Where Governance and Risk Management Align for Impact

Reporting Cybersecurity Risk to Directors and Senior Executives

Eduardo Delgado

GRC CONFERENCE 2022
IIA | ISACA

Agenda and objectives

GRC CONFERENCE 2022
IIA | ISACA

Today we will discuss:

Topic	Learning objectives	Slide
Current state	• Why typical reporting of cybersecurity risk does not support well-informed decisions	6
A better way		
• Build Scenarios	• Alternatives to model and measure risk	12
• Prioritize	• Risk measuring tools and techniques	15
• Measure Risk	• Reporting options and communication guidelines	20
• Reporting		24
Conclusion	• Summary	28


ERJ 145
CONTOUR

Local time at origin	5:45pm | 17:45
Flight Number	EDY1980
Distance traveled	1784 mi | 2935 km

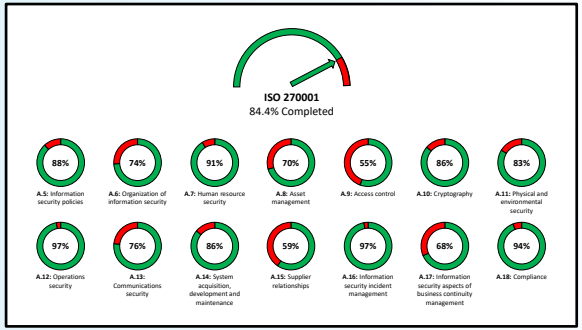
Local time at destination	6:45pm | 18:45
Estimated time of arrival	11:20pm | 23:20
Distance to destination	1880 mi| 3085 km

1. Current state

Examples of typical cybersecurity reports

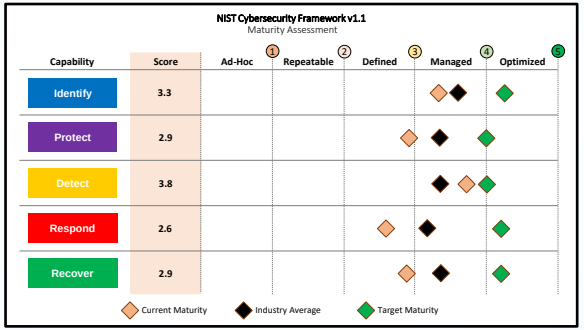
Report #1

Compliance checklist



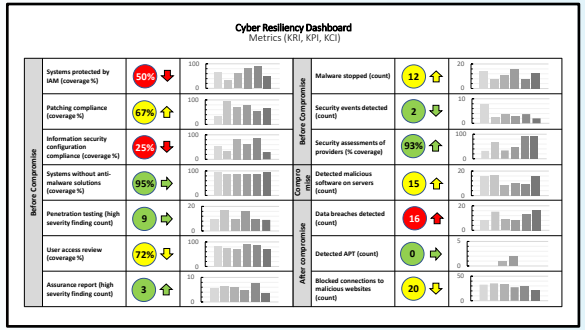
Report #2

Maturity Benchmark



Report #3

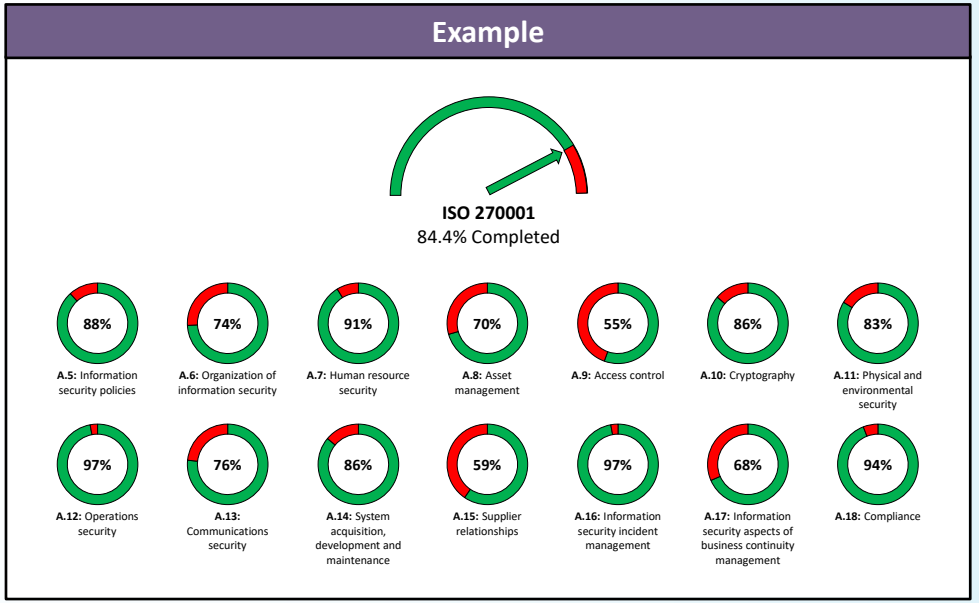
Metric Dashboard



1. Current state

Example #1: The compliance checklist

- Pick a famous industry-standard and perform compliance testing
- More compliance = Less risk?
  - False sense of security?
- Investments are based on compliance rather than risk reduction

