Cyber Risk Through a Situational Awareness Lens

Jack Jones
Chairman, FAIR Institute

How quickly do you need to fix this?

SQL injection vulnerability found
in a web application.

(CVSS scores it as “Critical”)

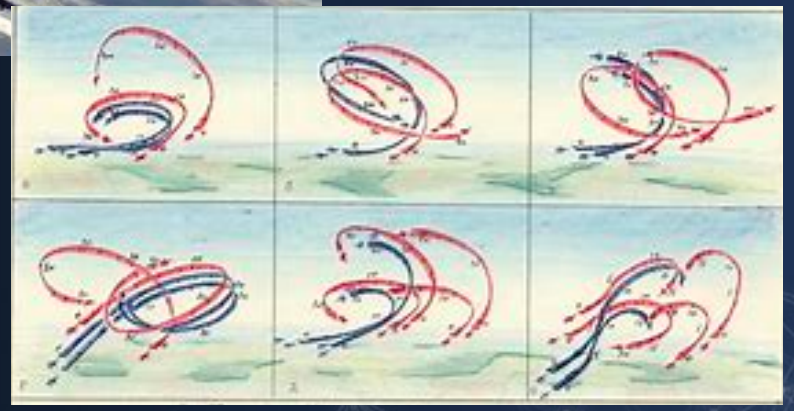
How would defend your decision?

Situational awareness

“Being aware of what is happening around you and understanding what that information means to you now and in the future”

Dr. Mica Endsley

Situational awareness levels



Level 1 - perception of the elements in the environment (data)

Level 2 - comprehension of the current situation (synthesis into a whole picture)

Level 3 - projection of the future (forecasting)

Required for effective decision-making

Endsley, Mica R.. Designing for Situation Awareness: An Approach to User-Centered Design, Second Edition. CRC Press.

Vulnerability prioritization example

1. SA Level 1 (data): A vulnerability scanner identifies a web application with a SQL injection weakness. The scanner's scoring model (CVSS) scores the weakness as "critical".

2. SA Level 2 (synthesis): A risk analyst applies additional relevant data such as — this application is: a) not Internet-facing, b) requires authentication in order to find and exploit the SQL injection flaw, and c) the database doesn't contain sensitive information.

3. SA Level 3 (forecasting): If the organization postpones remediation, it is extremely unlikely to experience a significant loss event. Therefore, resources can be better applied to other, higher-risk concerns. Monitoring of the situation should be maintained in case relevant conditions change.

Why this matters…

The cybersecurity landscape is:

Complex

Dynamic

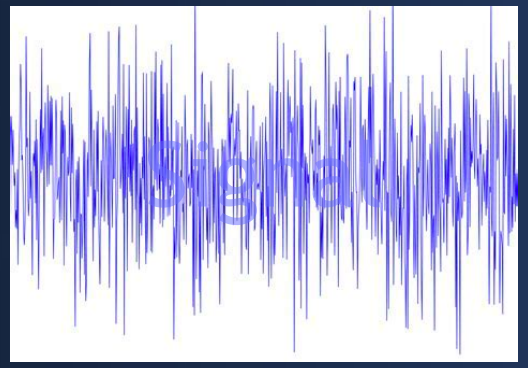
…and there are limited resources

Which means…

Organizations have to be very good at prioritizing their cybersecurity problems and choosing cost-effective solutions.

Prioritization and choosing solutions are forecasts

But…



SA Level 1 (data) challenges…

- Limited asset visibility
  - Poor asset management
  - Shadow IT (internal and cloud)
- Limited controls visibility
  - Resource limitations
  - Shadow IT (internal and cloud)
  - Third parties
- Limited threat visibility

Improving SA Level 1…

Define, identify, and place a greater focus on your organization's crown jewels

Defining a Risk Appetite That Works
https://www.youtube.com/watch?v=IxYsRiI8d84

Example - Improving asset mgmt. data (SA1)

