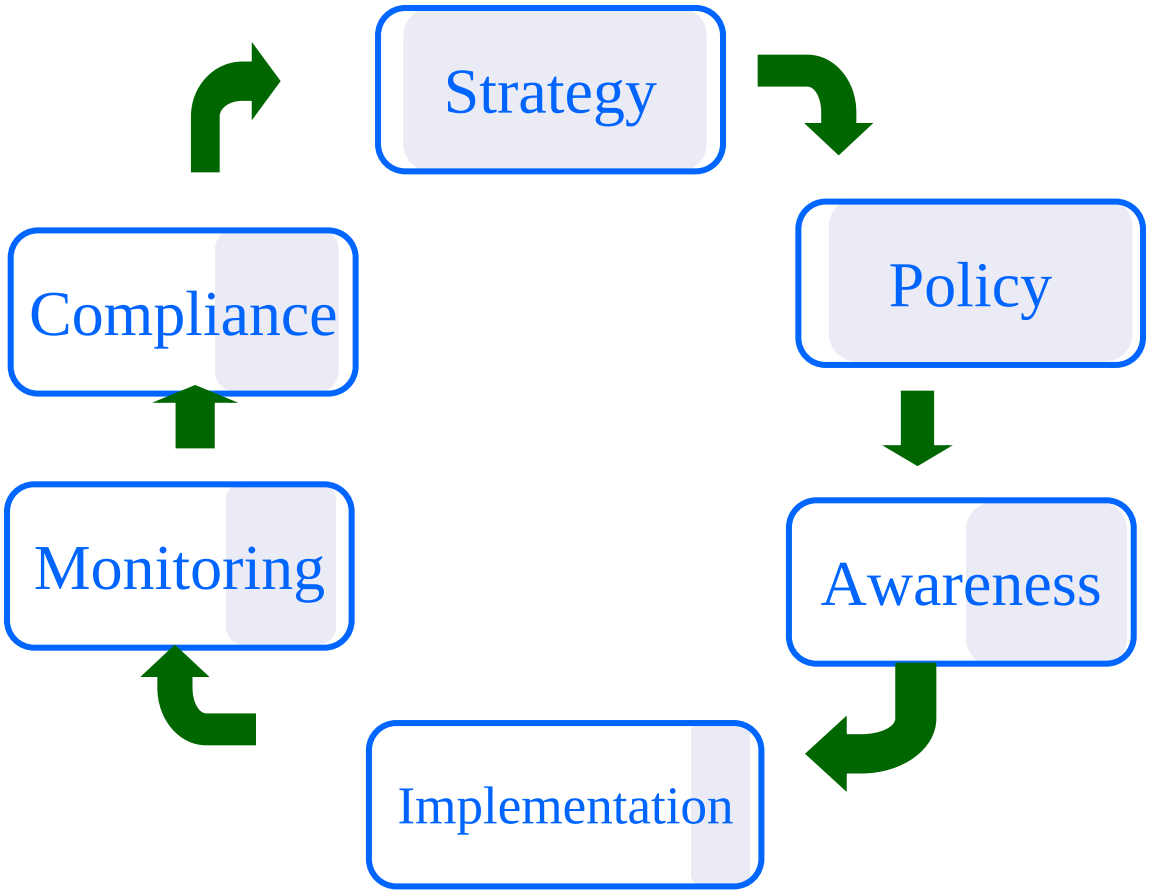


Story Source: Gostick, Adrian and Dana Telford, *The Integrity Advantage*, Gibbs Smith, 2004

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.”

Holistic Security Program



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

Triad and True

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

Security Specific.

CXOs already do this.

international CONFERENCE

For More Information:

Jennifer L. Bayuk

CISA, CISM, CISSP, CGEIT

Independent Consulting and Testimony

973-335-3530

jennifer@bayuk.com

www.bayuk.com