Advancing Information Risk Practices Seminar

Start Time	Title	Presenter
1:00 PM	Introduction	
1:05 PM	Risky Business: Quantifying Risk in the Absence of Statistical Data	Brook Schoenfield
1:55 PM	Risk Management: The Perspective of the Business Stakeholder	Doug Graham
2:45 PM	Break	
3:00 PM	Educating the Next Generation of Information Security Risk Managers	Summer Fowler
3:50 PM	Automation and Risk Management, Do They Mix?	Evan Wheeler (Moderator) Summer Fowler Doug Graham Brook Schoenfield Ben Tomhave
4:30 PM	Seminar Adjourns	

Security in knowledge

Risky Business:

Forget what you were taught, apply what you've learned

Brook Schoenfield
Principal Architect, McAfee, Inc.

Session ID: SEM-004

“Risk assessment…will identify threats to the organization’s mission; prioritize those threats into risk levels,…”

Risk Analysis Versus Risk Assessment
Thomas R. Peltier, SecureWorld Expo

“threats into risk”?
What was I thinking?!?

“Risk assessment…will identify threats to the organization’s mission; *prioritize* those threats *into* risk levels,”

Risk Analysis Versus Risk Assessment
Thomas R. Peltier, SecureWorld Expo

$\text{risk}_{\text{level}}$ = *Prioritize*(identifiedThreats[]);

"Risk assessment…will identify threats to the organization's mission; *prioritize* those threats *into* risk levels,"

Risk Analysis Versus Risk Assessment
Thomas R. Peltier, SecureWorld Expo

Infosec 101 Equation

Probability * Annualized Loss = ***Risk***

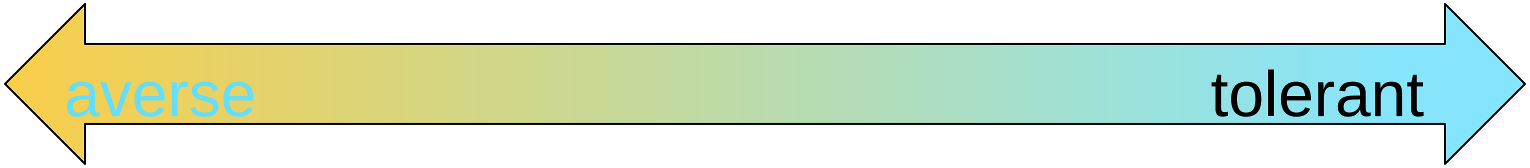
Calculates risk
based upon actuarial tables

Probability * Annualized Loss = ***Risk***

What do you actually need?

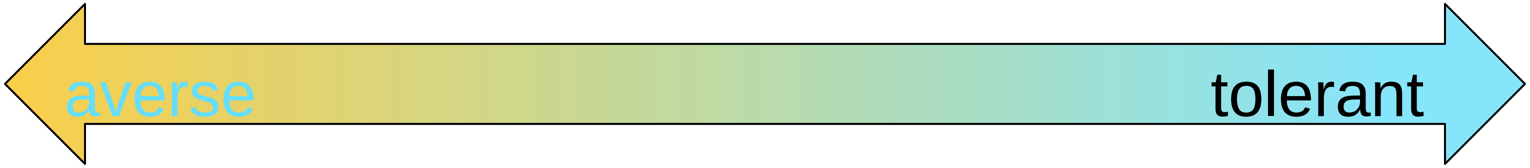
"Know Thyself"

What is your personal security posture?



“Know Thyself”

What is your personal security posture?



averse

tolerant

What posture is required?
Is mine different?

Nothing is *truly* secure. It’s all about *risk*.