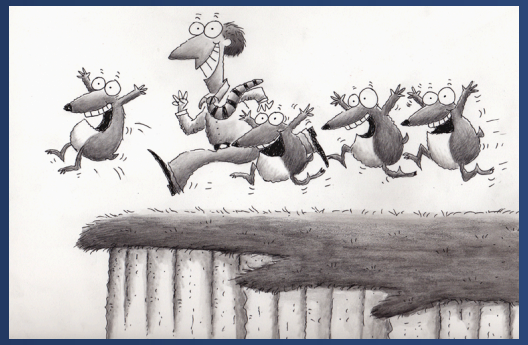
- Policy/standard
  - Asset management data must be 100% accurate at all times
    - Owner
    - Location
    - Criticality
    - etc…

Not feasible for all assets, but it is
feasible for crown jewels

SA Level 2 (synthesis) challenges…

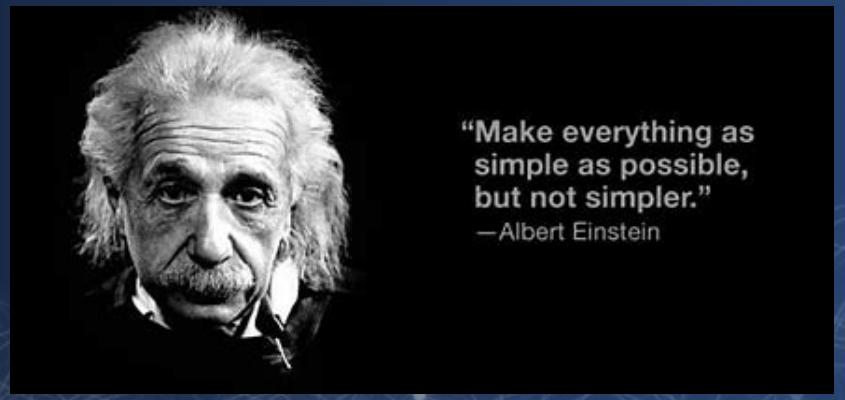
- Checklist mentality

- Over-reliance on “best practices”



- Over-simplified models

There is no easy button
for cybersecurity!



Improving SA Level 2…

- Recognize best practice and maturity model frameworks for what they are:
  - Sources of data (SA Level 1)
- Improve your models and exercise some critical thinking to put together the bigger picture
  - Identify and synthesize related data points

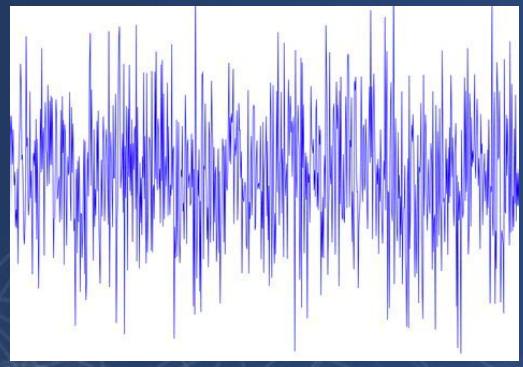
Example - Understanding current state (SA2)

- An audit finding declares that prohibiting the reuse of the last 3 passwords is insufficient (their view of best practice is to prohibit reuse of the last 5 passwords)
  - Password reuse is only a relevant control in very few (and uncommon loss event scenarios)
  - Most password attacks capture passwords thru keystroke logging or website impersonation, where reuse is less relevant as a control

