NEbraskaCERT

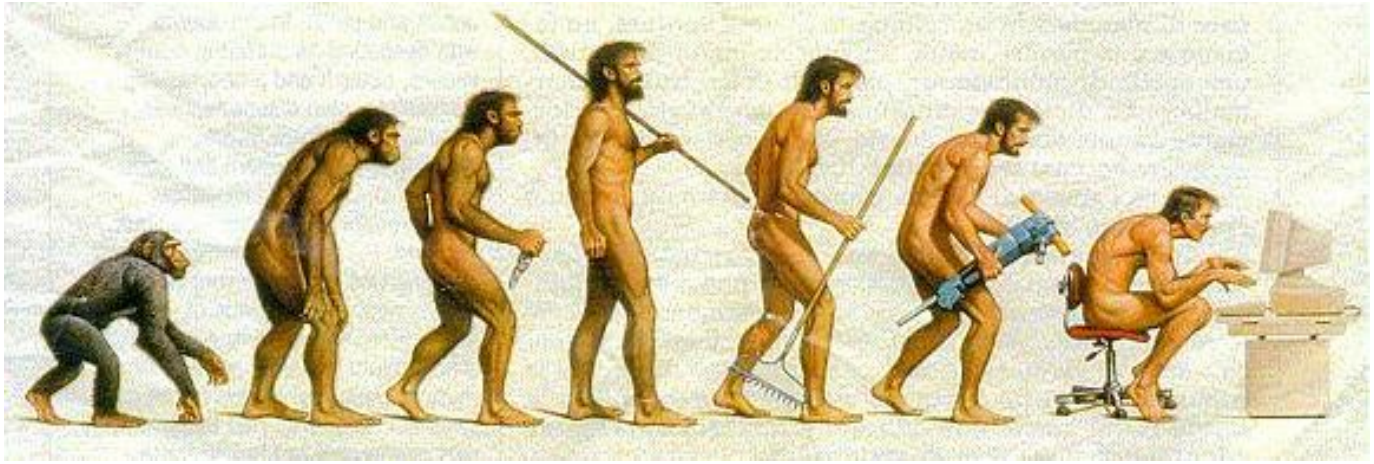
BELLEVUE UNIVERSITY

Real Learning for *Real* Life

Risky Business – The Art and Science of Security Risk Management

Ron Woerner – July 2013

Warning

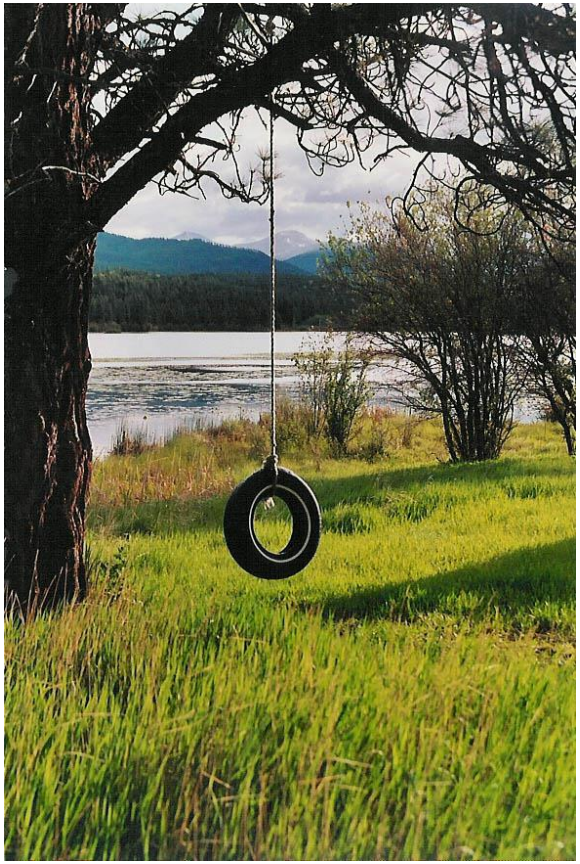


- These are my thoughts based on my studies and experiences.
- Feel free to disagree with me.
- Also make comments and ask questions.

