

# Risks Threats and Vulnerabilities

The Fundamentals of R-T-A

# Agenda

- Analysis vs. Assessment
- Risks
- Threats
- Vulnerability
- The Flow of R-T-A



# Analysis vs. Assessment

- An assessment is more of a general comparison of something to a standard, or between two something; which is better, more correct, which is closer to the color teal.
- An analysis requires deep scrutiny and calculated measuring and recording of criteria.
- An assessment is not exact, an analysis is more precise and less general than an assessment.



# HAZARDS

- Existing condition or possible (under current conditions) situation that **has the potential to generate a disaster**
- Natural hazards – naturally occurring phenomena – weather, topographic, geological, hydrological, etc.
- Human systems developed – caused by human activity, infrastructure, transportation, etc.
- Conflict based – civil war, terrorism, nuclear war, etc.



# HAZARDS - Examples

- Hurricanes and tornadoes during their seasons
- Earthquakes
- High hazard, poorly maintained dams
- Airlines with abysmal safety records
- Power production systems with either dangerous technologies or poorly maintained transmission systems

# Disasters

- The Highest DEGREE of any HAZARD...



# Risk

- The probability that a particular threat will exploit a particular vulnerability
- Need to systematically understand risks to a system and decide how to control them.
- Risk = Probability x Impact



# Examples of Risk

- **Overreliance on security monitoring software**
- **Inadequate system logging**
- **Technology innovations that outpace security**
- **Outdated operating systems**
- **Lack of encryption**
- **Data on user-owned mobile devices**
- **IT “diplomatic immunity” within your organization**
- **Lack of management support**
- **Challenges recruiting and retaining qualified IT staff**
- **Segregation of duties**



# Threat

- An expression of intention to inflict evil injury or damage
- Attacks against key security services
  - Confidentiality, integrity, availability
- The operationalization of vulnerability, expected impact of a developing hazard, and the probability that impact will work against your vulnerabilities
- Threat means something bad is coming your way – high threat means it is highly likely to hit you and it will be very bad



# Example Threat List

- T01 Access (Unauthorized to System - logical)
- T02 Access (Unauthorized to Area - physical)
- T03 Airborne Particles (Dust)
- T04 Air Conditioning Failure
- T05 Application Program Change (Unauthorized)
- T06 Bomb Threat
- T07 Chemical Spill
- T08 Civil Disturbance
- T09 Communications Failure
- T10 Data Alteration (Error)
- T11 Data Alteration (Deliberate)
- T12 Data Destruction (Error)
- T13 Data Destruction (Deliberate)
- T14 Data Disclosure (Unauthorized)
- T15 Disgruntled Employee
- T16 Earthquakes

- T17 Errors (All Types)
- T18 Electro-Magnetic Interference
- T19 Emanations Detection
- T20 Explosion (Internal)
- T21 Fire, Catastrophic
- T22 Fire, Major
- T23 Fire, Minor
- T24 Floods/Water Damage
- T25 Fraud/Embezzlement
- T26 Hardware Failure/Malfunction
- T27 Hurricanes
- T28 Injury/Illness (Personal)
- T29 Lightning Storm
- T30 Liquid Leaking (Any)
- T31 Loss of Data/Software
- T32 Marking of Data/Media Improperly
- T33 Misuse of Computer/Resource
- T34 Nuclear Mishap

- T35 Operating System Penetration/Alteration
- T36 Operator Error
- T37 Power Fluctuation (Brown/Transients)
- T38 Power Loss
- T39 Programming Error/Bug
- T40 Sabotage
- T41 Static Electricity
- T42 Storms (Snow/Ice/Wind)
- T43 System Software Alteration
- T44 Terrorist Actions
- T45 Theft (Data/Hardware/Software)
- T46 Tornado
- T47 Tsunami (Pacific area only)
- T48 Vandalism
- T49 Virus/Worm (Computer)
- T50 Volcanic Eruption

# Characterize Threat-Sources

<b>Threat-source</b>	<b>Motivation</b>	<b>Threat Actions</b>
<b>Hacker</b>	Challenge, ego, rebellion	Hacking Social engineering System intrusion Unauthorized access
<b>Terrorist</b>	Blackmail, Destruction, Revenge	Information warfare System attack System tampering
<b>Insider</b>	Ego, Revenge, Monetary gain	Blackmail Malicious code Input of falsified data System bugs

# VULNERABILITIES

- If you have a hazard you may or may not be vulnerable to it
  - Live in the flood plain – vulnerable to floods
  - Live on high ground – not vulnerable to floods
- Vulnerability is an assessment of how well or how poorly protected you are against an event
- Vulnerabilities are flaws / weaknesses in any system which can be utilized to generate “Threat”

# Vulnerabilities

- Flaw or weakness in system that can be exploited to violate system integrity.
  - Security Procedures
  - Design
  - Implementation
- Threats trigger vulnerabilities
  - Accidental
  - Malicious



# VULNERABILITIES

- Vulnerabilities may be reduced by mitigation measures (building construction, land use control, maintenance, etc.)
- Or by the level of preparedness you have achieved (well trained and equipped emergency teams, plans, exercises, etc.)