SA Level 3 (forecasting) challenges…

- Level 1 & 2 limitations

- Badly flawed risk measurement models and methods

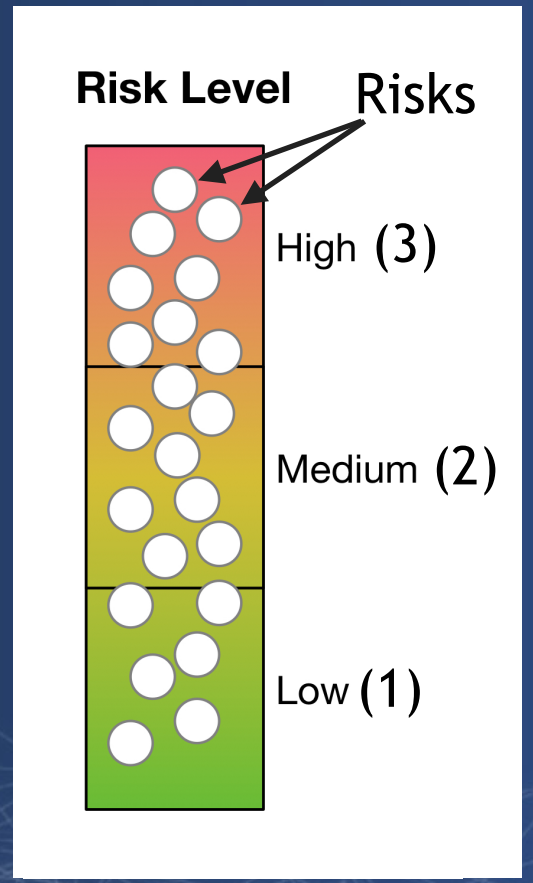


Risk measurement IS forecasting.

Ordinal scales are NOT quantitative

(Red x Green) / Yellow = ?

- How much more risk does the highest “high” represent than the lowest “high”? (And do we even agree on which one is highest?)
- How much more risk does the lowest “high” represent than the highest “medium”?
- How much risk is there in aggregate?
- What’s the unit of measure?
- Why are the lines drawn where they are?



Inaccurate model (example)