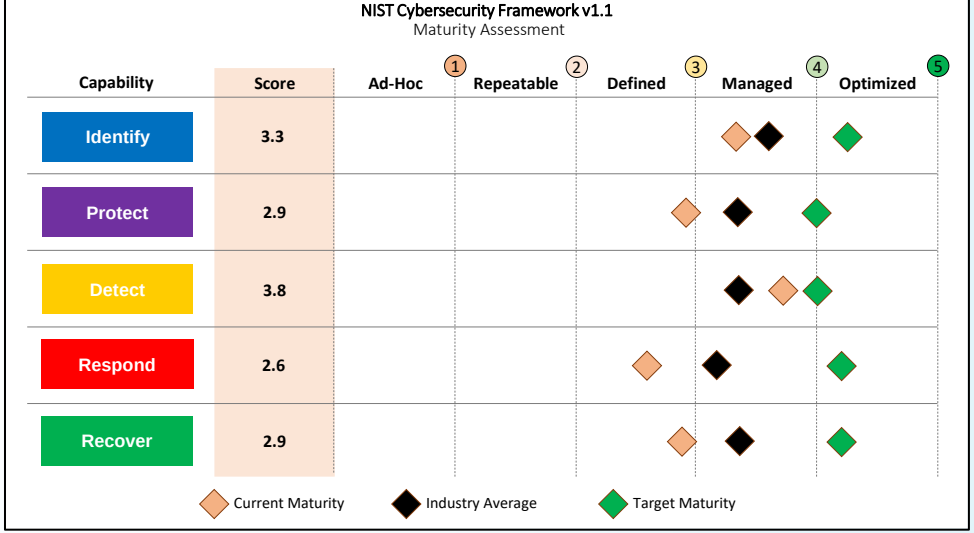


1. Current state

Example #2: Maturity Benchmark

- Very useful to compare against other organizations
- More mature = Less risk?
- Investments are based on maturity rather than risk reduction

Example

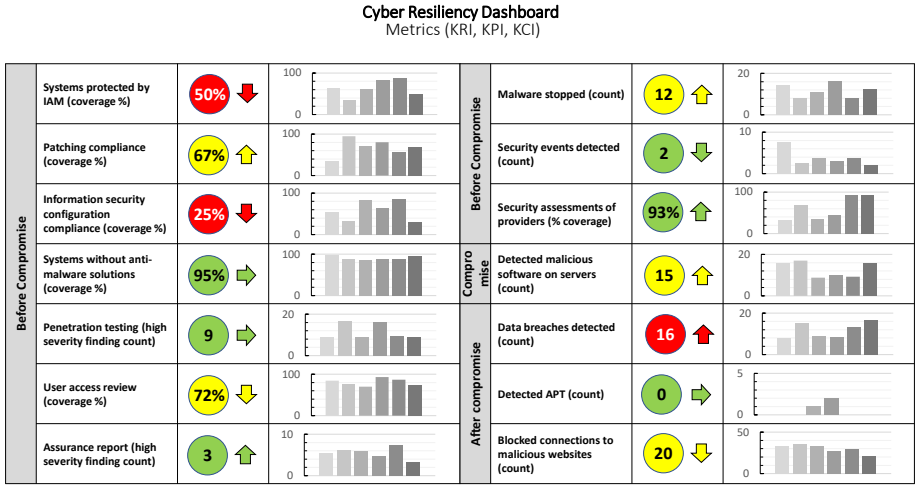


1. Current state

Example #3: Metric Dashboard

- Cybersecurity related metrics:
  - Key Performance Indicators (KPI),
  - Key Risk Indicators (KRI), and
  - Key Control Indicators (KCI)
- Difficult to understand
- More green = Less risk?
  - What is my residual risk?

Example



1. Current state

Typical reporting of cybersecurity risk does not support well-informed decisions

- Cybersecurity risk is “front and centre” topic for directors
  - Is my residual cybersecurity risk within risk appetite?
- Our current reporting approach no longer serves the business:
  - Is typically fuzzy, too technical, and/or difficult to understand
  - Does not clearly characterize risk (likelihood & impact)
  - Does not enable informed decisions
- We must pursue a better way

Approving cybersecurity investments has become an act of blind faith.

2. A better way

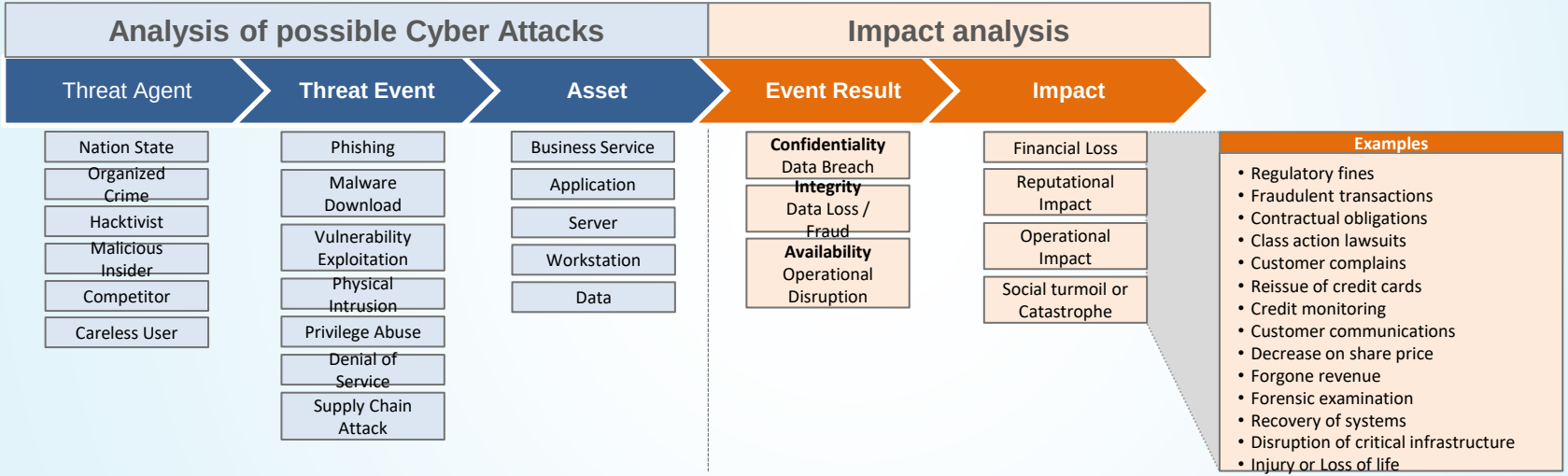
Steps

Build Scenarios	Prioritize	Measure Risk	Reporting
Make it real to the business	Focus on what matters	Likelihood and impact	Enable business to pursue value

2. A better way

GRC CONFERENCE 2022
IIA | ISACA

Build Scenarios: How do we make it real?