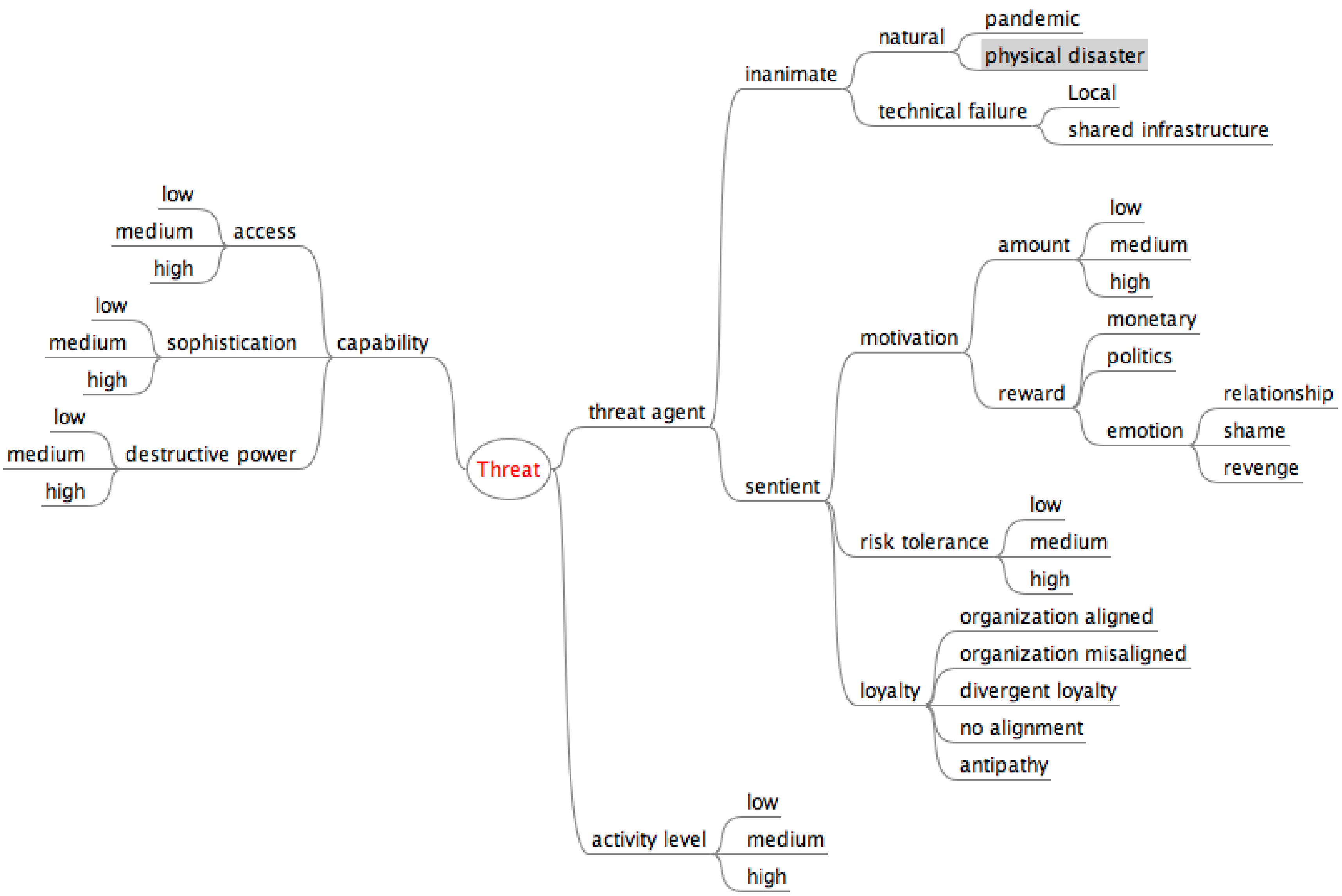
The Holy Grail

- Quantified
- Repeatable
- Useful to security
- Inform executive decisions

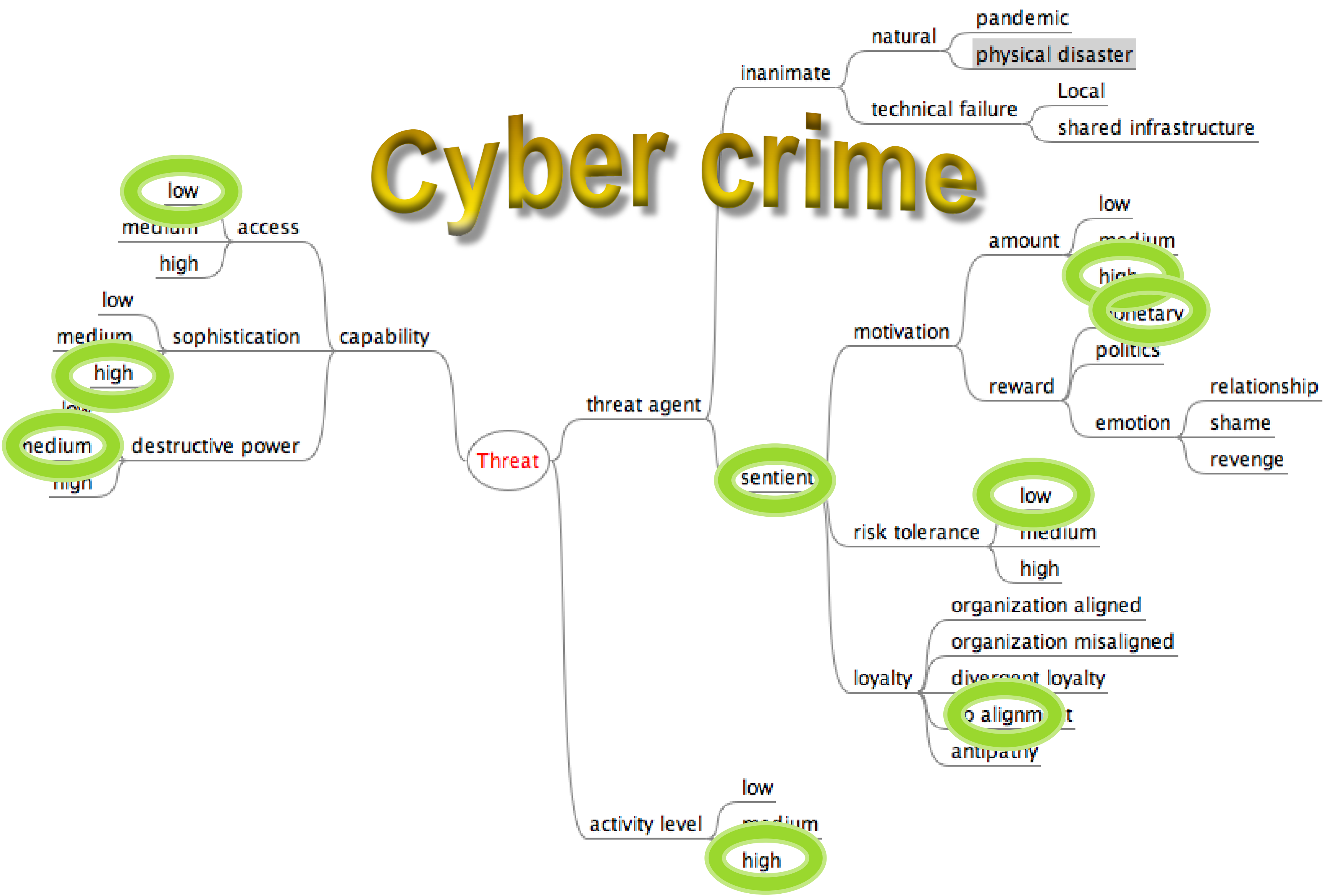
“Just Good Enough Risk Rating”