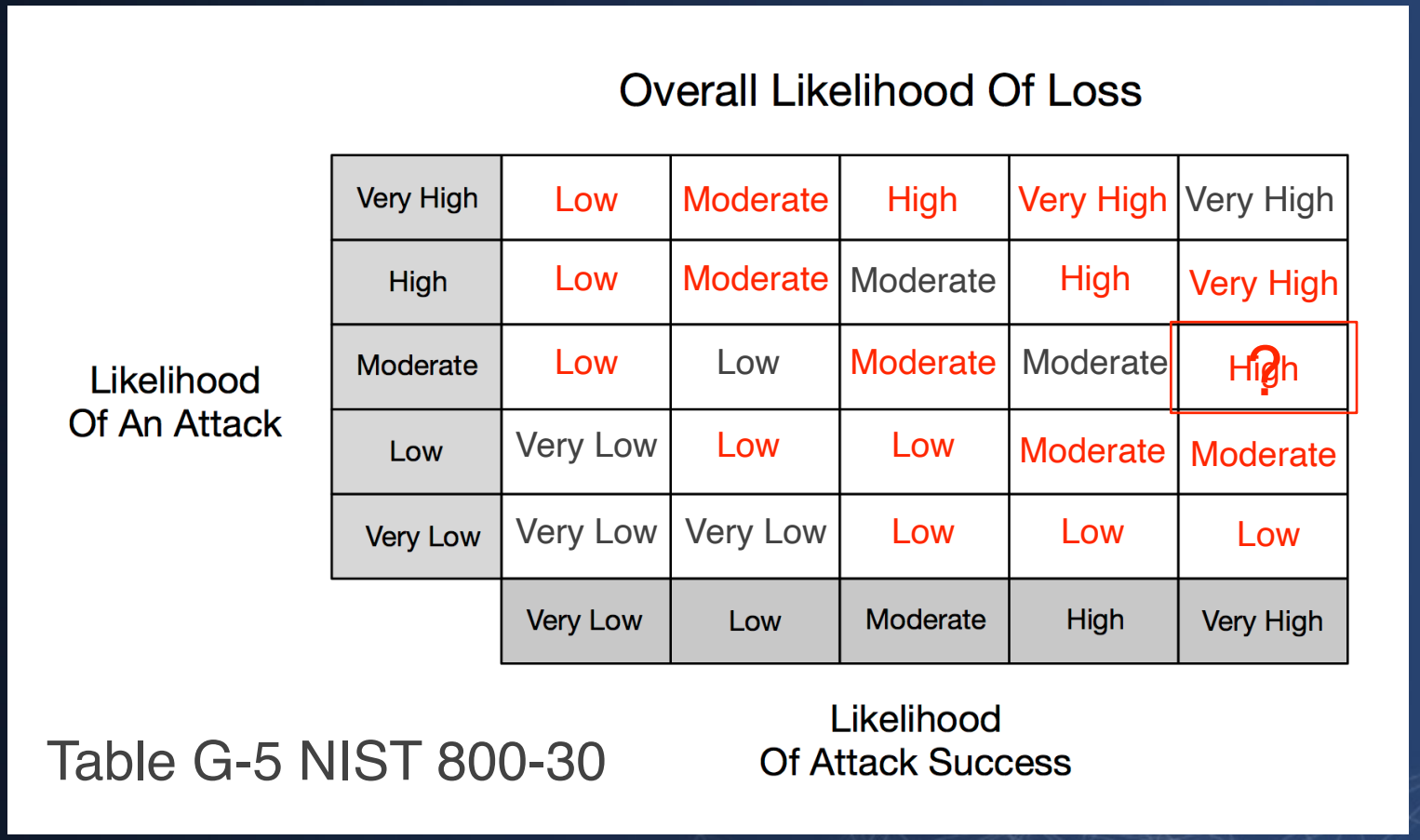


Table G-5 NIST 800-30

A measurement example

How fast are they going?

Qualitatively

Challenges…

- Is your “fast” the same as mine?
- What’s your formula for speed? Is it the same as mine?
- Which car am I referring to?
  - One in particular? (Slowest? Fastest?)
  - An average for all of them?
- Which part of the track am I referring to?
  - Corners?
  - The straightaway?
  - Average over the entire track?
  - This lap, or an average for the entire race?

Measuring speed

- Requires three elements:
  1. The scope of what's being measured
     - Which car(s)?
     - Which part of the track?