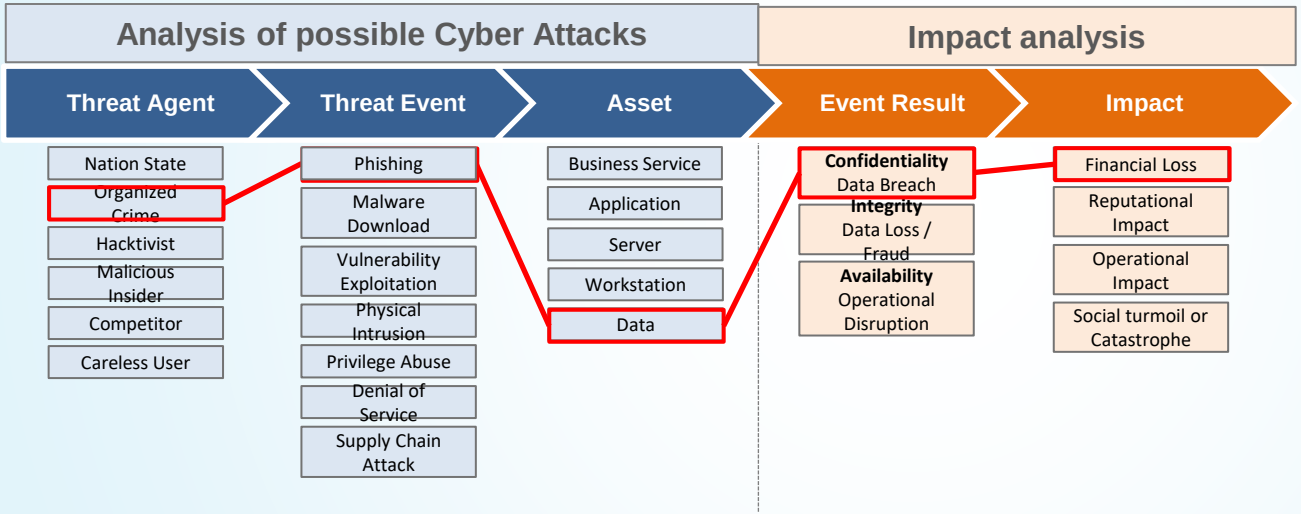


2. A better way

Build Scenarios | Prioritize | Measure Risk | Reporting

GRC CONFERENCE 2022
IIA | ISACA

Build Scenarios: How many scenarios?



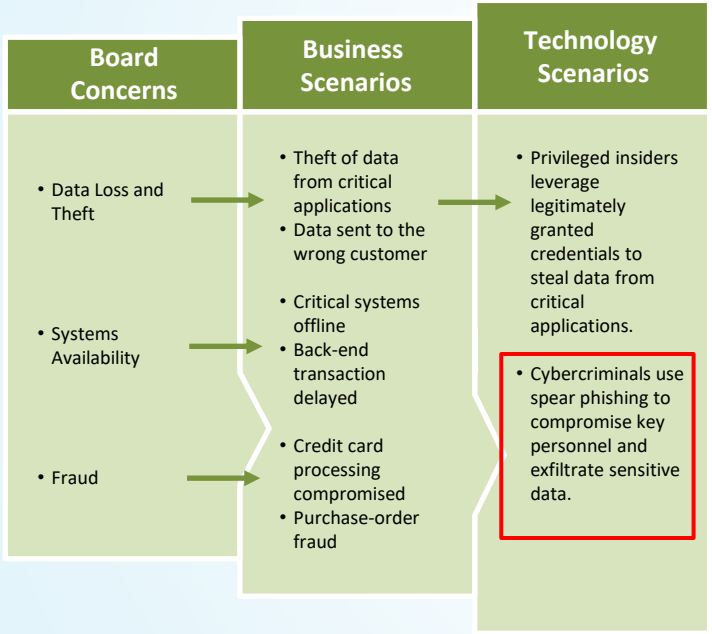
Example

Cybercriminals use spear phishing to compromise key personnel and exfiltrate sensitive data

Targeted cyber attack from a criminal organization where social engineering tactics are used to deceive a key employee by masquerading as a trustworthy entity in an email communication to gain unauthorized access to critical applications and exfiltrate sensitive data.

2. A better way

Build Scenarios: Decomposition of risk categories



- Decompose high-level board concerns into business and technology relevant scenarios
- Build the connection between the board, the business, and technical teams
- Allows to target different audiences
- Start with executive-friendly risk types and drill down into technology-friendly risk scenarios.