The Bald Tire Scenario*

***From: Jack Jones, Introduction to FAIR**

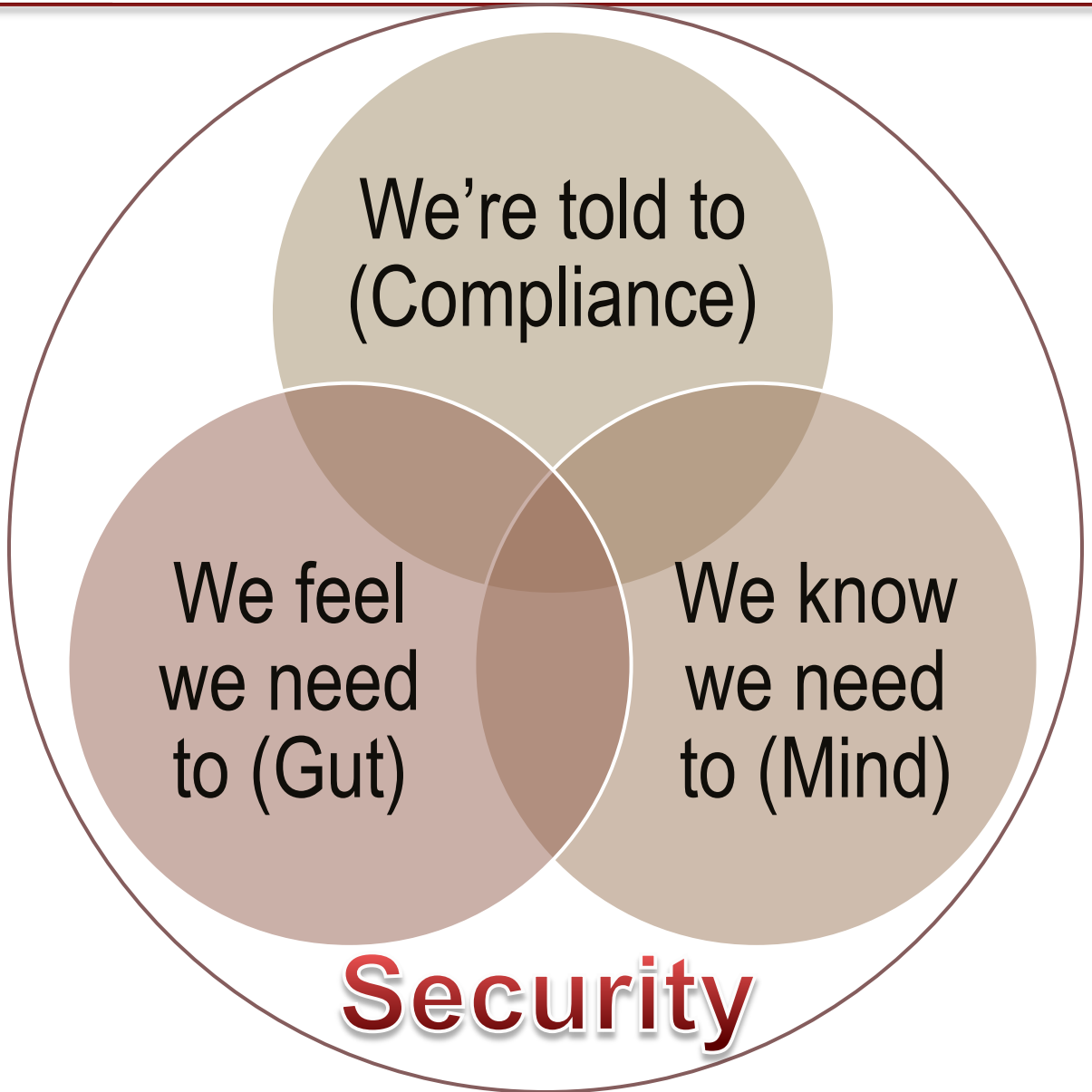
The Bald Tire Scenario*



***From: Jack Jones, Introduction to FAIR**


RISK

Why Security?