     - Which lap(s)?
  2. An analytic model
     - What data? (time, distance)
     - How to apply the data? (speed = distance/time)
  3. Data

Measuring risk

- Every risk measurement involves three elements:
  1. The scope of what's being measured
     - What asset?
     - What threat?
     - Which vector?
     - Which controls are relevant?
     - What type of event (e.g., C, I, A)?
  2. An analytic model (e.g., FAIR)
     - What data?
     - How to apply the data?
  3. Data

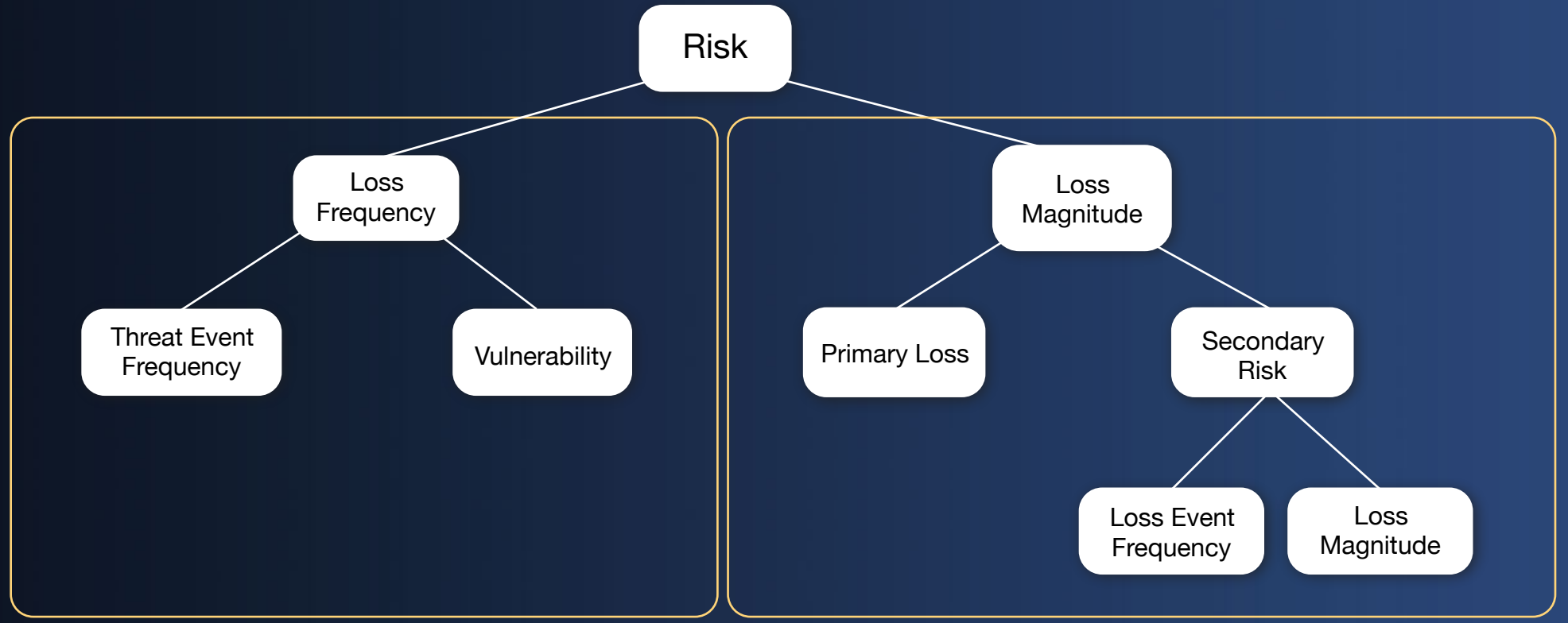
Without this kind of scoping rigor, the odds of measuring risk accurately are much lower…