- *JGERR*: *Rigorous, lightweight risk calculation for security practitioners*

- A more precise semantic
  - articulate the components of risk
- Capture mental risk “arithmetic”
- Substitute probability

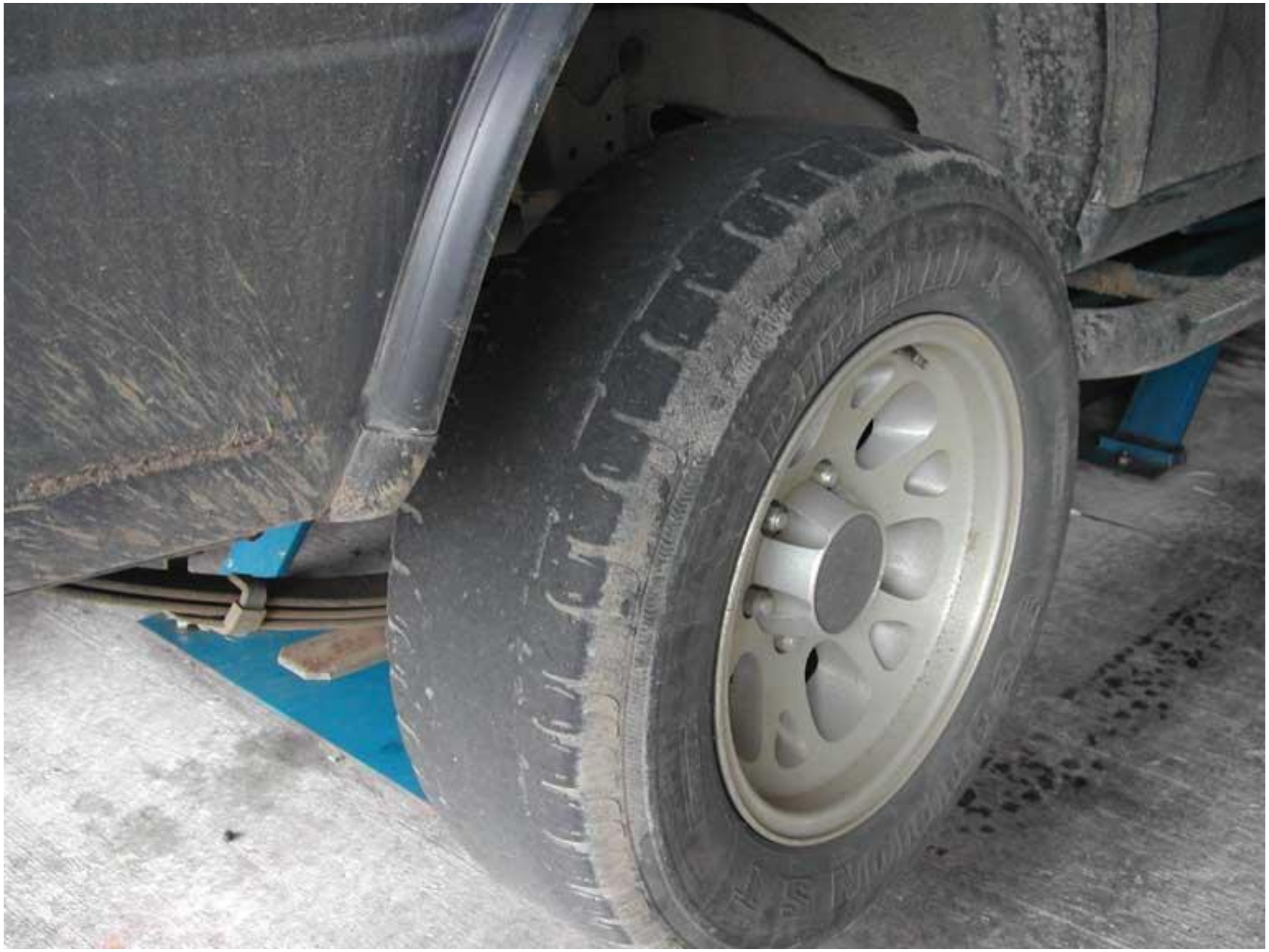

Threat
capability
access
low
medium
high
sophistication
low
medium
high
destructive power
low
medium
high
threat agent
inanimate
natural
pandemic
physical disaster
technical failure
Local
shared infrastructure
sentient
motivation
amount
low
medium
high
reward
monetary
politics
emotion
relationship
shame
revenge
risk tolerance
low
medium
high
loyalty
organization aligned
organization misaligned
divergent loyalty
no alignment
antipathy
activity level
low
medium
high