Problem with Perspective

Solution

Information Risk Management

"*Most business people are familiar with Risk Management, but few understand the emerging practice of IT Risk Management, and fewer still appreciate its role in today's connected organizations*." Symantec IT Risk Report, Feb08

What is Risk Management?

Risk – An uncertain event or condition that, if it occurs, has an impact on a project's or business' objectives.

Risk Management – **The process of:**

- **Determining an acceptable level of risk,**
- **Assessing the current level of risk,**
- **Taking steps to reduce risk to the acceptable level, and**
- **Maintaining that level of risk.**

GOAL

Informed Decisions

Why Risk Management?

- Align business risk tolerance and IT actions
- Minimize operational surprises and losses
- Proactive decision making
- Identify and manage cross-enterprise risks
- Provides a breaking mechanism
- Simplicity, Collaboration & Accountability

Where are you?

Risk Capability Maturity Model

Difference of Opinions

Feeling vs. Action

Art vs. Science

Quantitative Vs. Qualitative

Psychology of Risk

- How do people think about risk?
- 82% of sampled college students rated themselves as above average drivers.
- Components of risk behavior
  - Experiences
  - Beliefs
  - Emotions
  - Control

Psychology of Risk

Pet risks

Risk Prioritization

HOW?

Information Risk Mgt Principles

- In a nutshell:

  Risk = Impact X Probability / Cost

  [ref: United States v. Carroll Towing Co. (1947)]

- You can't mitigate a risk if you haven't identified it and don't understand it.
- There is no hiding from risks.