# Factors influencing VULNERABILITY

- Three factors may influence the determination of vulnerability
  - Criticality – how important is the asset or function that is subject to impact
  - Exposure – to how much of the force of the event is the resource exposed
  - Time – does vulnerability fluctuate over time of day, month, season?

# Examples of Vulnerabilities

## •Physical

- V01 Susceptible to unauthorized building access
- V02 Computer Room susceptible to unauthorized access
- V03 Media Library susceptible to unauthorized access
- V04 Inadequate visitor control procedures
- (and 36 more)
- Administrative
- V41 Lack of management support for security
- V42 No separation of duties policy
- V43 Inadequate/no computer security plan policy

- V47 Inadequate/no emergency action plan
- (and 7 more)
- Personnel
- V56 Inadequate personnel screening
- V57 Personnel not adequately trained in job
- ...
- Software
- V62 Inadequate/missing audit trail capability
- V63 Audit trail log not reviewed weekly
- V64 Inadequate control over application/program changes

## Communications

- V87 Inadequate communications system
- V88 Lack of encryption
- V89 Potential for disruptions
- ...
- Hardware
- V92 Lack of hardware inventory
- V93 Inadequate monitoring of maintenance personnel
- V94 No preventive maintenance program
- ...
- V100 Susceptible to electronic emanations



# IMPACT

- Assessment of interaction of hazard effects with your vulnerabilities
- Scalar based on the two key variables – hazard strength and vulnerability level
- Will be hazard specific in aggregate (hurricane impacts), but may be functionally common to a variety of hazards in the specific (power loss)



# IMPACT

## MODERATE

Strong Hazard  
Low Vulnerability

## HIGH

Strong Hazard  
High Vulnerability

## LOW

Weak Hazard  
Low Vulnerability

## MODERATE

Weak Hazard  
High Vulnerability

# Factors influencing IMPACT

- Two other factors are related to impact
  - Magnitude – the absolute size and power of the event
  - Intensity – the measurement of the effects of the event – how it is felt
- All else being equal an event with greater magnitude will tend to be a more intense event and generate greater impacts

# CONSEQUENCES

- Result of the interaction of the Impact of the event with other systems
  - Political,
  - Social and cultural,
  - Economic, etc.
- May set the stage for either:
  - Future events, or
  - Vulnerability reduction through mitigation and preparedness

# CONSEQUENCES

- The border between consequence and impact is fuzzy, but
  - Impacts tend to be directly related to the effects of the event, consequences more second order
  - Impacts tend to be shorter term (hours to decades), consequences longer term (weeks to centuries)
  - Although coupled to impacts, consequences are neither automatic nor irreversible
  - Consequences tend to be more human-centric, impacts more event-centric – we make the consequences, the event makes the impact

# PROBABILITY

- A mathematical assessment of how likely it is that a specific event will occur
- Based on a wide variety of factors – history, global warming, infrastructure and demographic changes, new industries, changes in your activities and processes, etc.