Cyber crime

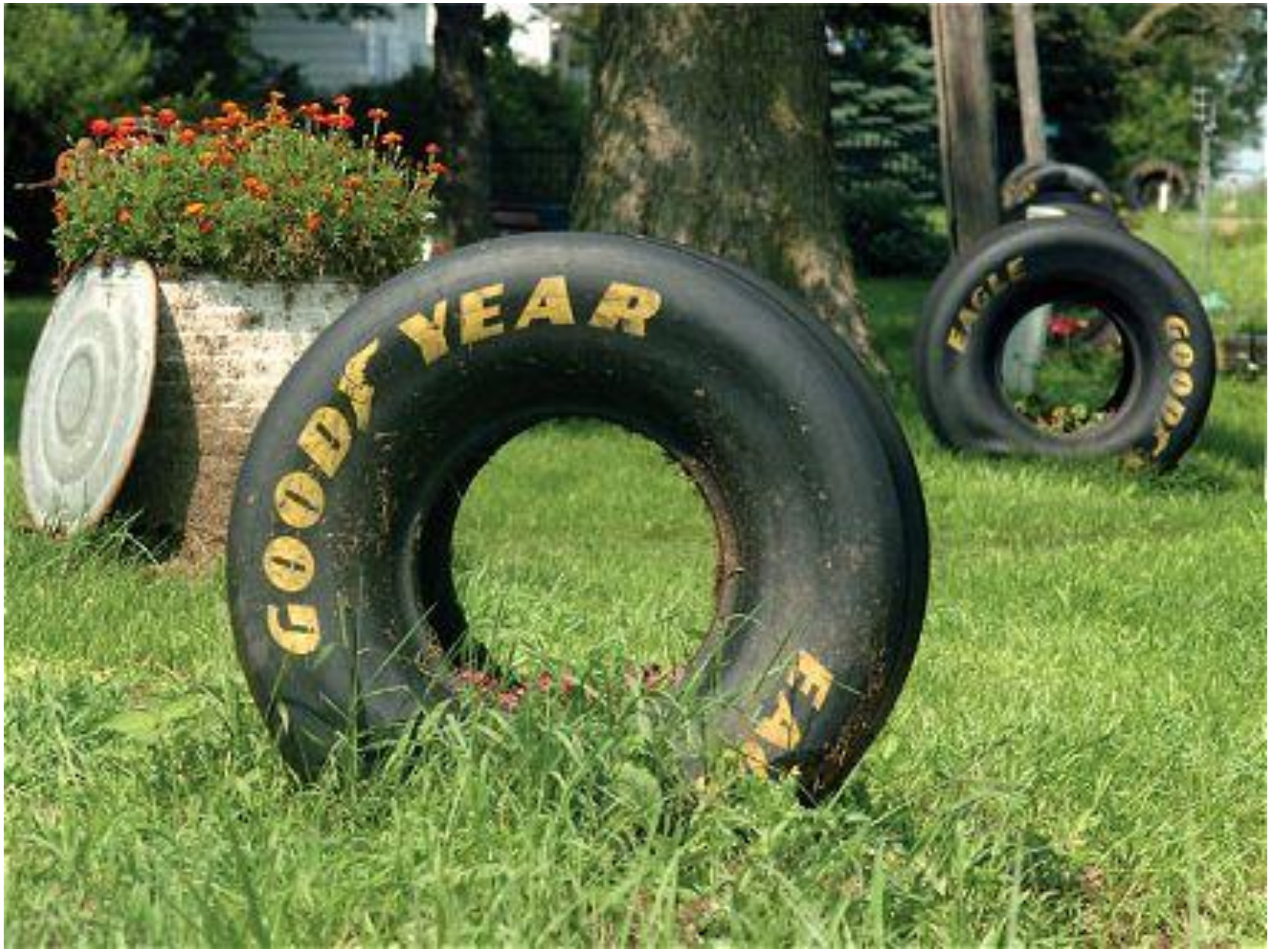


- Threat
  - capability
    - access
      - low
      - medium
      - high
    - sophistication
      - low
      - medium
      - high
    - destructive power
      - low
      - medium
      - high
  - threat agent
    - inanimate
      - natural
        - pandemic
        - physical disaster
      - technical failure
        - Local
        - shared infrastructure
    - sentient
      - motivation
        - amount
          - low
          - medium
          - high
        - reward
          - monetary
          - politics
          - emotion
            - relationship
            - shame
            - revenge
      - risk tolerance
        - low
        - medium
        - high
      - loyalty
        - organization aligned
        - organization misaligned
        - divergent loyalty
        - no alignment
        - antipathy
  - activity level
    - low
    - medium
    - high

Risk Rating, Please?



Bald Tire Risk Rating?



Risk Term	Definition
Threat	Entity that can harm
Vulnerability	Weakness that has impact
Exploit	Method to exercise a vulnerability
Exposure	Availability of vulnerability for exploitation
Impact	Damage or loss from exploitation of vulnerability by a threat

A vulnerability has risk when:

1. The vulnerability is exposed to a credible, active threat capable of exploitation[1]
2. The exercise of the vulnerability will have a significant impact

[1] "attack vector"

Attack vector:

A credible threat exercising an exploit on an exposed vulnerability

Tribal Knowledge → Attack Vectors & Impacts → Risk Assessment

- *Distill* existing security *expertise*
- Smoke out *exceptions* (to standards)
- *Separate* terms: attack vector from impact
- *Transform* knowledge into assessment questions
- *Scale (bucket-ize)* answers

Approximating Probability

0-1

Substitute Probability[1] $= 0 \leq N \leq 1$

- "Attack vector" replaces the probability term
- Scale the relative importance of each "attack vector"
  - Questions may have different combinations of the terms
- Estimation must be *reasonably* consistent
  - Generate[2] a number between 0 and 1

