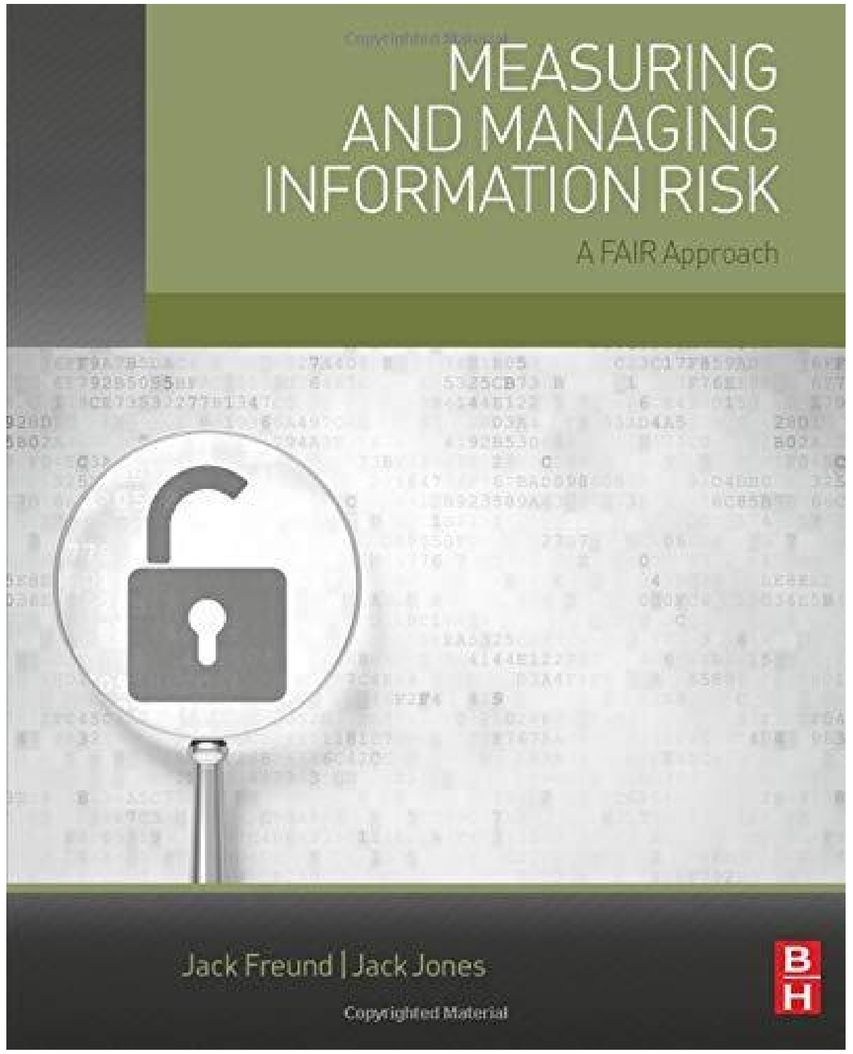
BOOK CLUB

Measuring and Managing Information Risk

Part 5: Chapters 10 - 11



What Will We Cover Today?

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

Chapter 10

Common Mistakes

Chapter 11

Controls

Chapter 10: Common Mistakes

Results Look Flat Out Wrong

This is a common issue - especially when you're new to the analysis process

There are a few steps you can take to check your results and figure out where you may have gone wrong!

We call this the 'smell test' - check out the next slide for the 'how to'.

FYI: Depending on what tools you use to perform your analysis work some of the reporting areas may not be available for your smell test process - use what you have!

Smell Test

Step-by-Step Quality Assurance Process of Results

Review Annualized Loss Exposure

Does the output look as expected?

Review 'Per Event' Metrics

Does your frequency look too high/low? Does your magnitude look too high/low?

Issues With Frequency

Focus here on the inputs you have for frequency and vulnerability. Are your ranges too wide or too tight? Can you refine your estimates further?

Issues with Magnitude

If the magnitude seems too high/low you should revisit your forms of loss and see what area is driving this.

