

Modern Cyber and Technology Risk Measurement

Jack Jones
Chairman, The FAIR Institute

Copyright 2017 The FAIR Institute
All rights reserved

1

What we'll cover today...

- What's wrong and why it matters
- An introduction to FAIR
- Common concerns
- Measurement
- The hard part...
- Example analysis
- Practice analysis
- Wrapping it up

Copyright 2017 The FAIR Institute
All rights reserved

2

2

Priorities

- 1
- 2
- 3



Organizations must prioritize their cyber risk problems and solutions.

Copyright 2017 The FAIR Institute
All rights reserved

3

3

Prioritization implies...

Comparing their various concerns and solution options, which requires...

Measurement

4

How is cyber risk being measured?

Just like any other complex measurement objective... by using a model and data.

An simple example is speed:

$$\text{Speed} = \text{Distance}/\text{Time}$$

5

What is the most commonly used cyber risk measurement model?

6



A weak foundation

What are your organization's top ten cyber risks?

What was #11, and how much less risk does it represent than #10?

Which of the following are risks?

- Disgruntled insiders
- Internet-facing web servers
- Untested recovery process
- Network shares containing sensitive consumer information
- Weak passwords
- Cyber criminals

What is the classic formula for risk?

10

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Likelihood and Impact of what?

Loss Events

These aren't loss events

11

Disgruntled insiders

Internet-facing web servers

Untested recovery process

Network shares containing sensitive consumer information


Weak passwords

Cyber criminals

You can only assign likelihood and impact to loss events.

Infosec Risk Seminar Survey

12

What are the top 3 risks for your organization? 



Votes: 25

Infosec Risk Seminar Survey

From the topics in the agenda, what are your greatest pain points?



13



14

Other causes of inaccurate risk measurement

Absence of critical thinking
(Reliance on "best practices")



Broken models

Focus on possibility
vs. probability



15

common
Other causes of inaccurate risk measurement
^

16

Poorly defined measurement scales



Bad estimates



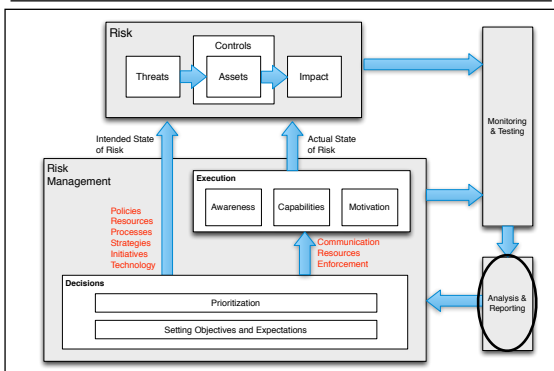
Math on ordinal scales (Red x Green) / Yellow = ?

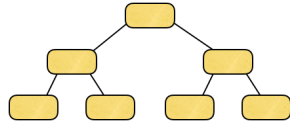
70% to 90% of "high risk" issues, aren't

17

Why it matters...

18





FAIR Ontology

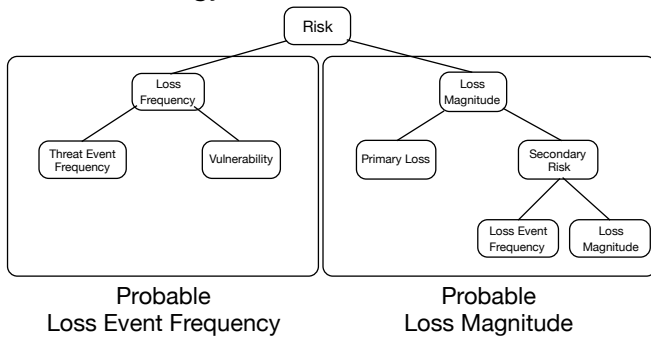
Risk...

The probable frequency and probable magnitude of future loss

In other words...