Source: Freund, J.; "Communicating Technology Risk to Nontechnical People: Helping Enterprises Understand Bad Outcomes," ISACA Journal, vol. 3, 2020, https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/communicating-technology-risk-to-nontechnical-people

2. A better way

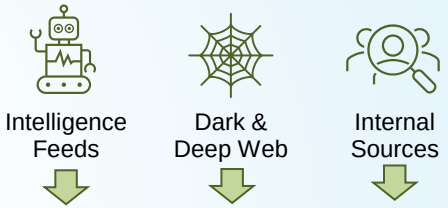
Build Scenarios | **Prioritize** | Measure Risk | Reporting

GRC CONFERENCE 2022
IIA | ISACA

Prioritize: Focus on your top cyber threats

- Cyber Threat Intelligence:
  - Valuable information used to understand the cyber threats that have, will, or are currently targeting the organization

- Prioritization and characterization of cyber threats
  - Cyber threat profiles
  - Forecast frequency and likelihood



Example

Cyber Threat Profile

Name	Organized Crime
Motive	Financial
Capabilities	Highly Technical (8) Expert in social engineering (8)
Tolerance	Medium to High (7)
Probability of Action	Opportunistic (5)

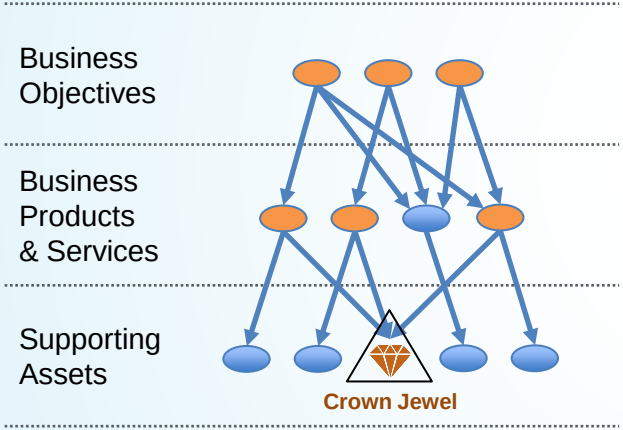
2. A better way

Build Scenarios | Prioritize | Measure Risk | Reporting

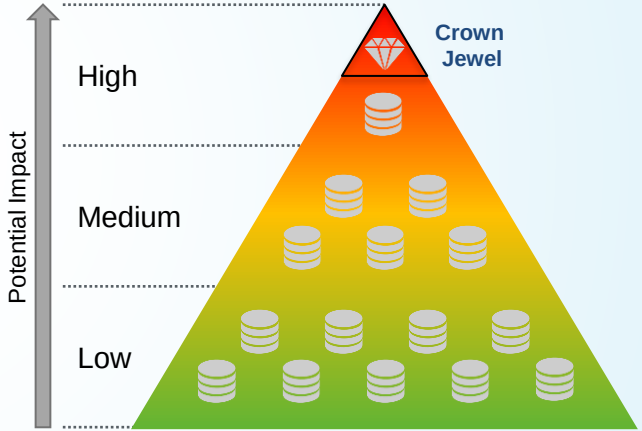
GRC CONFERENCE 2022
IIA | ISACA

Prioritize: Focus on your top digital assets

Business process mapping



Classification of Assets

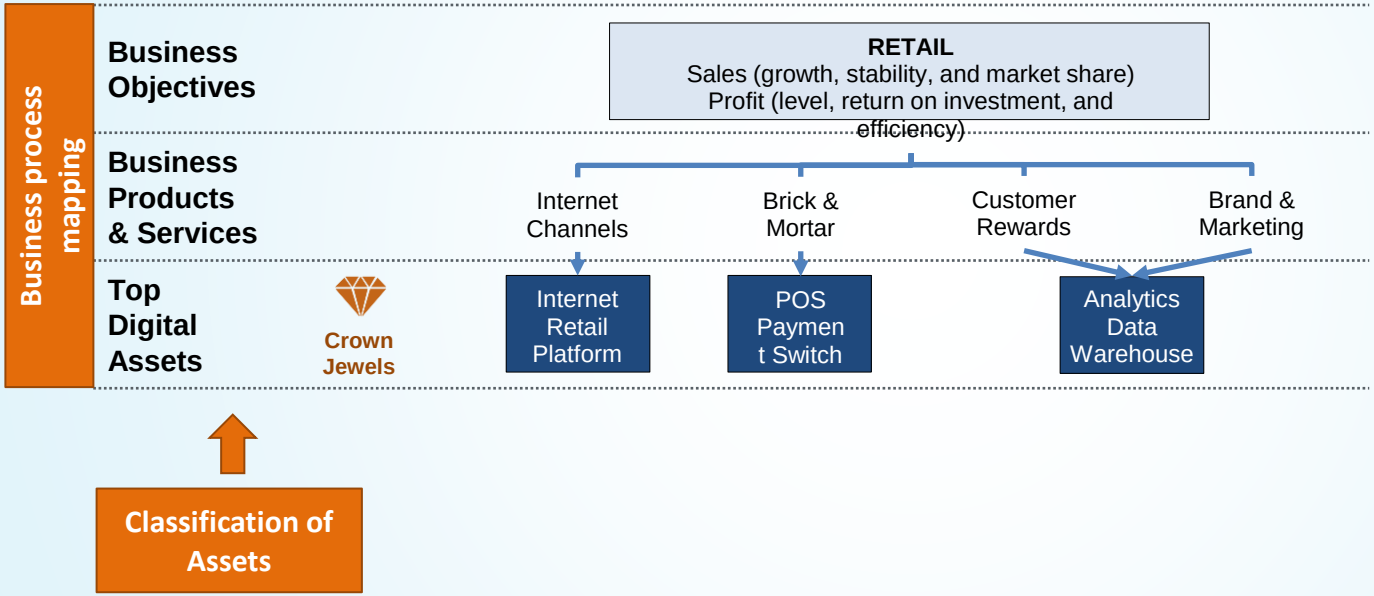


Source: CROWN JEWELS ANALYSIS, MITRE Systems Engineering Guide, The MITRE Corporation
https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