Make sure you're not double counting!!!

Group Discussion

Focus on those areas of trouble for your group!

As you have applied your FAIR knowledge throughout book club or even in practice at your organization what obstacles have you run into? What part of the process seems daunting to you?

Not Enough Data?

This is a common issue - have you found the right person? Is there industry data you can start with? **Have you calibrated your estimates?**

Estimating Vuln?

Unable to estimate vulnerability effectively? Go back to our example in the prior guide and find strategies that work internally. As an analyst you should focus on making the process easy for SME's by breaking it down in layman's terms.

Calibration Game

When someone says, 'We don't have any data.' Play this game!

Decompose the question

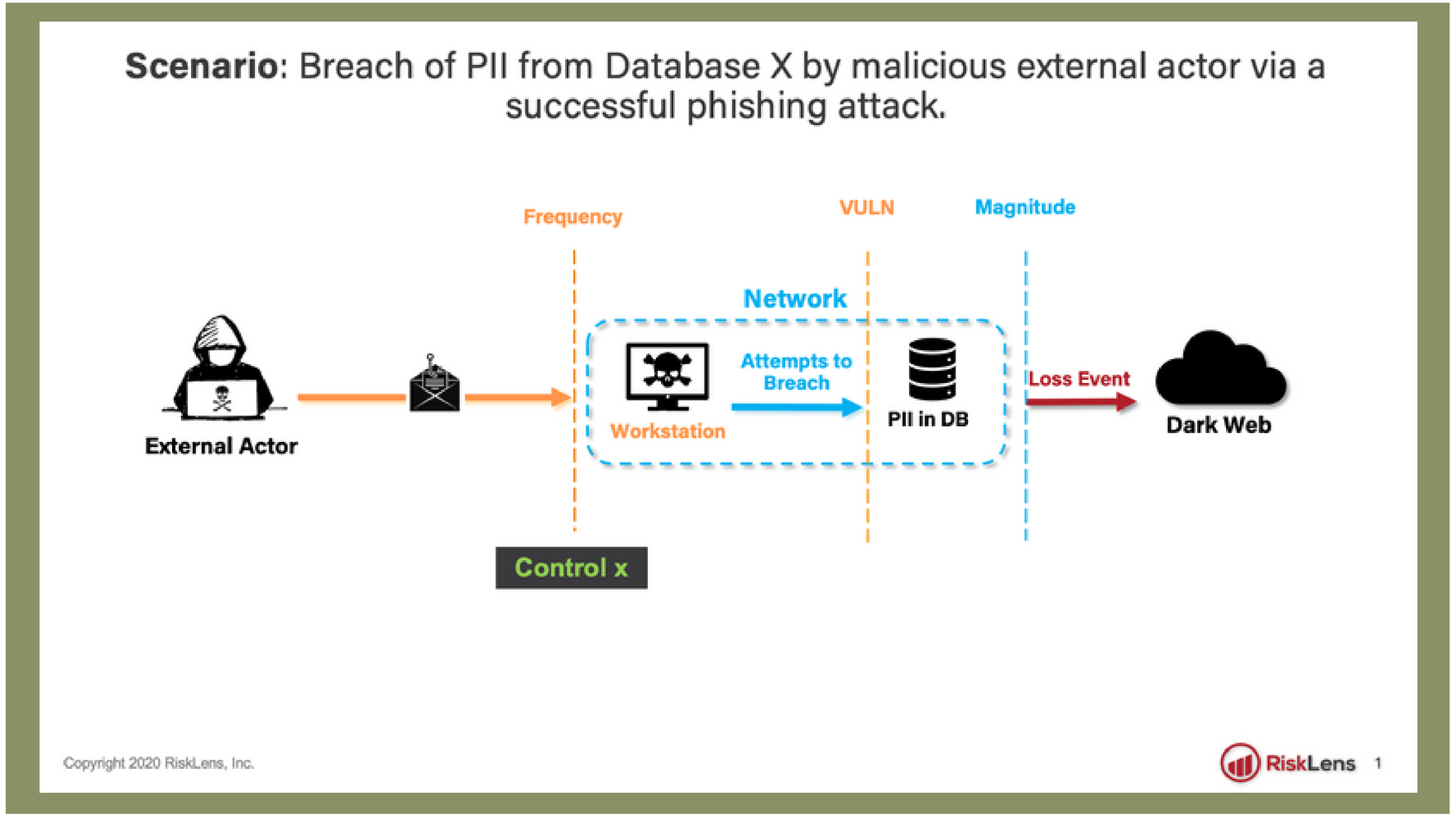
Start with the absurd

Eliminate highly unlikely values and reference what you know

Play a calibration game, revising your range iteratively