How often loss is likely to happen,
and how bad it's likely to be when it happens

FAIR Ontology



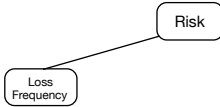
Risk

Risk | The probable frequency and probable magnitude of future loss

Copyright 2017 The FAIR Institute
All rights reserved

22

22



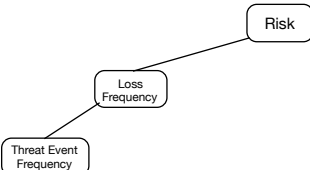
```
graph LR; LF[Loss Frequency] --- R[Risk]
```

Loss Event Frequency | The probable frequency, within a given timeframe, that a threat action will result in loss

Copyright 2017 The FAIR Institute
All rights reserved

23

23



```
graph LR; TEF[Threat Event Frequency] --- LF[Loss Frequency]; LF --- R[Risk]
```

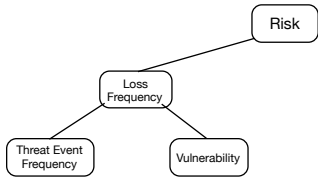
Threat Event Frequency | The probable frequency, within a given timeframe, that a threat will act in a manner that may result in loss

Copyright 2017 The FAIR Institute
All rights reserved

24

24

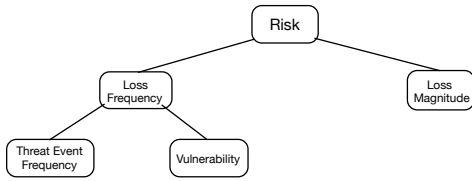
25



Vulnerability

The probability that a threat event will become a loss event

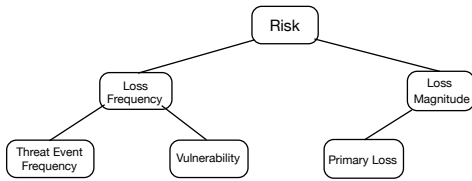
26



Probable loss magnitude

The probable magnitude of loss resulting from a threat action

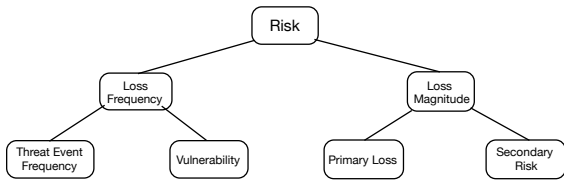
27



Primary loss

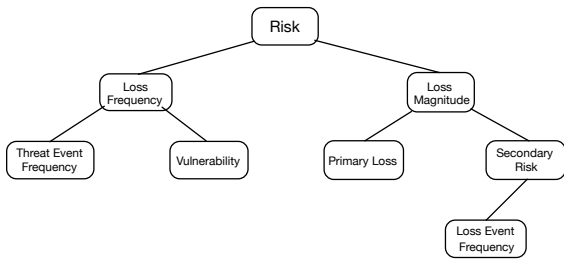
Loss that occurs directly as a result of the threat act against the asset.

28



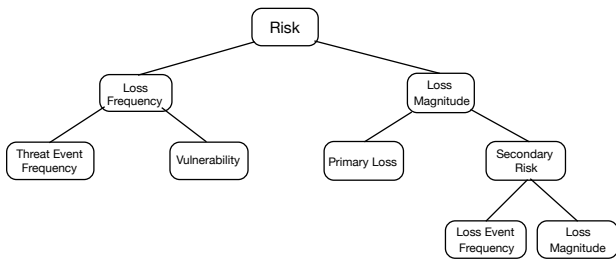
Secondary Risk | Loss that occurs as a result of secondary stakeholder reaction to the primary loss event.

29



Secondary LEF | The probable frequency of loss generated by secondary threats

30



Secondary LM | The probable loss magnitude resulting from secondary threat actions

Forms of loss



31

Forms of loss



Productivity Is the reduction in an organization's ability to generate its primary value proposition (e.g., income, goods, services, etc.)

32

Forms of loss



Response Expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, etc.)

33

Forms of loss



Replacement The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop, etc.)

Forms of loss



Competitive Advantage Losses associated with diminished competitive advantage. CA loss is specifically associated with assets that provide competitive differentiation between the organization and its competition. Examples would include trade secrets, merger and acquisition plans, etc.

Forms of loss



Fines & Judgements Legal or regulatory actions levied against an organization. Note that this includes bail for any organization members who are arrested.

Forms of loss

37

- Productivity
- Response
- Replacement
- Comp Adv
- Fines & Judgements
- Reputation

Reputation Losses associated with an external perception that an organization's value proposition is reduced or leadership is incompetent, criminal, or unethical.



But...

38



Common concerns

39



Isn't quantifying cyber risk different and harder (or even impossible)?



How does qualitative measurement solve/avoid those concerns?

A simple estimation problem



How fast was the car going?