2. A better way

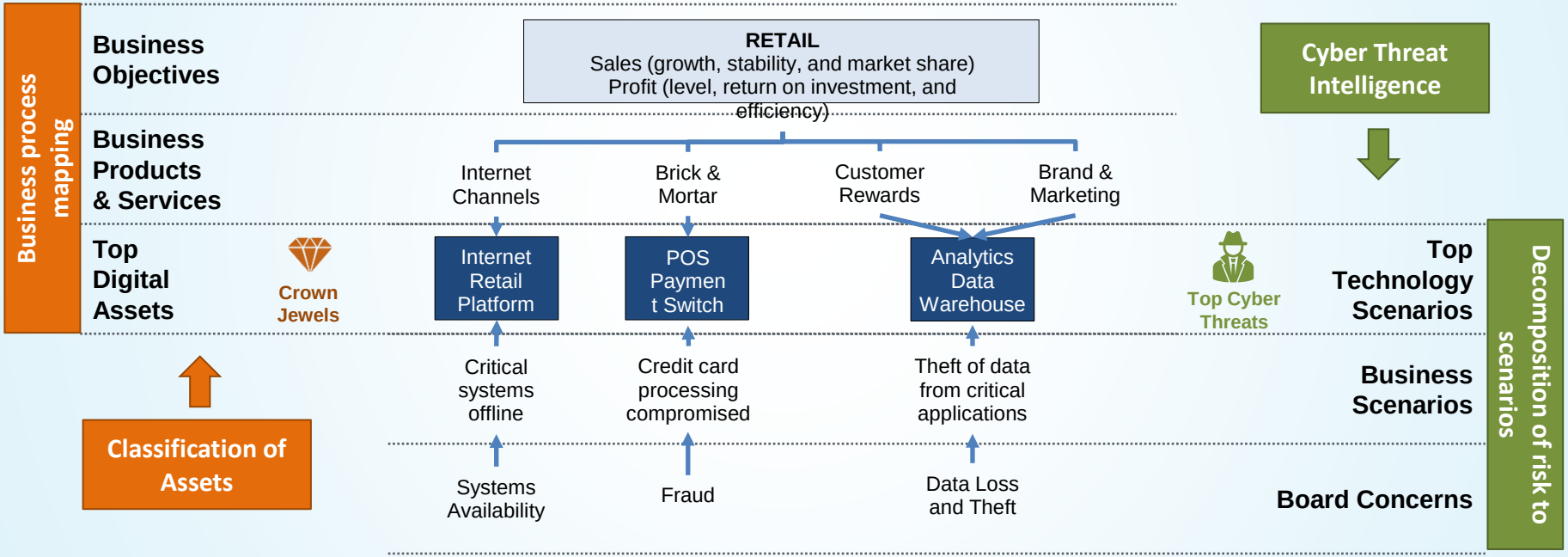
GRC CONFERENCE 2022
IIA | ISACA

Prioritize: Example



2. A better way

Prioritize: Example

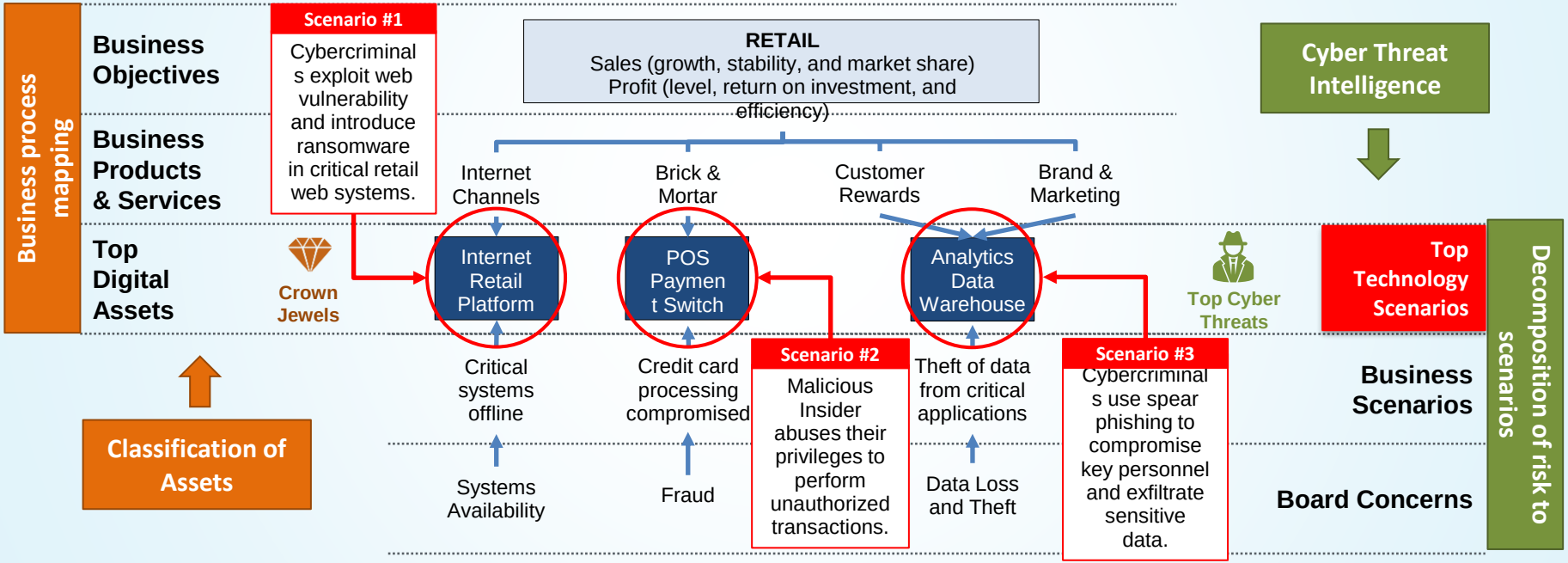


2. A better way

Build Scenarios | Prioritize | Measure Risk | Reporting

GRC CONFERENCE 2022
IIA | ISACA

Prioritize: Example



2. A better way

GRC CONFERENCE 2022
IIA | ISACA

Measure Risk: Scenario Analysis

- Process to obtain expert opinion from business and technical SMEs to estimate Risk (Likelihood and Impact).

