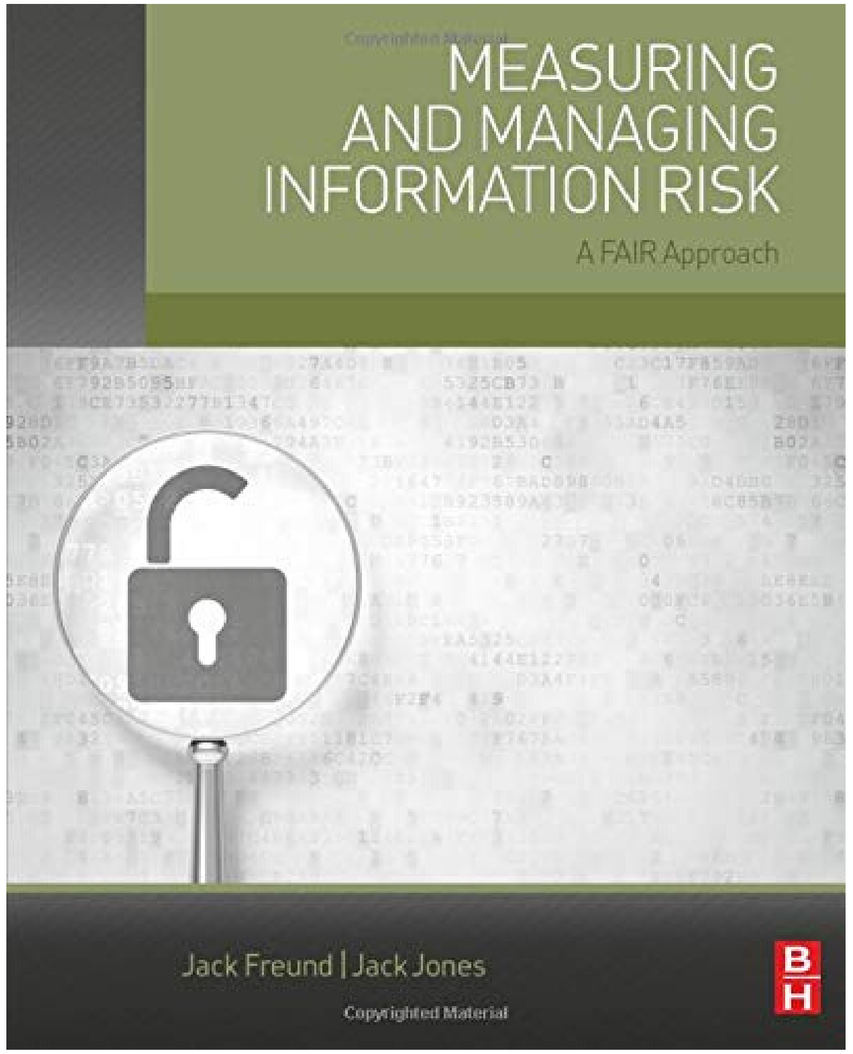
BOOK CLUB

Measuring and Managing Information Risk

Part 2: Chapters 4 - 5



What Will We Cover Today?

Use the following guide during your book club to drive discussion around the chapters outlined

Chapter 4

FAIR Terminology

Chapter 5

Measurement

Chapter 4

Speaking in the same language

Asset

Identify a critical asset in your organization. Do you each have a different meaning to what an asset is?

Tip: As you think through this, focus on where the confidential data sits or what systems run critical business processes.

Threat Event

"...has the potential to cause harm."

What type of system data do you have to represent a true 'threat event' from a malicious external actor?

Loss Event

"...is a threat event where loss materalizates and/or where liability increases" - Chapter 4

What truly defines a loss event? Would you consider a phishing attack a loss event? What about misdelivery of a single PII customer record? Do you experience loss daily - probably - but what are grounds for measurement?

Group Activity: Choose a loss event and as a group talk about how it would unfold - it's okay if there are differing opinions - *keep it high level!*

Chapter 4

Threat Actors: Who are you and what do you want?!?

1

Malicious or Non-Malicious?

Based on your organization and industry do you expect to focus more on malicious or non-malicious actors? Maybe both?

...

2

Opps I did it again...

Insiders causing accidental outages, erroneously disclosing data, etc. - sound familiar? Has your organization considered this as a threat - does this change your current approach?

3

Threat Communities

From an external perspective - what communities do you think are most likely a concern for your organization? What is their motive and what do you have?