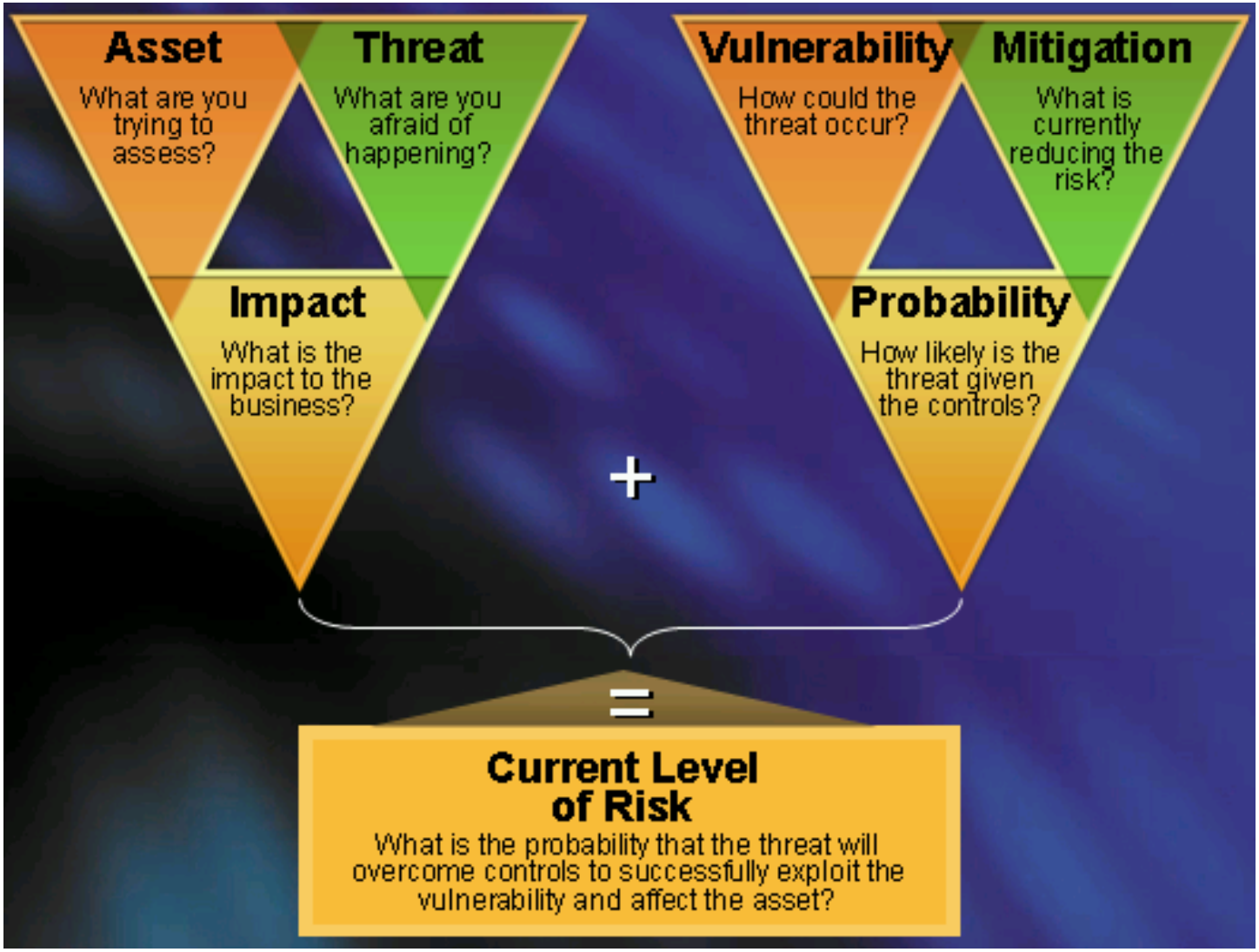
Basic Risk Management – Steps

1. Know your assets, data, services, & customers
2. Identify & assess risks, threats, & vulnerabilities
   a) Impact
   b) Likelihood
   c) Costs of mitigation ($ & time)
3. Collaborate on risk response
4. Implement controls
5. Measure residual risk
6. Rinse & repeat

