Uncertainty as a Factor of Risk

ConSec '12

Austin, Texas

September 18th, 2012

Brian A. Engle

Chief Information Security Officer

Texas Health and Human Services

Agenda

- Risk Defined
- Risk Factors
- Uncertainty – The Case for Quantifying Risk
- Un-FUD'ed Uncertainty – Remove Fear Doubt
- Stalemate Removal – BYOD Example

Risk Defined

1. A probability or threat of a damage, injury, liability, loss, or other negative occurrence that is caused by external or internal vulnerabilities, and that may be neutralized through preemptive action.
2. Finance: The probability that an actual return on an investment will be lower than the expected return.

http://www.businessdictionary.com/definition/risk.html#ixzz255Kw3iSy

Risk Math

Composite Risk Index =
Impact of Risk event x Probability of Occurrence

Risk = Impact X Probability

Risk Factors

- Probability (Likelihood of Occurrence)
- Threat (Threat Agent, Threat Actor)
  - Motivation, Capability
- Vulnerability (Exposure, Weakness)
- Impact (Damage, Injury, Liability or Loss)
- Asset (Items, Valuables)
- Preemptive Actions (Countermeasures, Controls)
- Frequency (Rate of Occurrence)
- Secondary Factors (Contributors to value or impact)

Secondary Risk Factors

- Regulatory Compliance Requirements
- Service Dependency
- Financial Value
- Confidentiality
- Integrity
- Availability
- Loss Magnitude

Risk Math

Risk = Probability X Impact

Probability

- Threat
- Vulnerability
- Motivation
- Capability
- Preemptive Actions

Impact

- Asset Value
- Frequency
- Secondary Factors

Risk Math

Probability = Threat X Vulnerability

Threat = Capability X motivation

Vulnerability = Control Deficiency

Vulnerability {Presence} AND {Preemptive Action ability to withstand threat agent[s] capability and motivation}

Risk Math

Impact = Asset Value X Frequency X Loss Magnitude

Asset Value =

Confidentiality Rating + Integrity Rating + Availability Rating

X Regulatory Compliance Rating

X Service Dependency Factor

X Financial Factor

Risk Math

Risk = [Asset Value X Frequency X Loss Magnitude] X [Capability X motivation X Control Deficiency]

*Using Percentages means that the smaller the number, the lower the risk

**Mathematical principle, multiply by 0, answer is 0

Voodoo Risk Math

"When you deal with events that have a very, very high damage [amount], and a very, very low probability of occurrence, you multiply infinity by zero and get whatever you want."

-Bruce Schneier

#Securityism 3 – Quote the Bruce

Risk Factors

Uncertainty

Risk Math

Risk = Probability X Impact

X

Uncertainty?

Risk Math

Risk = [Asset Value X Frequency X Loss Magnitude] X [Capability X motivation X Control Deficiency]

X

Uncertainty?

Risk Math

Risk =

[Asset Value - uncertainty X

Frequency - uncertainty X

Loss Magnitude - uncertainty] X

[Capability - uncertainty X

motivation - uncertainty X

Control Deficiency - uncertainty]

UnFUD'ed Uncertainty

Remove Fear and Doubt

- Isolate factors
- Measure what can be measured
- Estimate and approximate with disclosure
- Use ranges and confidence levels/error margin
- Create your own actuarial data

Limiting Uncertainty

Threat Actors

- Users
  - Privileged and Unprivileged
  - Customers, Partners, Visitors
- External Parties
  - Hackers, Attackers
  - Others
- Malicious Software
- Environmental Conditions

Limiting Uncertainty

Threat Actor Capability

- Move past what is possible to what is likely
- Consider percentages of a threat population
- Time
- Resources and Costs
- Skills

Control Deficiency

Control Deficiency	Description
100%	No Controls implemented, no detective measures. Processes do not exist.
75%	Detective control, but no preventative control. Processes are ad hoc or not well defined.
60%	Single untested control. Infrequent processes performed.
50%	Single control tested as effective for some but not all conditions.
40%	Single control tested as effective for most but not all conditions.
30%	Multiple controls implemented but not completely tested.
20%	Highest levels of controls implemented in layers, tested to be effective. Infrequent ongoing detective processes performed.
10%	Highest levels of controls implemented in layers, tested to be effective. Ongoing detective measures have been implemented.
1%	Highest levels of controls implemented in layers, tested to be effective against all conceivable conditions. Continual monitoring processes have been implemented and have reached a mature state of continuous improvement.

Limiting Uncertainty

Asset Value - Confidentiality Rating

5 - The system contains, processes, or has access to "Organization Confidential Data"

3 - The system contains, processes, or has access to "Organization Sensitive Information"

(Not for public consumption)

1 - The system contains, processes, or has access to "Publicly Available Information"

Limiting Uncertainty

Asset Value - Integrity Rating

5 - Information can not be invalid under any circumstances

3 - Information can be incomplete or contain some invalid data and be tolerated by the system

1 - The system contains, processes, or has access to Publicly Available Information

Limiting Uncertainty

Asset Value – Availability Rating

Base on mission criticality, tie to revenue generation, etc.

5 - Critical availability classification

3 - Necessary availability classification

1 - Deferrable availability classification

Limiting Uncertainty

Loss Magnitude (1% - 100%)

The magnitude of system loss experienced if a threat is successful in harming a system with an action. Because loss can come in a variety of flavors ranging from system performance degradation to complete loss of system response, damage is typically associated with availability of a system.

It is difficult to say that a breach of confidentiality if it were to occur would be measured in terms of a percentage. If an incident were to occur that resulted in data leakage of some sort, confidentiality may be measured by how much data was lost.

Stalemate Removal – BYOD Example

Risk Math

Risk =

[Asset Value

X Frequency%

X Loss Magnitude%]

X [Capability%

X motivation%

X Control Deficiency%]

REWARD

THE BENEFIT SIDE OF THE RISK DICE

Risk and Uncertainty - Summary

- Risk and Uncertainty will always exist
  - Do not seek to remove them, instead frame them
- Risk and Uncertainty will never be zero
  - Reduce, and define when to quit trying
- Discomfort is a fundamental driver for change
  - Illuminate risk, clarify uncertainty
  - Change will follow

About…

Capitol of Texas ISSA

The preeminent trusted global information security community

http://www.austinissa.org @austinissa

COMMUNITY -- KNOWLEDGE -- LEARNING -- CAREER

HHSC

HHSC oversees the operations of the health and human services system, provides administrative oversight of Texas health and human services programs, and provides direct administration of programs.

$30B/Year - 200 programs - 56,000 Employees – 1,000 locations - 5 agencies Serving the citizens of Texas

HACKFORMERS

Teach Security, Teach Christ; Teach Security In Christ

http://www.hackformers.org @hackformers

Thank You!

Questions?

Contact Info:

Brian.Engle@hhsc.state.tx.us

@brianaengle

www.infosec-land.com