- Typically resource intensive
  - Prioritize your scenarios to a manageable number
  - Emerging tools support scenario analysis at scale

- How to reduce subjectivity
  - A robust Risk Framework & Model
  - An established measure approach and practice

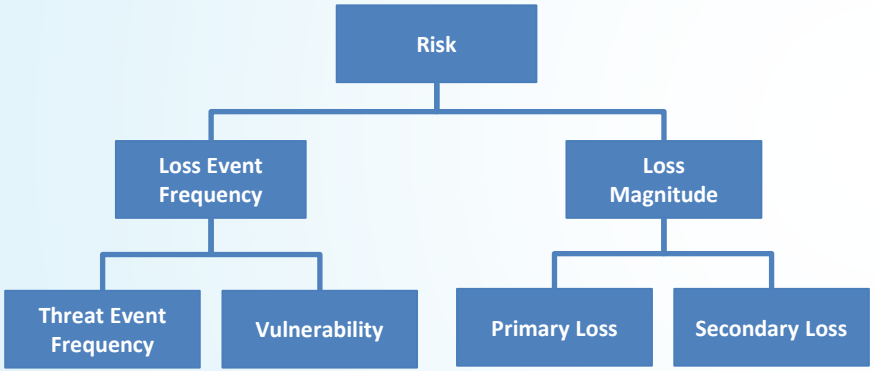
Industry leading practices

- **Open FAIR™**
- **NIST sp800-30 Risk Management guide**
- **NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM)**
- **OCTAVE℠**

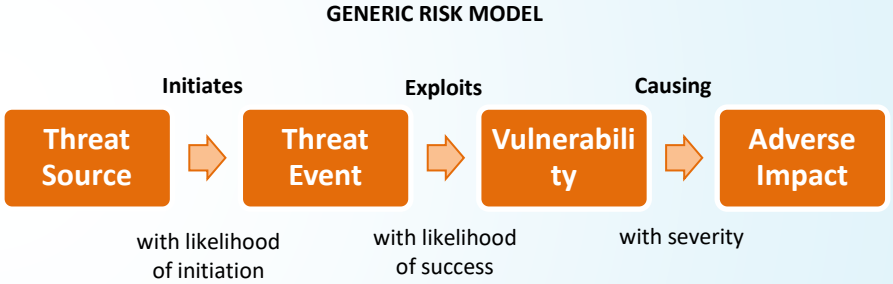
2. A better way

Measure Risk: Risk Framework & Model

Open FAIR™



NIST sp800-30 Risk Management guide



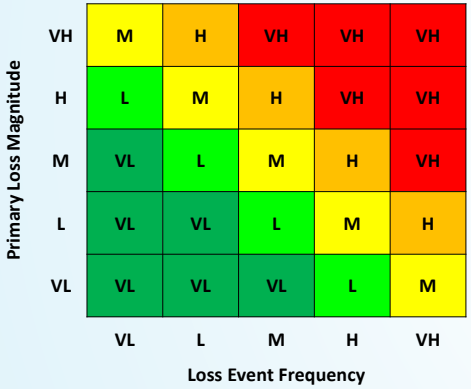
2. A better way

Build Scenarios | Prioritize | Measure Risk | Reporting

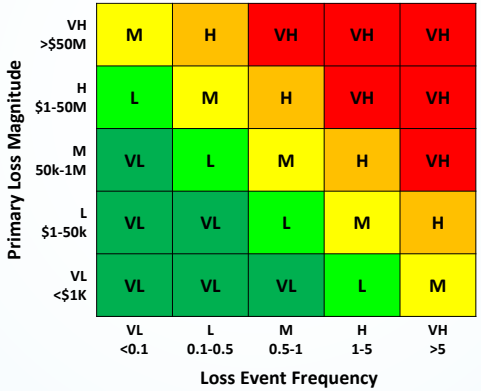
GRC CONFERENCE 2022
IIA | ISACA

Measure Risk: Assessment approach

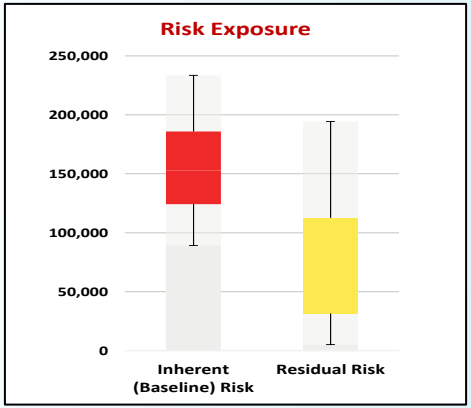
Qualitative
Ordinal scales / Non-numerical