Chapter 11 - Controls

When thinking through controls I always like to focus on **WHERE** they come into play throughout the attack chain. Below is an example of a breach. Depending on the control I am modeling and what it does within the scenario I would look to change the variables of the FAIR Model.



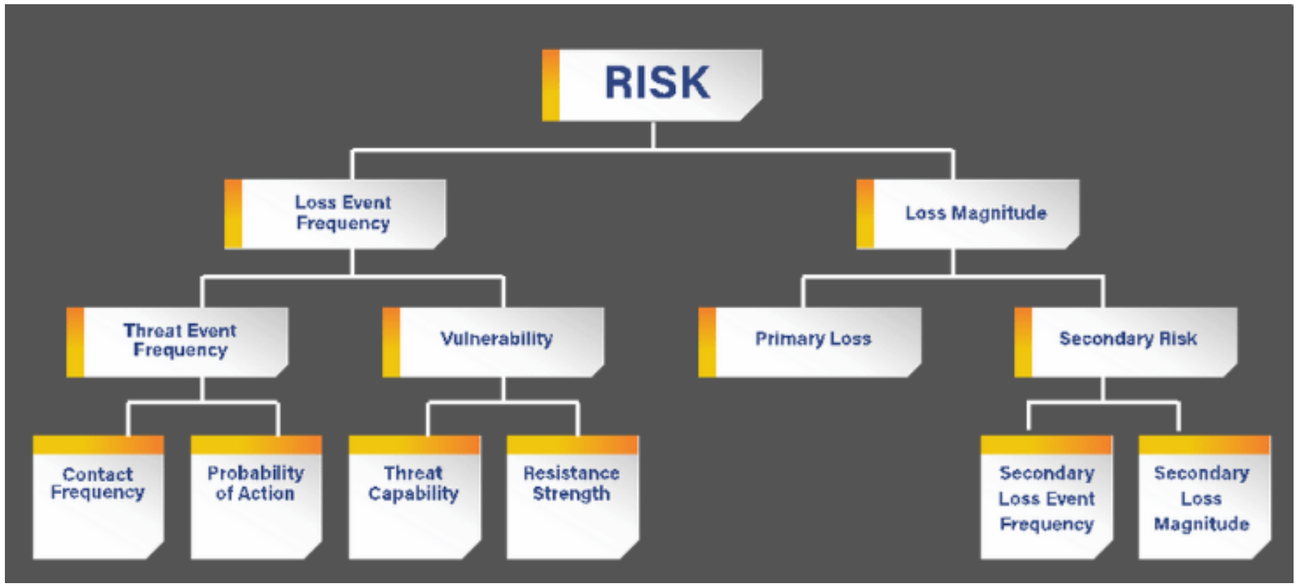
Modeling Controls

Where would you model the following controls?

Where would you go to understand the change in risk - industry data, a subject matter expert in your organization, etc?

Are there any controls that could be modeled in different parts of the FAIR Model? Why? What assumptions are you making?

- Multi-Factor Authentication
- DLP
- Column Level Encryption
- Security Cameras
- Identity Access Management
- Security Awareness Training
- File Level Encryption
- Efficient Incident Response Plan
- Background Checks
- Security Guard to Enter Office



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!