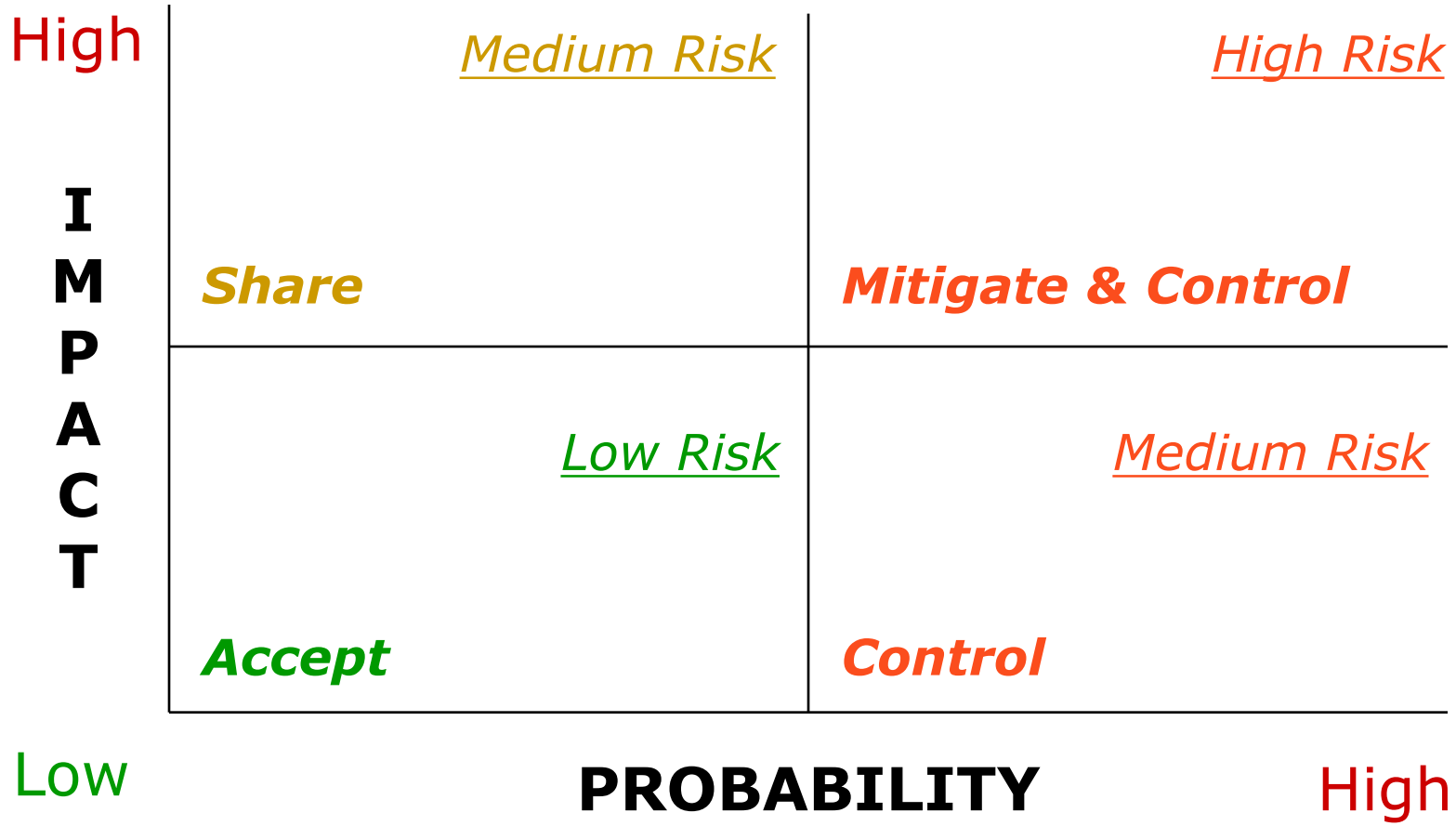
Event Identification

- Identify potential incidents or issues
- “What-if” and “worst-case” scenarios
- Consider risk categories – business processes, human, and technology (network, host, application).
- How will the threat be realized?
- Document risks, threats and vulnerabilities