1. An "attack vector", as defined
2. *Garnered from a presentation at RSA*

Real World[1] Risk Calculation

estimated attack vector * *scaled* size of impact =

calculation akin to risk

[1] Information security risk assessment

Speak *Risk* to Executives

- Communicate your reasoned assessment
  - Credible active attack vectors, prioritized
  - Likelihood of occurrence
  - Technical difficulty
- Communicate your best understanding of impact
  - Impact includes business participation
  - Include the range of impacts
  - Add in additional *technically enabled* impact
- Be credible; no FUD

Let risk owner decide

Q & A

www.brookschoenfield.com
brook@brookschoenfield.com

Credits

- Rakesh Bharania & Catherine Blackadder Nelson
- Vinay Bansal & the Cisco “Web Arch” team
- Jack Jones & FAIR
- John and Ann-Marie Borrelli & the KnowledgeConnect forum participants
- That unnamed trust researcher at RSA
- The Information Security Risk Methodology working group at Cisco Systems, Inc:

Doug Dexter, Marc Passey, Richard Puckett, Jim Borne, Brook Schoenfield

Formal Definitions

Vulnerability	Any weakness, administrative process, or act or physical exposure that makes an asset susceptible to exploit by a threat
Threat	A potential cause of an unwanted impact to a system or organization. (ISO 13335-1)
Exposure	The potential damage to or loss of an asset from a given threat and/or vulnerability after consideration of existing controls
Impact	The overall (worst case scenario) loss expected when a threat exploits a vulnerability against an asset
Exploit	A means of using a vulnerability in order to cause a compromise of business activities or information security

Some Information Risk Methodologies

- CVSS: Vulnerability, exposure, some impact: technically focused
- Microsoft STRIDE: exploit, exposure, some threat - Assumes impact
- Bruce Schnier's attack tree methodology
- FAIR: Approach partly upon which JGERR is based
- The Security-specific Eight Stage Risk Assessment Methodology
- LAVA
- Vendors' tools…

RSACONFERENCE2013

Security in knowledge

RISK MANAGEMENT: THE PERSPECTIVE OF THE BUSINESS STAKEHOLDER

Doug Graham
EMC Corporation

Session ID: SEM-004

FROM A FEW TO MANY

- Security organization demand is at an all time high
  - Most organizations can't scale horizontally
  - We have more risk than we can handle
  - We need help
- Risk management must be a shared responsibility
  - Look at any large scale model e.g. personal healthcare
  - Collective responsibility is a force multiplier

COMMUNITY BASED SECURITY

- Empowers the consumers to participate in security
- Fuels organizational and operational growth
- Improves security awareness
- Enables trust in the business and it's employees
- Protects the business through confidence

REACHING THE BUSINESS

Congruity

Harmonization of thinking with the business

- Lack of alignment leads to conflicting priorities
- No connection of security goals to business objectives
- Humans will take drastic measures to remove incongruity

Consistency

Deliver clear and coherent guidelines for operations

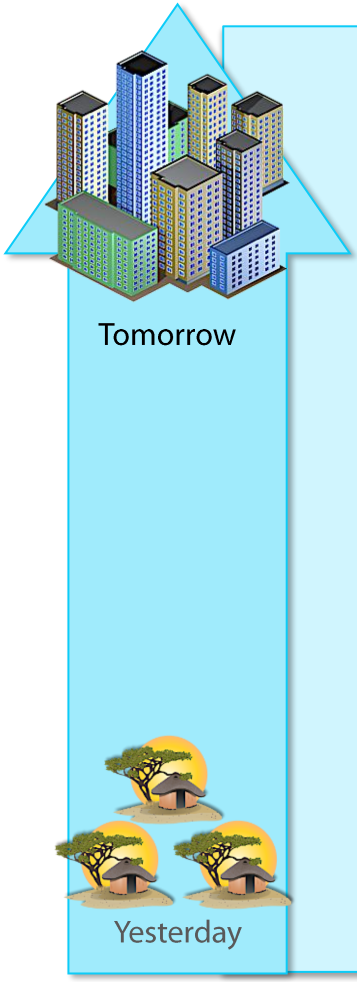
- Unclear direction results in unpredictable outcomes
- We can't measure success with different yardsticks
- Set expectations for default behaviors and actions

Necessity

People like to understand why they need to do things

- "Because I told you so" doesn't work with adults
- We want people to buy in to security rather than just accept it
- We need to justify any infringement on user freedom

BUSINESS SECURITY ENABLEMENT



Centralized

- Governance
- Foundational Controls
- Consulting
- Monitoring & Response
- Accountability
- Reporting

Federated

- Governance
- Customized Controls
- Accountability
- Reporting

Centralized

- Policy
- Foundational Controls
- Detailed Controls
- Monitoring & Response
- Accountability
- Reporting

Guiding Principles

- Maintain investment in foundations
- Risk based standard controls
- Shared security responsibility
- Security should be agile and transparent
- We must empower, enable, and protect the business
- Aim is to drive more resources focused on security

Key Considerations

- Security IS everyone's responsibility
- Accountability must be broad
- Controls must be measured and reported
- This is a cultural change

THE SECURITY LIAISON

- BSMs, ISOs, BISOs (pick what works)
- Role: **Interact** with the business
- Represent security to the business
- Represent the business to security

Interact First — Sell Second

COMMUNICATING RISK

An Industry Problem

Our language of “riskeze” isn’t getting it done!

We must understand

- How secure do we need to be?
- How secure we are?
- How do we compare to our peers?