Semi-Quantitative
Interval scales / Bins



Quantitative
Ratio scales / Numerical

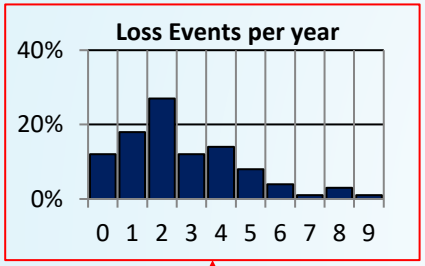


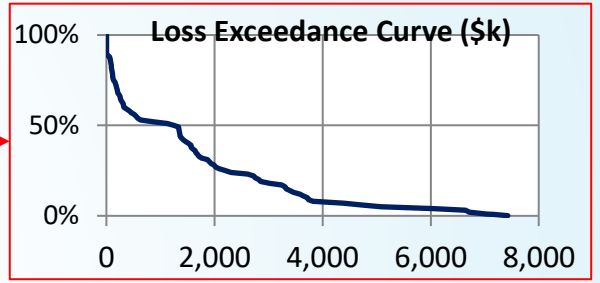
Objective measurements

2. A better way

GRC CONFERENCE 2022
IIA | ISACA

Measure Risk: Example – Measuring risk using Open FAIR (Quantitative)





Risk

The forecast annualized risk of this scenario

$1,535,800

Loss Event Frequency

Derived from estimates of Threat Event Frequency and Vulnerability

Loss Magnitude

Derived from estimates of Primary and Secondary Loss

Threat Event Frequency

Minimum: 0.5
Most Likely: 4
Maximum: 8

Vulnerability

Minimum: 0.3
Most Likely: 0.7
Maximum: 0.9

Primary Loss

Minimum: $40,000
Most Likely: $76,000
Maximum: $216,000

Secondary Loss

Minimum: $800,000
Most Likely: $1,346,000
Maximum: $2,000,000

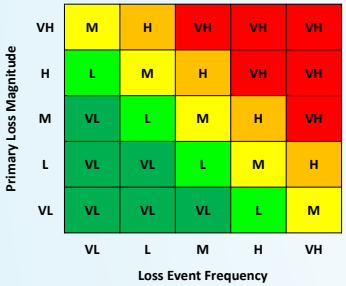
2. A better way

Build Scenarios | Prioritize | Measure Risk | Reporting

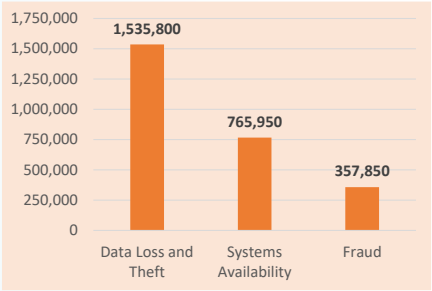
GRC CONFERENCE 2022
IIA | ISACA

Reporting: Selecting the report type depends on organizational culture and risk management knowledge