- ▶ Qualitatively
- ▶ Quantitatively



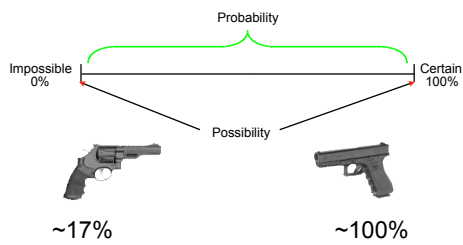
Oh look! It fits!

Qualitative and ordinal risk measurements are subject to the same challenges as quantitative measurements, they just sweep the problems under the rug rather than force us to deal with them.

Probability vs. Prediction



Probability vs. Possibility



The dirty word of measurement: **SUBJECTIVITY**

Objective



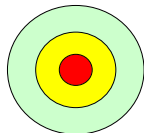
Subjective



Reality

Precision vs. Accuracy

What we typically see...



- Inaccurate & Imprecise
- Inaccurate & Precise
- Accurate & Precise
- Accurate & Imprecise

Measurement



Estimating

How tall am I?

- ▶ 5'5"
- ▶ 5'6"
- ▶ 5'7"
- ▶ 5'8"
- ▶ 5'9"
- ▶ 5'10"
- ▶ 5'11"
- ▶ 6'0"
- ▶ 6'1"
- ▶ 6'2"

Would you bet \$1,000 on your estimate?

Was that estimate subjective or objective?

Estimating using ranges

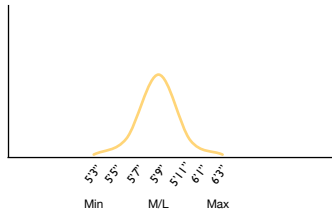
How tall am I?

- ▶ < 5'5"
- ▶ 5'5" - 5'11"
- ▶ 6'0" - 6'6"
- ▶ < 6'6"

We achieve accuracy with an acceptable level of precision.

Estimating using distributions

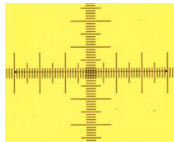
How tall am I?



52

What is calibration?

A method for measuring and improving an individual's ability to make good estimates



53

Why calibration?

Garbage in, garbage out...

The ability to estimate effectively varies from person to person

People can be trained to estimate more effectively

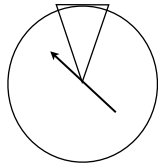
54

Example

55

What is the wingspan of a Boeing 747?

- 1 to 1000 feet?
- 50 to 500 feet?
- 100 to 300 feet?
- 125 to 250 feet?



Benefits of calibration

56

Reduces the probability of gross error

Surfaces assumptions

Establishes the basis/rationale for estimates

Provides values that can be plugged into
Monte Carlo or other analytic functions

Monte Carlo Simulations

57

Combining uncertain values

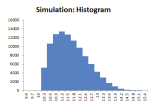
58

$$\text{Speed} = \text{Distance} / \text{Time}$$

How to derive speed when distance and/or time measurements have some amount of uncertainty or variability?

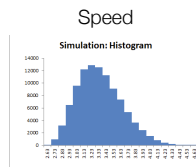
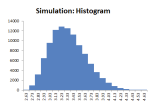
Distance:

- Min: 10 mile
- Max: 15 miles
- ML: 11 miles



Time:

- Min: 3 hours
- Max: 4 hours
- ML: 3.5 hours



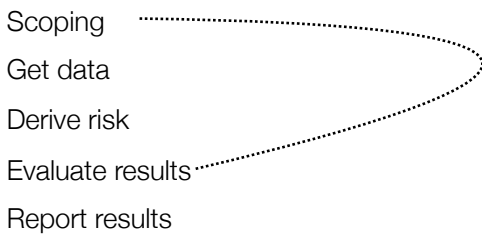
The Hard Part...



59

The analysis process

60



Bald Tire

How much risk?



61

There will always be assumptions in any analysis.
The key is to surface them.

62

Scoping - step 1

What is the loss event (risk) we're trying to understand/measure?

- ▶ Compromise of sensitive information?
- ▶ Loss of availability?
- ▶ Project cost-overrun?

63

Scoping - step 2

What is/are the relevant asset(s)? Where does the loss event occur?

- › Laptop?
- › Server?
- › Web application?
- › Network transmission?

64

Scoping - step 3

Who/what is the relevant threat?

- › Cyber criminals?
- › Privileged insiders?
- › Mother nature?
- › Customers?
- › Technology?

65

Scoping - step 4

What type of threat event is it?