…regardless of whether you're doing qualitative or quantitative measurement

Improving SA Level 3…

- Adopt a risk model and analytic methods that enable more reliable risk measurement (forecasting).
- Accept the fact that you will never have perfect data.
- Make the best use of the data you have, and faithfully reflect uncertainty in your measurements using ranges.

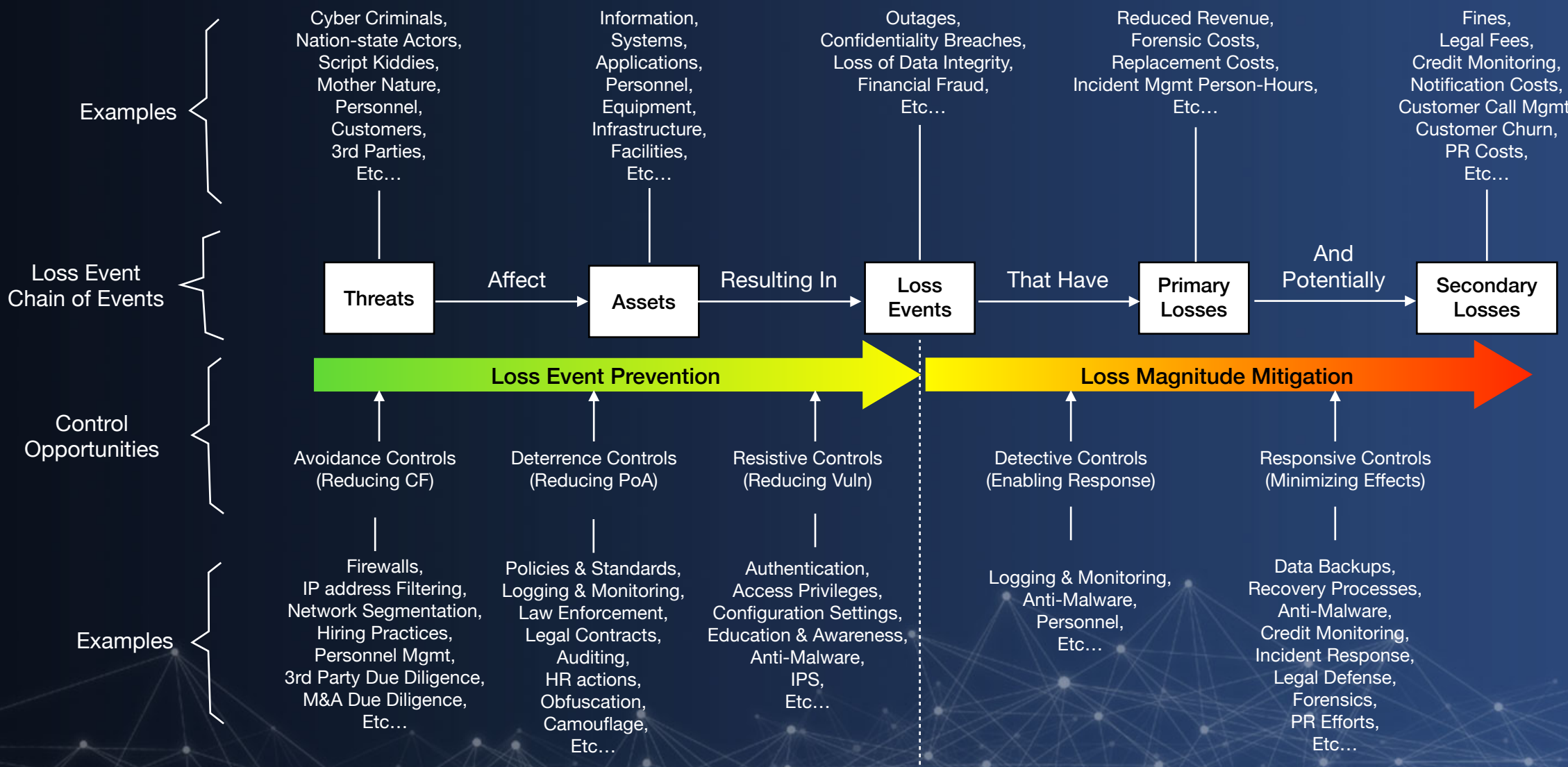
FAIR Model



Probable
Loss Event Frequency

Probable
Loss Magnitude

Loss Event Controls…



SA applied to risk management decision-making

- XSS vulnerability in client-facing web app containing millions of customer records - how much do we care/how quickly does it need to be fixed? (SA Level 1)
  - High value/liability asset
  - Active threat landscape
  - A resistive control weakness
- What are the conditions of the relevant controls in the LE chain — I.e., how much does this LE control deficiency matter from a risk perspective? (SA Level 2)
  - Implies a scenario comprised of a cyber criminal threat, network vector, XSS method, with a confidentiality breach event type
  - Avoidance (CF reduction) - IP address filtering (client IP addresses only)
  - Deterrence (N/A) - external actor
  - Resistance - Currently broken (vulnerable to XSS) ← Application firewall
  - Detective - logging but no active monitoring ← Monitor for XSS
  - Response - incident response process (rapid time to containment)
  - Bottom Line: Current exposure is limited due to an effective avoidance control
- How important is it to fix the XSS vulnerability quickly? (SA Level 3)
- What other improvement opportunities do we have that affect the probability of a significant future loss event due to this vulnerability? (SA Level 3)

Summary

- You can have the best data in the world, but if you aren't able to synthesize it effectively or forecast with it to drive decision-making, then it just doesn't matter.
- Cybersecurity data will never be perfect — we have to do the best we can with the data we have.
- We can make significant improvements in our ability to manage cybersecurity, but only if we address the weaknesses in all three levels of situational awareness.

Your homework ;-)

- Strengthen your Level 1 SA — Data
  - Has your organization defined what constitutes a “crown jewel”? If not, do so.
  - If it has, does it track them closely? If not, put the policies and processes in place to do so.
- Strengthen your Level 2 SA — Synthesis
  - Recognize common frameworks for what they are — sources of data.
  - You have to put the pieces together correctly in order to accurately understand your current situation.
- Strengthen your level 3 SA — Forecasting
  - Risk measurement IS forecasting. If you can’t do that well, then all the data in the world won’t matter.
  - Look into FAIR as a means of improving your organization’s ability to measure risk.

Questions?