We must communicate

- Why we need security
- How business decisions impact security
- How security decisions impact the business

Creating the Message

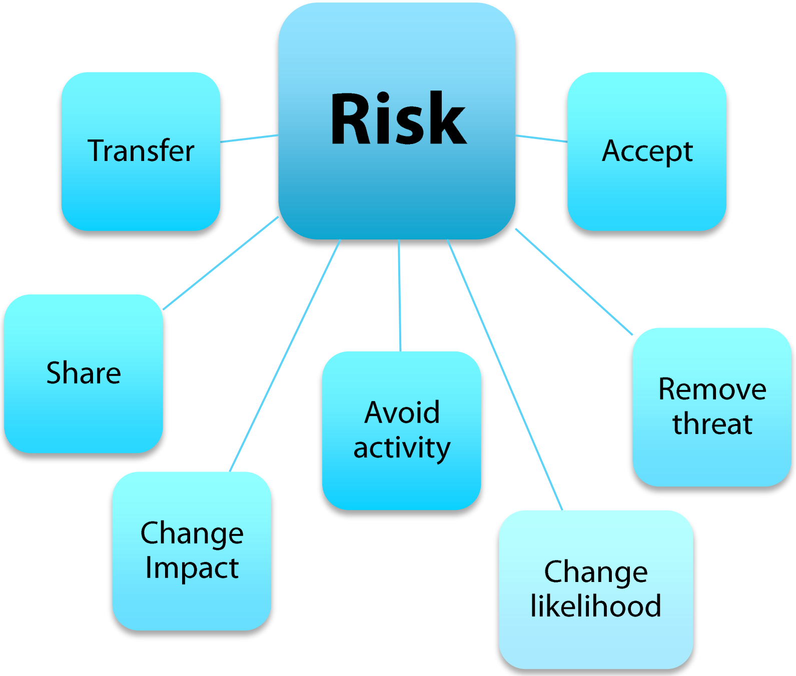
Master the ‘art’ of communication

Hints & Tips

- Don’t ‘force’ security negotiate
- Use evidence based on risk
- Use plain language
- Listen adjust and adapt

GIVING THE BUSINESS OPTIONS

Risk is a business driven function that requires a series of business decisions



How many options can we drive purely from a security perspective?

THE CORPORATE DIALOGUE

Map the risk dialogue to the business dialogue

Board of Directors

Audit Committee

- Oversee risk management

CEO Staff

- Investment Tradeoffs
- Prioritization
- Board of Directors Communication

Management Risk Committee

- Monitor, manage and report on enterprise risk management program

BU's and Functions

- Develop strategy
- Identify BU/function Specific Risks
- Define Mitigation Plans
- EVP Awareness

GRC Council

- Create Mandate for Risk Assessments
- Communication to BU's and Functions
- Assess and Prioritize Risk Activities
- Collate and Report
- Budget and Planning of Mitigation

GUIDING PRINCIPLES

1. Formalized Interaction	▶ Clearly define and communicate liaison roles ▶ Establish formal interaction processes ▶ Ensure that senior leadership has visibility about the role
2. Integrated Workflows	▶ Identify touch points and ways to integrate the liaison role into key business and security activities
3. Streamlined Responsibilities	▶ Narrow the breadth of the liaison role by: ▶ Pairing liaisons with other staff ▶ Removing delivery responsibility
4. Community of Liaisons	▶ Keep liaisons connected ▶ Shared goals and methodologies
5. Focus on the soft skills	▶ Develop two-way communication skills, and business logic

RSACONFERENCE2013

SEM-004: ADVANCING INFORMATION RISK PRACTICES SEMINAR

EDUCATING THE NEXT GENERATION OF INFORMATION SECURITY RISK MANAGERS

Summer C. Fowler
Carnegie Mellon University
Software Engineering Institute
CERT™

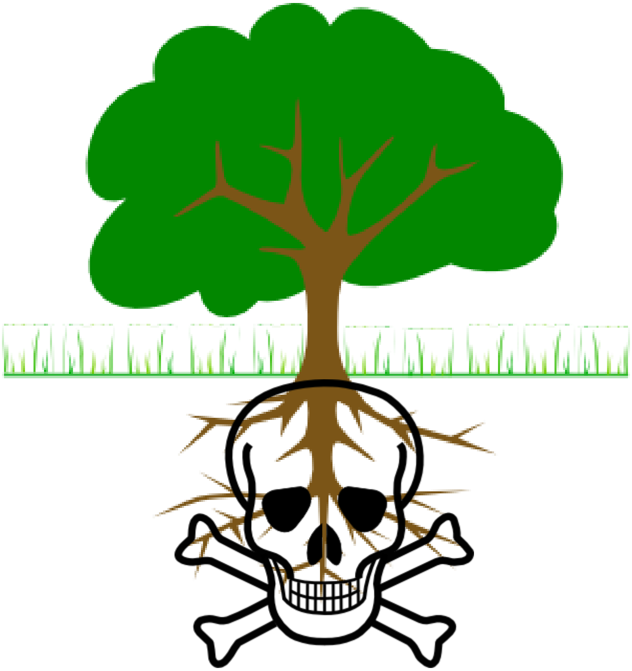
Security in knowledge

Agenda – more than an education

- Perception & "Constructive Paranoia"
- Risky Business
- United Nations of Risk
- Exercise IS good for you
- Heading in the Right Direction
- Risks are Realized – Resilience Rules!

Did You Shower Today?