- › Accidental?
- › Intentional but not malicious?
- › Intentional and malicious?
- › Other?

66

Scoping - step 5

In what manner does the threat event occur (vector)?

- ▶ Over the network?
- ▶ Locally to the system?
- ▶ Direct physical contact?
- ▶ Through an unwitting accomplice?

67

Without this kind of scoping rigor, the odds of measuring risk accurately are much lower, regardless of whether you're doing qualitative or quantitative measurement

68

Example Analysis



69

An audit discovered that privileges for accounts in the customer support application aren't consistently being updated when personnel change roles.

Gut check

Is this a risk?

Why?

How much risk does this represent?

Scoping this analysis...

What is the asset at risk? Customer information

Who/what is the threat actor(s)? Personnel with inappropriate access

What type of action Malicious

What type of event is it (C, I, or A)? Confidentiality

What is the loss event? The confidentiality of customer data is maliciously compromised by an employee with inappropriate access

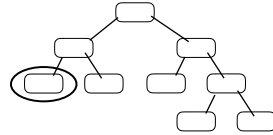
This is the risk

Threat Event Frequency

73

Definition

The probable frequency, within a given timeframe, that a threat will act in a manner that may result in loss



Who is the threat agent?

Estimates

Qualitative?

Min: .05 yr (1 in 20 yr)

ML: .1 yr (1 in 10 yr)

Max: 5 yr

Data/Rationale

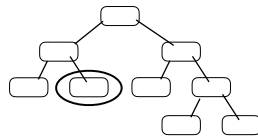
- 30 user accounts (out of 200) with inappropriate access levels (15%)
- HR records show 2 events of misuse in the past 3 yrs ("snooping")
- Snooping was performed by personnel **with appropriate access**
- No history of malicious misuse

Vulnerability

74

Definition

The probability that a threat event will become a loss event



Estimates

Qualitative?

100%

Data/Rationale

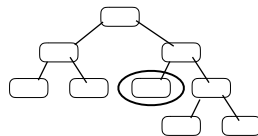
- These are privileged insiders who don't have to overcome controls in order to execute the illicit action

Primary Loss Magnitude

75

Definition

Loss that occurs **directly** as a result of the threat act against the asset.



Estimates

Qualitative?

Min: \$ 25k

ML: \$ 40k

Max: \$ 150k

Data/Rationale

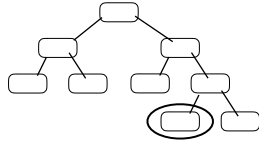
- Combination of forensic/investigative costs and costs associated with replacing the malicious employee

Secondary Loss Event Frequency

76

Definition

The probable frequency of loss generated by secondary threats



Estimates

Qualitative?
100%

Data/Rationale

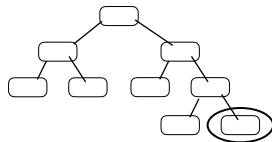
- Assumes that any compromise of customer information would require notification and other secondary costs

Secondary Loss Magnitude

77

Definition

The probable loss magnitude resulting from secondary threat actions



Estimates

Qualitative?
Min: \$ 100
ML: \$ 17k
Max: \$ 500k

Data/Rationale

- Minimum of 1 customer record
- Most Likely 20 customer records
- Maximum 100 customer records due to user account access limitations
- Includes notification costs, credit monitoring, legal defense, and customer churn

Qualitative results...

78

High?

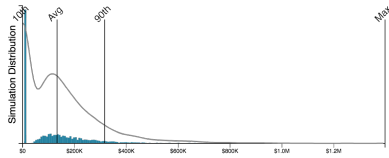
Medium?

Low?

Analysis results

79

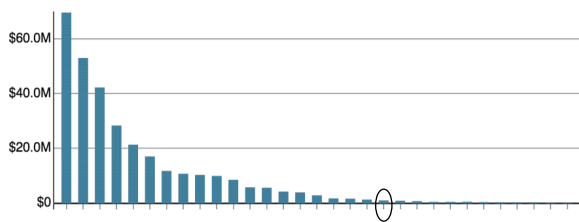
	Minimum	Average	Maximum
Primary			
Loss Events / Year	0.05	0.89	4.29
Loss Magnitude	\$25K	\$56K	\$137K
Secondary			
Loss Events / Year	0.05	0.89	4.29
Loss Magnitude	\$114	\$94K	\$426K
Total Loss Exposure	90	\$133K	\$1.4M