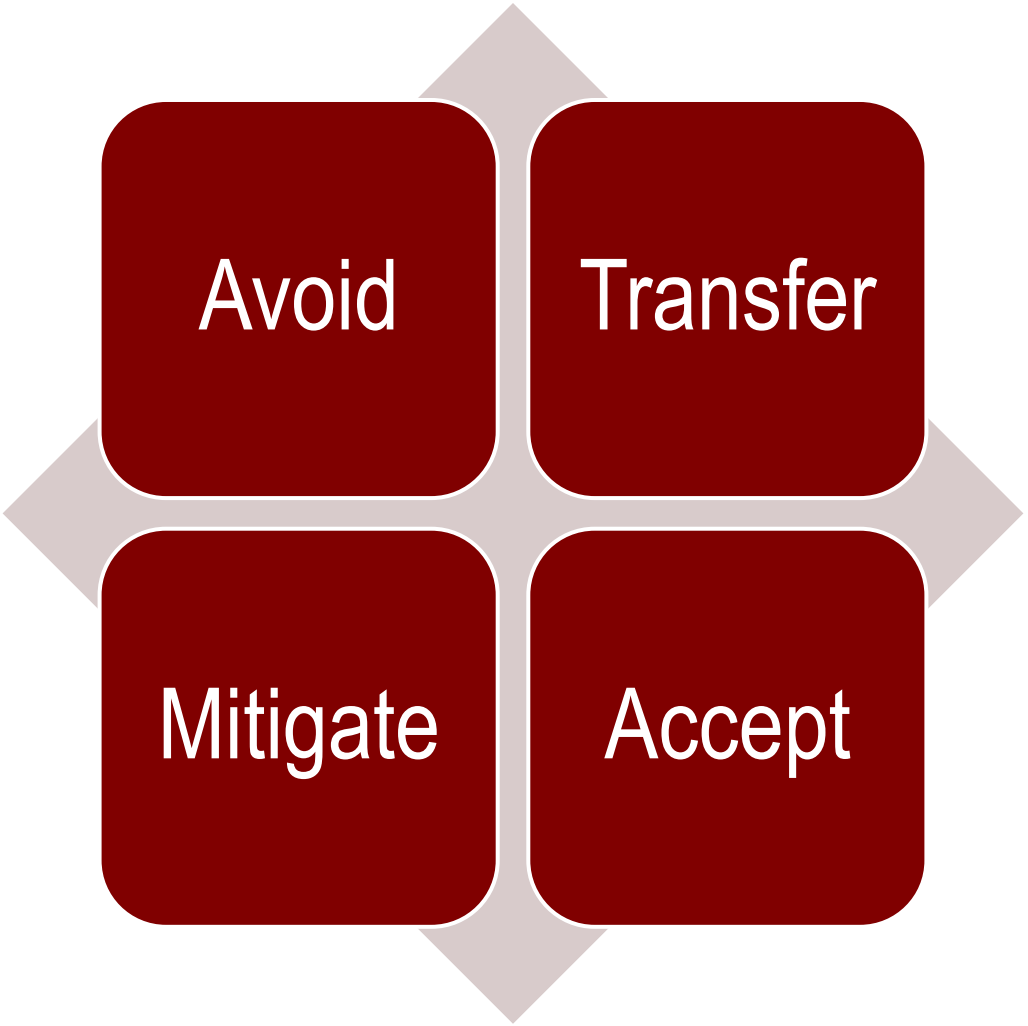
Components of a Risk Assessment



Impact & Probability



Risk Response



Risk Response

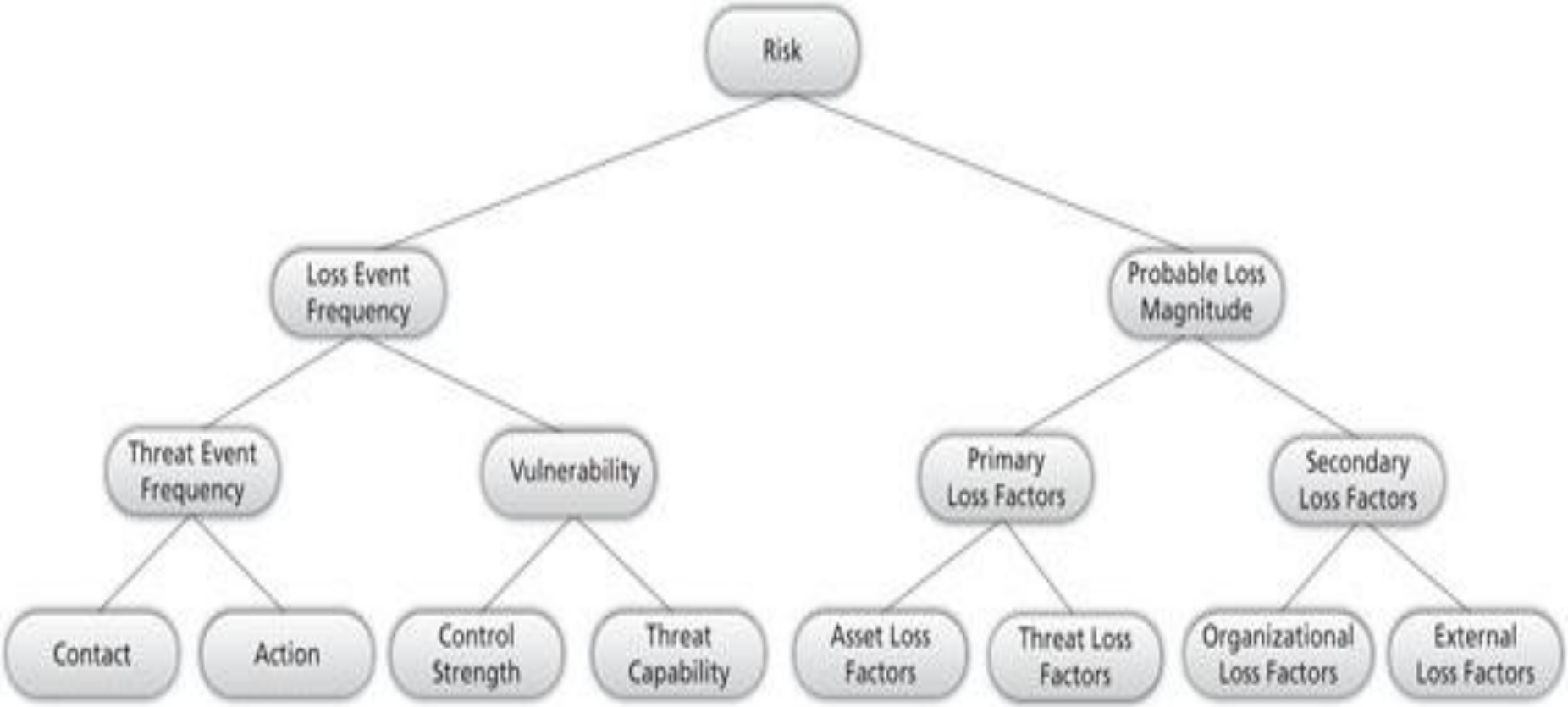
- Decide on a Mitigation Plan
  - Controls or safeguards that will lower the likelihood of occurrence, decrease the impact or minimize the risk.
  - May include accepting the risk
- Control / Safeguard types:

Policies / Standards	Procedures / Processes	Awareness / Training
Host / Network Defenses	Incident Detection	Logging / Auditing
Access Control	Password Protection	Encryption
Backup & Recovery	Patch Application	Security Software

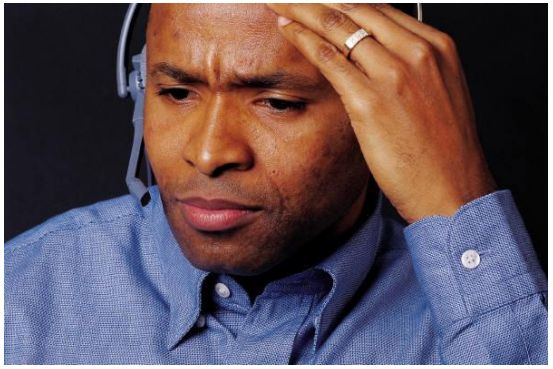
Risk Management Frameworks

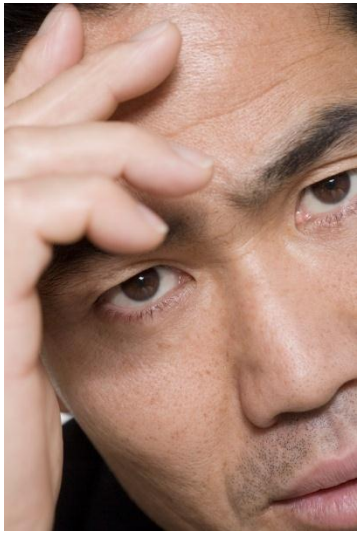
- *ISACA, Risk IT*
- IIA, *Guide to the Assessment of IT Risk (GAIT & GAIT-R)*
- *Factor Analysis of Information Risk* (FAIR), Jack Jones
- OCTAVE®, CERT
- ISO 27005, *Standard for Information Security Risk Management*, http://www.27000.org/iso-27005.htm
- NIST, Computer Security Resource Center (CSRC)
  - SP 800-30 Rev 1, Guide for Conducting Risk Assessments
  - SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

FAIR Framework



Who owns the Headache?





Take Aways

- **Understand perspective**
- **Choose an approach**
- **Risk = Impact X Probability / Cost**
- **Know, “Who owns the headache?”**
- **Collaborate on risk response**

You can either take action, or you can hang back and hope for a miracle. Miracles are great, but they are so unpredictable.

Peter F. Drucker

You'll have more fun & success helping other people achieve their goals than you will trying to reach your own goals first.

Dale Carnegie

Resources

- Society for Information Risk Analysts – https://www.societyinforisk.org/
- SIRACon, October 21-22, 2013, Seattle, WA - https://www.societyinforisk.org/content/siracon2013

Celebrate and Collaborate

ronald.woerner@bellevue.edu
http://academic2.bellevue.edu/~rwoerner
402-557-7539
@ronw123

By working together,
we all become stronger.