- Perception == Reality?
  - Standards and guidelines recommend risk-based approaches to information security
  - Calculations for likelihood and impact of risk differ greatly
  - Perceived Risk versus Computed Risk



Perceived Risk vs. Computed Risk

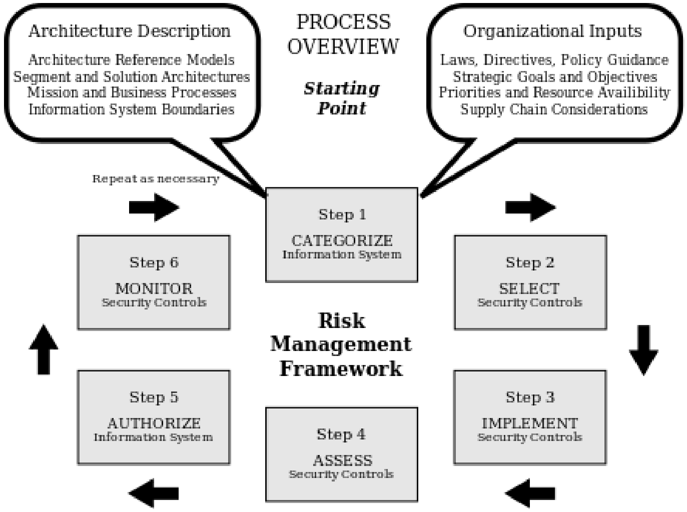
- Perceived Risk is a Psychological Construct
  - Endogenous factors (attitudes, beliefs)
  - Exogenous factors (environmental circumstances)
  - Measured indirectly by the aggregation of several underlying factors
- Computed Risk
  - Risk = Likelihood x Impact
  - Frequently recommended to conduct “risk assessments”

Concept of “constructive paranoia” embraces perceptions of risks

Get Nosy – Risky Business is YOUR Business

- Risk isn't just a concern for the Risk Manager
  - Universities are offering courses in Risk Management
    - In three years, CMU's offering went from 30 students in technical programs to over 130 students from ALL majors

Where is your role in this framework?



The Risk Management Framework (NIST Special Publication 800-37).

Definitions of Risk

Risk is the potential that a chosen action or activity (including the choice of

Risk: the variability in possible outcomes, usually in reference to the possibility of negative results

Risk can be seen as relating

HUNDREDS OF DEFINITIONS

Risk is the

probability of a hazard resulting in an adverse event, times the severity of the event

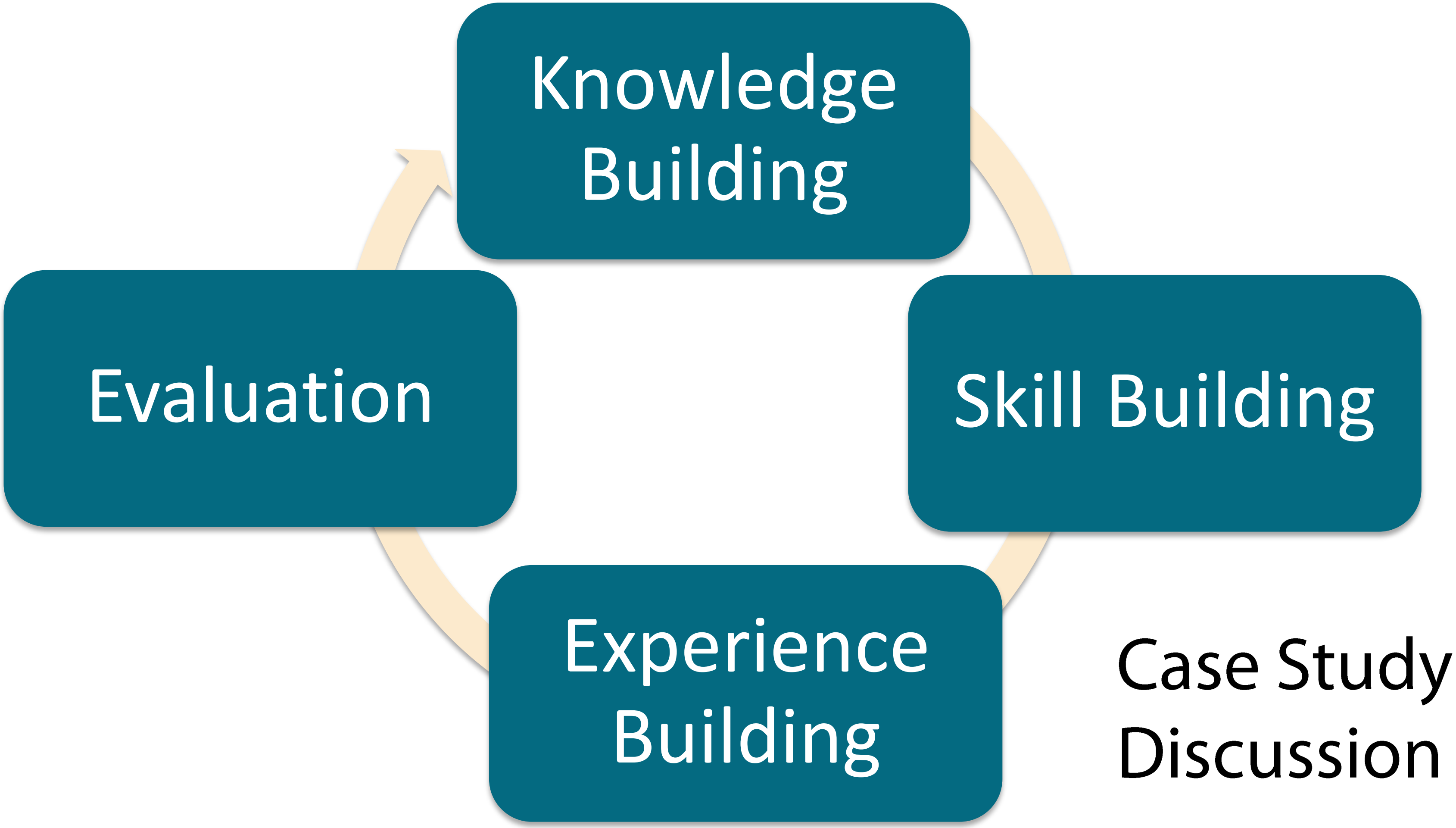
threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

© EPA

Anyone Have An Interpreter?