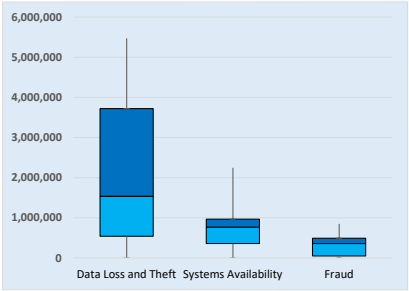
A. Qualitative



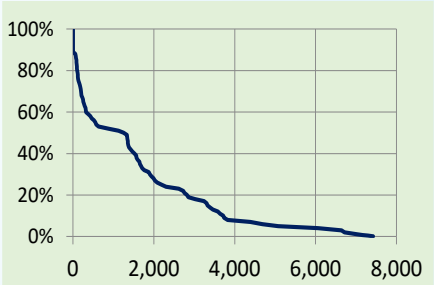
B. Annualized Risk Exposure



C. Box-and-whisker Plot



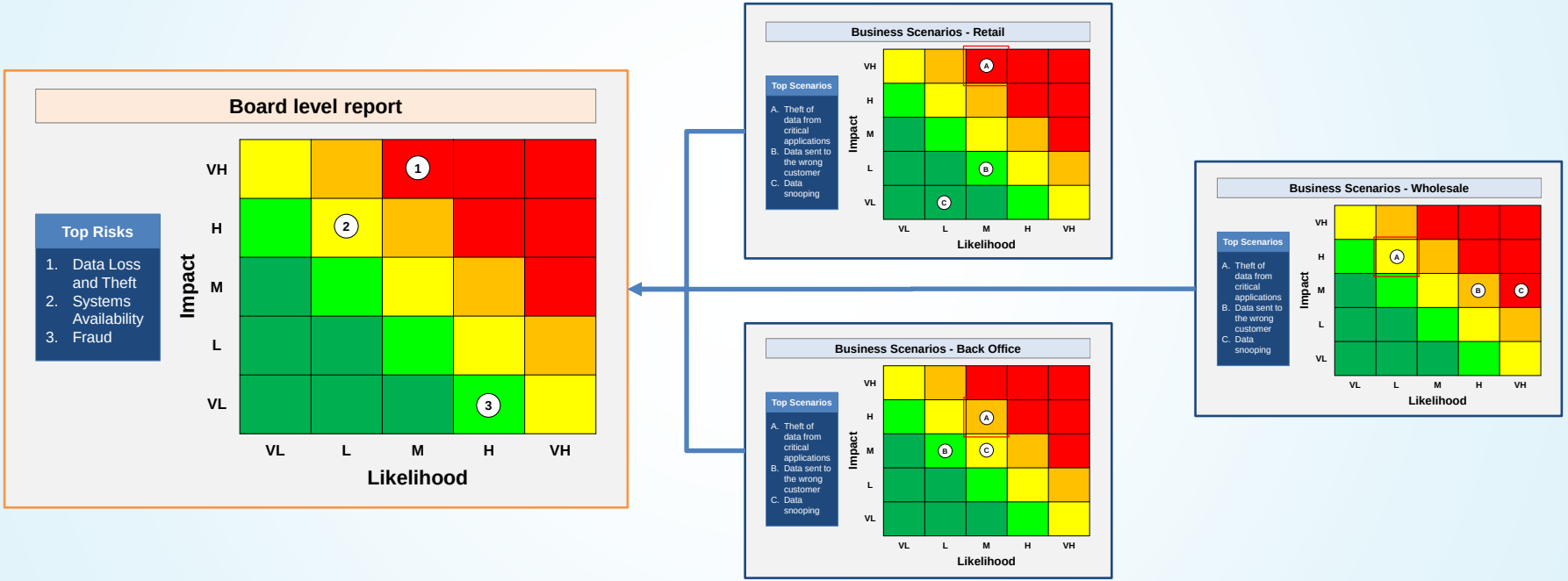
D. Loss Exceedance Curve



Complexity on interpretation

2. A better way

Reporting: Example – Qualitative risk aggregation / consolidation



2. A better way

GRC CONFERENCE 2022
IIA | ISACA

Reporting: Example – Reporting guidelines

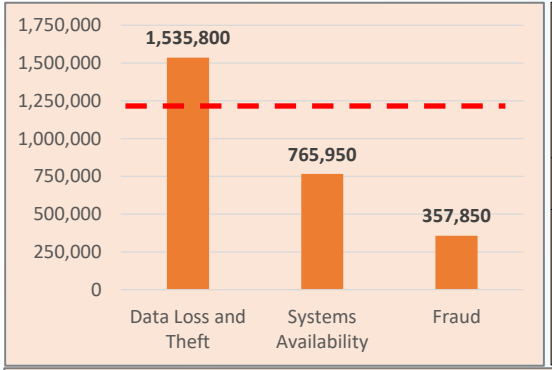
1 Header

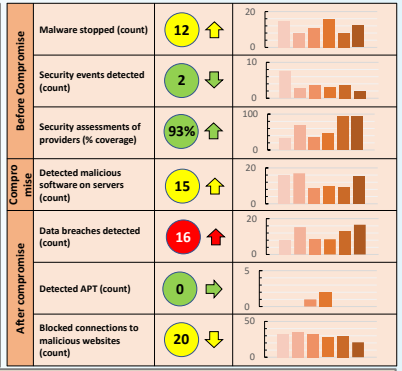
2 **Diagram** with Cyber Risk Characterization & Risk Appetite

3 **Risk Metrics** (KRI, KPI, KCI) or other relevant info

4 **Description** of the risks, business impacts, and mitigation activities

Example - Cyber Risk Analysis Report





Data Loss and Theft: Phishing attacks continue to be our top cyber threat. In our last quarter we enhanced our phishing training and simulation exercises, specially on Retail employees with access to our "Analytics Data Warehouse" crown jewel. In addition, we recently reviewed our Data Loss Prevention policies and rules, effectively boosting our detection capabilities for data exfiltration.

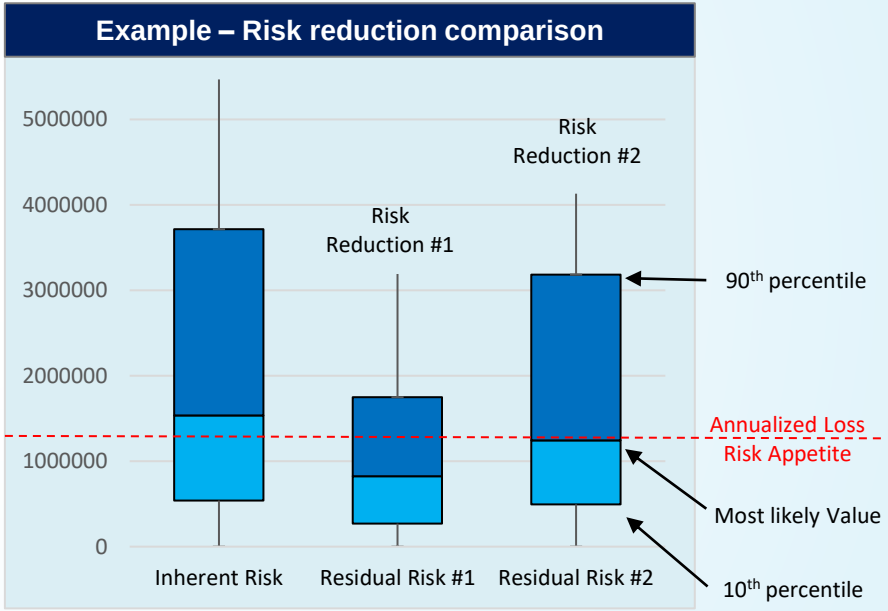
2. A better way

Build Scenarios | Prioritize | Measure Risk | Reporting

GRC CONFERENCE 2022
IIA | ISACA

Reporting: Example - Benefits of quantitative risk reporting

- Better articulation of residual risk vs the risk appetite
- Compare return on investment (ROI) of cybersecurity initiatives
- Effectively support business decisions and prioritization of mitigation efforts
- Improve business accountability / risk ownership.



3. Conclusion

There is a better way!

- Focus on communicating a clear characterization of risk. Enable business to make effective comparisons and well-informed decisions.
- Prioritize, keep it simple, and be objective. Pursue the quantitative approach to measure risk.
- Select the report that fits the organization culture & risk management practices. Train directors & senior executives on cybersecurity matters.
- Never stop fostering “the better way!”

GRC CONFERENCE 2022
IIA | ISACA

THANK YOU!

DON’T FORGET TO FILL OUT THE SESSION SURVEY AFTER THIS AND EVERY SESSION!