Copyright 2017 The FAIR Institute
All rights reserved

Prioritization

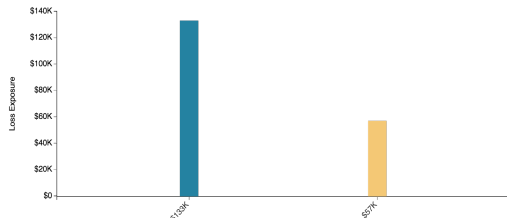
80



Copyright 2017 The FAIR Institute
All rights reserved

Mitigation benefit analysis

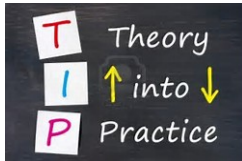
81



	Analysis	Period	Min	10 th %	Avg	90 th %	Max
■	Equal presentation	Q3 2017	\$0	\$0	\$133k	\$317k	\$1.4M
■	With improved controls	Q3 2017	\$0	\$0	\$57k	\$189k	\$565k

Copyright 2017 The FAIR Institute
All rights reserved

Let's do an analysis...





Wrapping it up

FAIR Advantages

Improves risk measurement and prioritization/focus (whether qualitative or quantitative)

- ▶ Provides a framework for critical thinking
- ▶ Normalizes terminology and mental models

Improves the ability to speak in business-risk terms and establish useful risk appetite thresholds

Complements common "good practice" frameworks

Can be used to analyze any form of risk

Reduces religious arguments

Is an open international standard (The Open Group)

Maturity concerns

“We’re not mature enough to do quantitative risk analysis”

“We don’t have enough data”

85

Minimal adoption approach

Adopt the ontology as a standard risk model for your organization

- ▶ Normalizes terminology
- ▶ Normalizes mental models

Adopt the scoping principles

Assign specific responsibilities

- ▶ Not everyone is cut out to do risk analysis
- ▶ Requires
 - Critical thinking skills
 - Being comfortable with uncertainty
 - Awareness of basic probability principles

86



Ignorance is bliss...

...but you're no longer ignorant

87

From this point forward, you can choose to ignore what I've shared, but you're no longer ignorant of the issues.

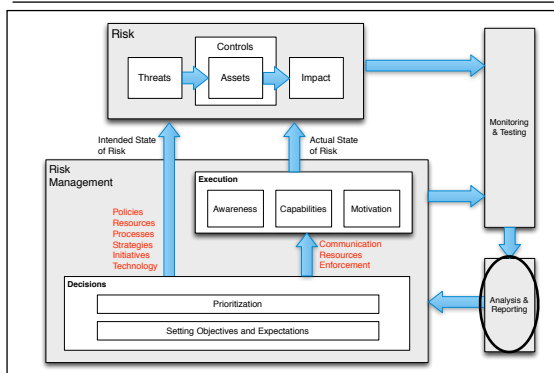
Or, you can become a change agent by:

Seeking clarification...

- What was the scope of that "medium risk"?
- Is that a calibrated estimate?
- What does "medium" mean?
- Does it represent best case, worst case, or something else?

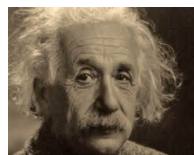
Socializing the need for higher quality risk measurement standards and practices

Why it matters...



When it comes to risk measurement...

You get what you pay for



Everything should be made as simple as possible, but not any simpler.

Albert Einstein

The FAIR Institute

Nonprofit dedicated to building a community of experts in more evolved and effective risk management methods

No cost to join

Over 1700 members to-date

Very active blog and numerous white papers

Soon will offer a free online FAIR tool and pre-defined university curriculum

Local chapters in large cities (e.g., Chicago, NYC, San Francisco, Washington DC, Toronto)

Several active workgroups

- Cyber risk management
- Data utilization
- Operational risk
- University educators

91

2nd Annual FAIR Conference

When: Oct 16 & 17

Where: Dallas, TX

Same week/location as the RSA Charge conference (RSA is a sponsor of FAIRCon)

Register thru the fairinstitute.org website

92

The Open Group

Professional certification for FAIR practitioners

Resources for certification prep and for applying FAIR

Trainer accreditation process

Continually developing new resources

93

Resources

94

The FAIR Institute

- ▶ <http://www.fairinstitute.org>

The Open Group

- ▶ <http://www.opengroup.org/standards/security>

Measuring and Managing Information Risk: A FAIR Approach

- ▶ amazon.com

<http://www.RiskLens.com/resources>

Questions?

95