# PROBABILITY

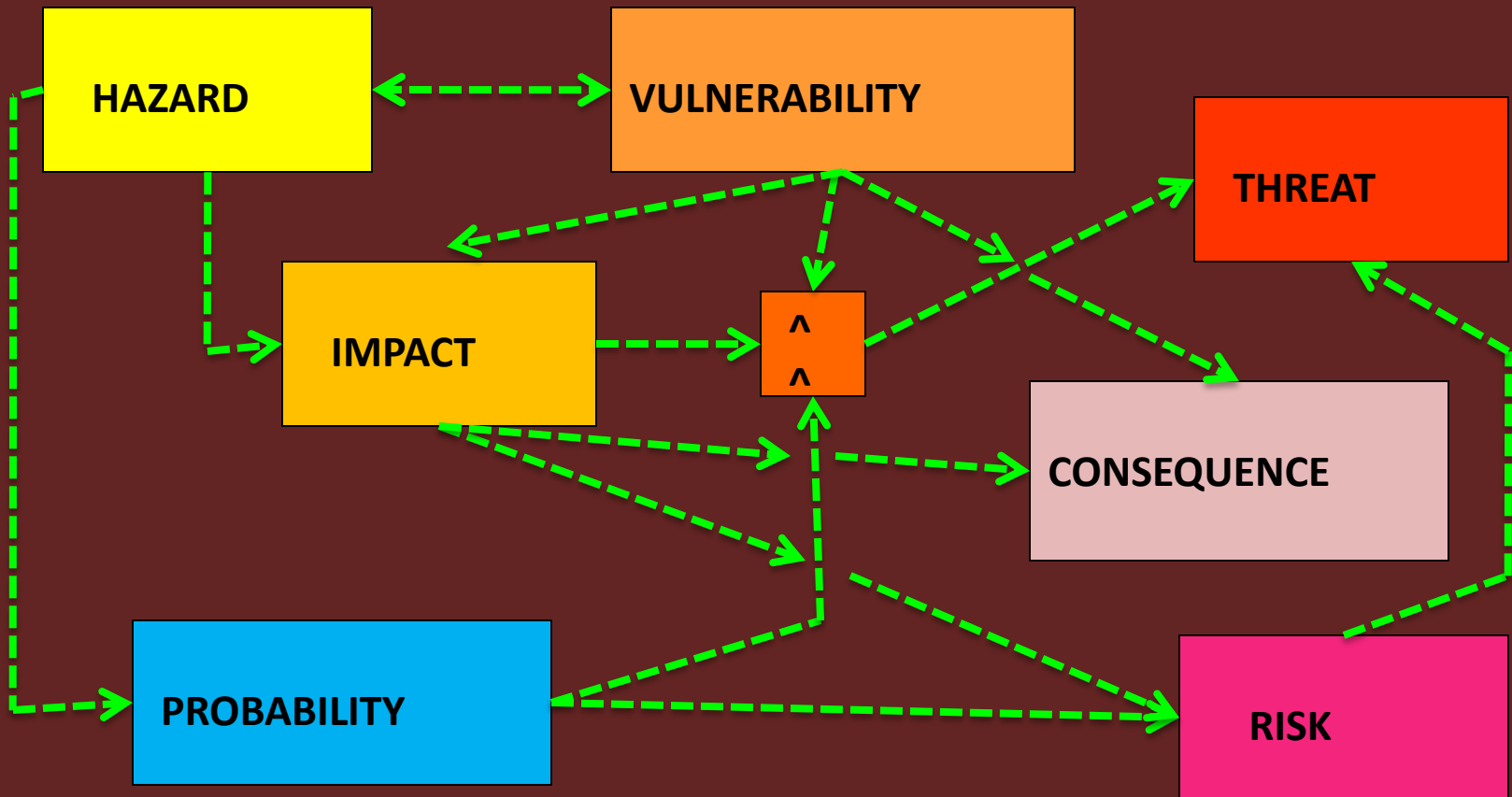
- Expressed in a variety of ways:
  - This year we expect 14 named tropical storms, 8 hurricanes, 3 great hurricanes ... (an assessment of general level)
  - There is a 45% chance of ... (a numerical assessment)
  - A 500 year flood ... (a statement of cycles)
  - And then there is likelihood: “I think it is highly likely that ...” (a qualitative assessment)

# LIKELIHOOD

- An inexact, qualitative statement of how one assesses probability
- Generally expressed in broad bands that cover a range of probability values
  - High – “likely”
  - Low – “unlikely”
- Easily understood, but also misleading – likely is interpreted as “yes, it will,” unlikely as “no, it will not”



# THE FLOW



# Asset, Vulnerability, Threat, Risk & Control

- **Asset**= anything has value to the organization
- **Vulnerability**= any Weakness of Asset
- **Threat**= any possible Danger
- **Risk**= Vulnerability exposed to Threat  
**Risk**= Vulnerability X Threat
- **Control**= Countermeasure to reduce Risk

Here are some important characteristics of the three components:

- **Threats (effects) generally can NOT be controlled.**

One can't stop the efforts of an international terrorist group, prevent a hurricane, or tame a tsunami in advance. Threats need to be identified, but they often remain outside of your control.

- **Risk CAN be mitigated**

Risk can be managed to either lower vulnerability or the overall impact on the business.

- **Vulnerability CAN be treated**

Weaknesses should be identified and proactive measures taken to correct identified vulnerabilities.