'Mini' Case Study

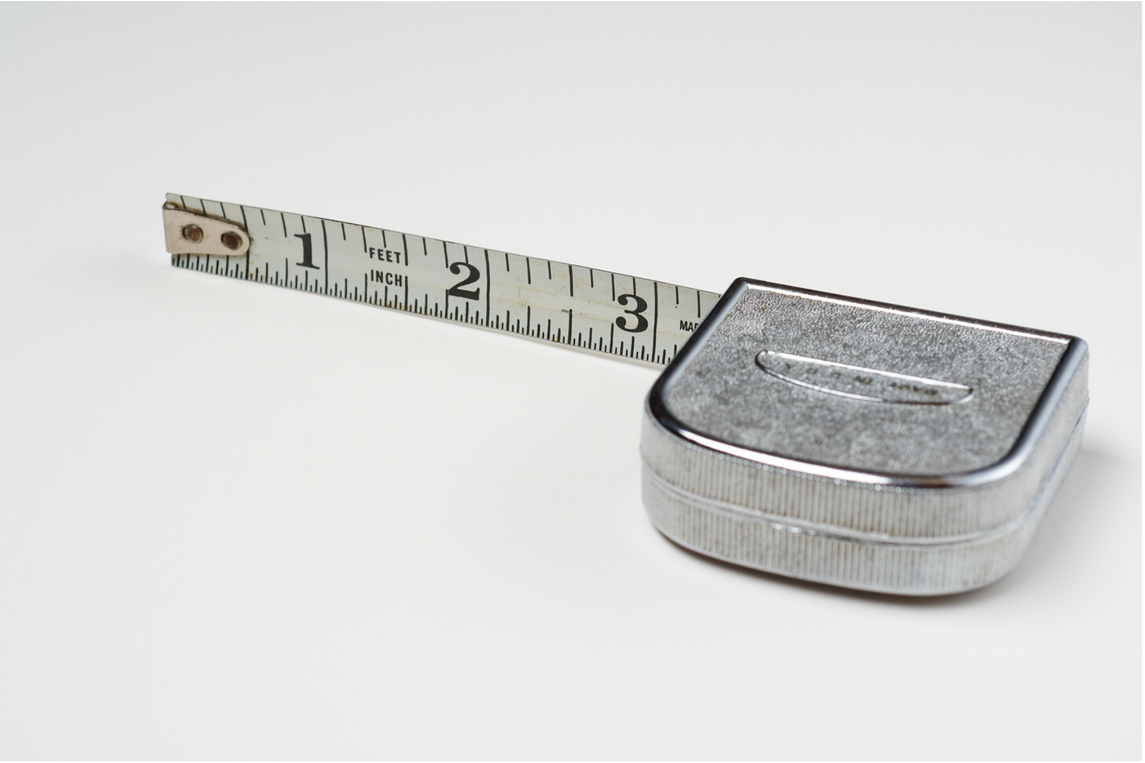
Outage of Key System

Imagine there was an outage (or loss of availabilitiy) of a key system. What forms of loss would you expect to materialize from that loss event?

Tip: Agree on key system first!

Note: FAIR is meant to be flexible - you can alter this scenario to account for ERM or IT scenarios - just rethink some wording above.

Chapter 5



Measurement is a reduction in uncertainty

- Measuring and Managing Information Risk

If Management asked how much risk do we have - which example would you prefer to use?

Ex 1: Qualitative Measurement - 'Gut Feeling'

"This loss event seems high - because we have seen it in the news so much and it's happening to our competitors."

Loss Exposure Example:
High Risk

Ex 2: Calibrated Quantitative Measurement

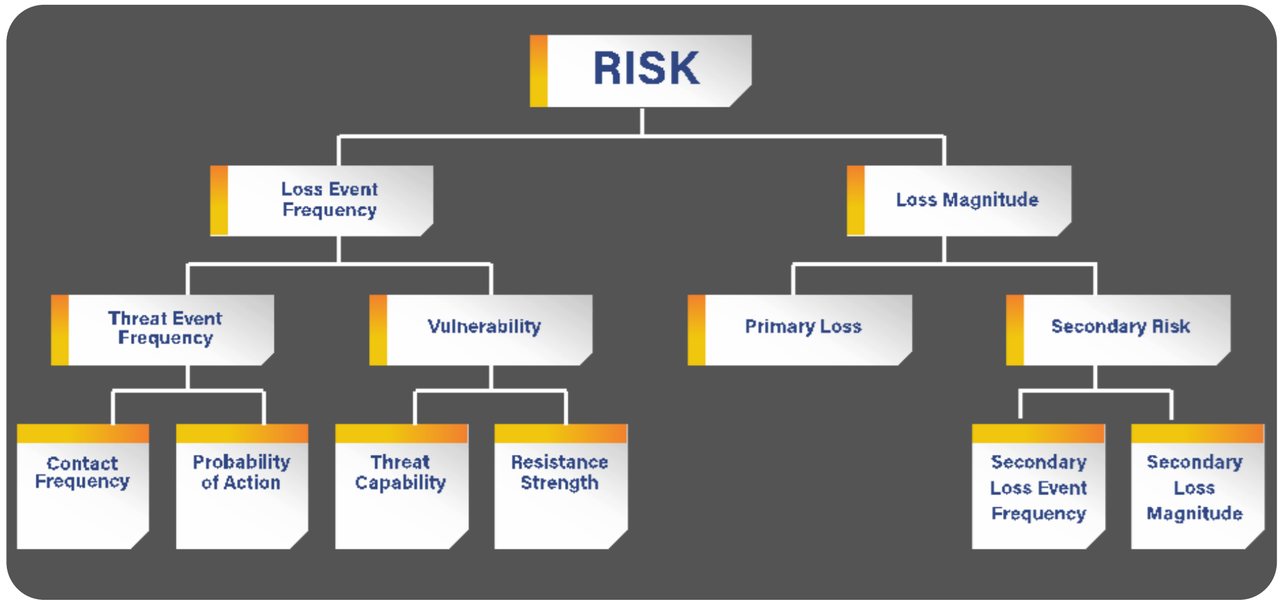
" We can use a PERT distribution and gauge what you know from historical data, industry data, and current events to build a useful distribution of loss exposure."

Loss Exposure Example:
Between $100K - 500K

Group Discussion: Example 2 probably seems like the obvious choice - but ask yourself why are you not answering questions like this from mgt in financial terms?

Or...If you currently are, are you using a distribution?

What is holding you back?



Final Thoughts?

Open discussion...

Join the Book Club discussion online! Share your club's insights, your feedback to the Guide or pose a question at the FAIR Institute's LINK community site (FAIR Institute membership and LINK signup required).

Join the Book Club discussion online!