- For Information Security Risk Management to mature, we need a risk taxonomy
  - Other fields that do this well: Medical, Construction
  - Until the field converges, your company can adopt/create a dialect!
    - **ISO31000: 2009 Risk Management Standard**
    - **National Initiative for Cybersecurity Education (Cybersecurity Workforce Framework)**

Give a man a risk or teach him how to manage risk?


Knowledge Building

Skill Building

Experience Building

Evaluation

Case Study Discussion

Not just *how* to teach, but *what* to teach

- Comprehensive National Cybersecurity Initiative resulted in NICE Cybersecurity Workforce Framework
  - Developed by over 20 Federal D/As & 18 non-profit/GO’s
- Organized cybersecurity discipline into seven high-level categories with specialty areas
  - Roles for Risk and Vulnerability Analyst and Risk Executive, e.g.
  - Over 100 references to RISK in the framework
  - KSAs provided for specialty areas

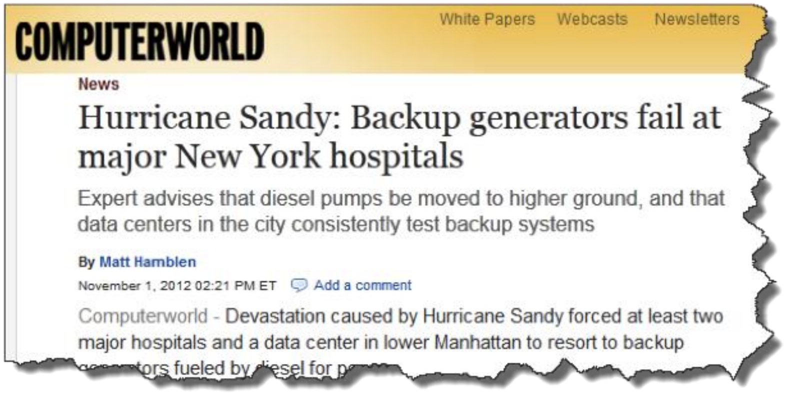
http://csrc.nist.gov/nice/framework/

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

It Happens…How Will You Respond?

- Hurricane Sandy:
  - Expected: Wind damage, Loss of Power, Need for Generators
  - Unexpected: Failures, Blizzard, Fires



COMPUTERWORLD

White Papers Webcasts Newsletters

News

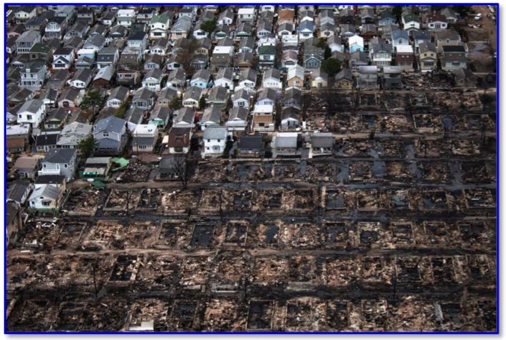
Hurricane Sandy: Backup generators fail at major New York hospitals

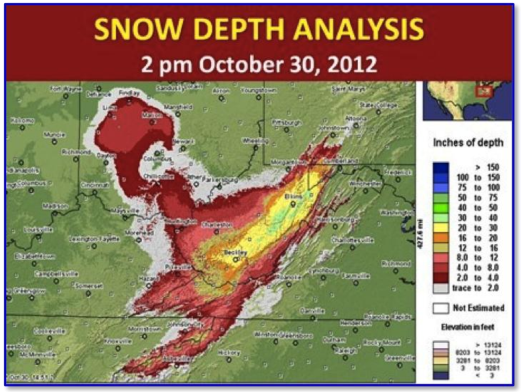
Expert advises that diesel pumps be moved to higher ground, and that data centers in the city consistently test backup systems

By Matt Hamblen

November 1, 2012 02:21 PM ET Add a comment

Computerworld - Devastation caused by Hurricane Sandy forced at least two major hospitals and a data center in lower Manhattan to resort to backup generators fueled by diesel for p





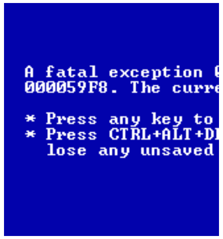
SNOW DEPTH ANALYSIS

2 pm October 30, 2012

From Risk to Resilience

- Operational resilience: The emergent property of an organization exhibited when it continues to carry out its mission after disruption that does not push it beyond its operational limit [CERT®-RMM]

Actions of people



```
A fatal exception 0
000059F8. The curre

* Press any key to
* Press CTRL+ALT+DE
  lose any unsaved
```

Systems & technology failures

Failed internal processes

External events

QUESTIONS?

Security in knowledge

AUTOMATION AND RISK MANAGEMENT, DO THEY MIX?

MODERATOR:

Evan Wheeler

Omgeo

PANELISTS:

Brook Schoenfield

McAfee, Inc.

Doug Graham

EMC Corporation

Summer Fowler

CERT

Ben Tomhave

LockPath

Discussion Topics