RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: GRC-R11

Math is Hard: Compliance to Continuous Risk Management

Max Blumenthal

Senior Cyber Assurance Architect
Sandia National Laboratories
https://www.linkedin.com/in/maxblumenthal

Christie Gross

Cybersecurity Solutions Engineer Lead
Delta Dental of California
https://www.linkedin.com/in/christiegross

State of Cyber Risk Management

According to the December 2018 Tenable *Measuring & Managing the Cyber Risks to Business Operations* study:

Less than half of organizations measure the business costs of cybersecurity risk

Only 38% of organizations believe their measures of business cost of cyber risk to be very accurate

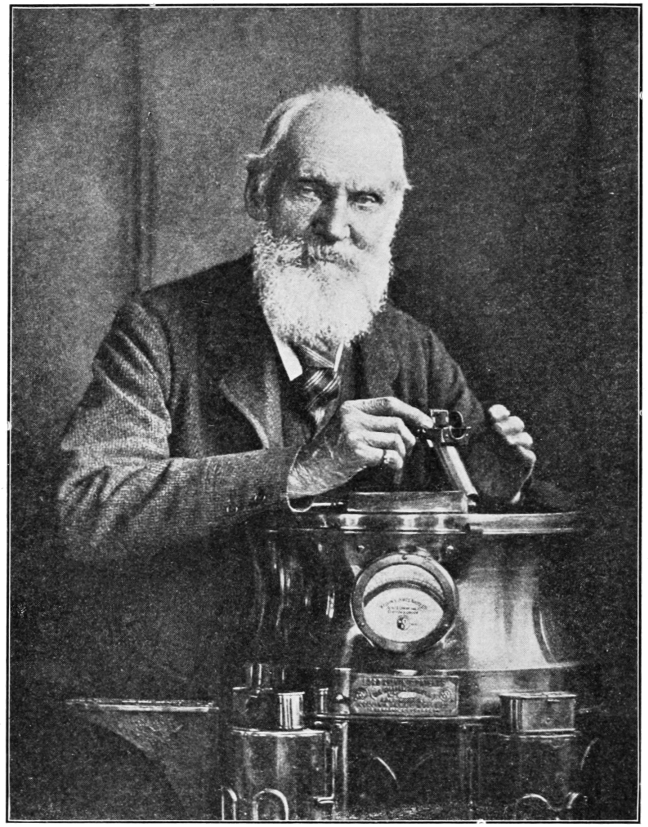
Why Risk Management?

How does your organization identify, monitor, and communicate the value and effectiveness of its cybersecurity program?

How does your organization identify, prioritize, and address top cybersecurity risks?

How does your cybersecurity program gain buy-in to mature from a compliance mindset to a quantitative risk based mindset?

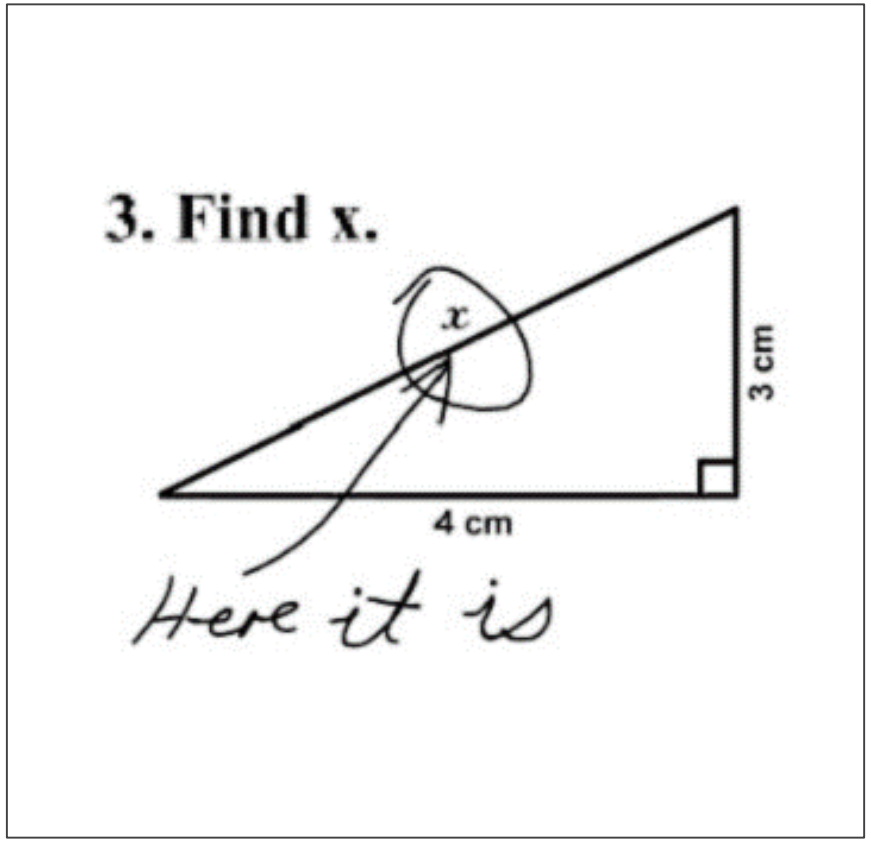
Lord Kelvin



- “When you can measure what you are speaking about, and express it in numbers, you know something about it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts advanced to the stage of science.”
- "I can state flatly that heavier than air flying machines are impossible."

Topics

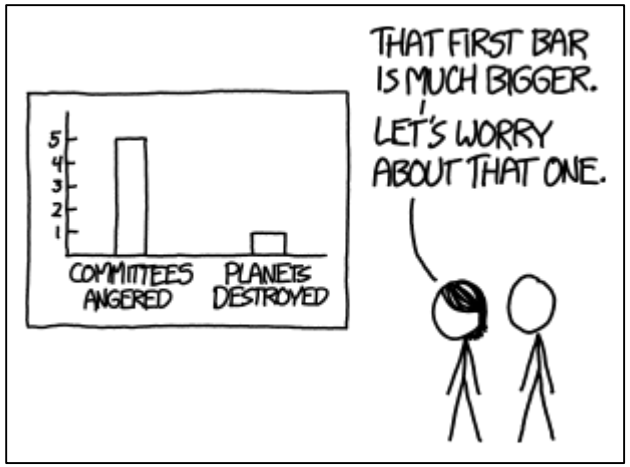
- Identifying Your Risk Management Goals
- Selecting a Risk Management Framework
- Implementing Continuous Monitoring
- Maturing Your Risk Assessment Method
  - Qualitative
  - Semi-Quantitative
  - Quantitative
- Advanced Methods for Gap Analysis
- Quick Start Guide



- Note: Opinions expressed are solely our own and do not necessarily express the views/opinions of organizations we work for.

Goals of Risk Management

- Frameworks are moving towards a risk-based approach
- Customers increasingly want proven security maturity (competitive edge)
- Reduce waste, prioritize relevant security, and avoid fear mongering
- Make better, more efficient, and cost-effective decisions



https://what-if.xkcd.com/imgs/a/147/consequences.png

Initial Steps to Ensure Buy-in

Identify Champions

Tie to Business Goals/Objectives

Have industry-relevant use cases ready

Conduct a proof-of-concept

Common Issues to Avoid

Unproductive Criticism of Current Approach

- Focus on ideas that move toward process maturation

Failing to Receive Input from Stakeholders

- Ensure that the planning process is inclusive

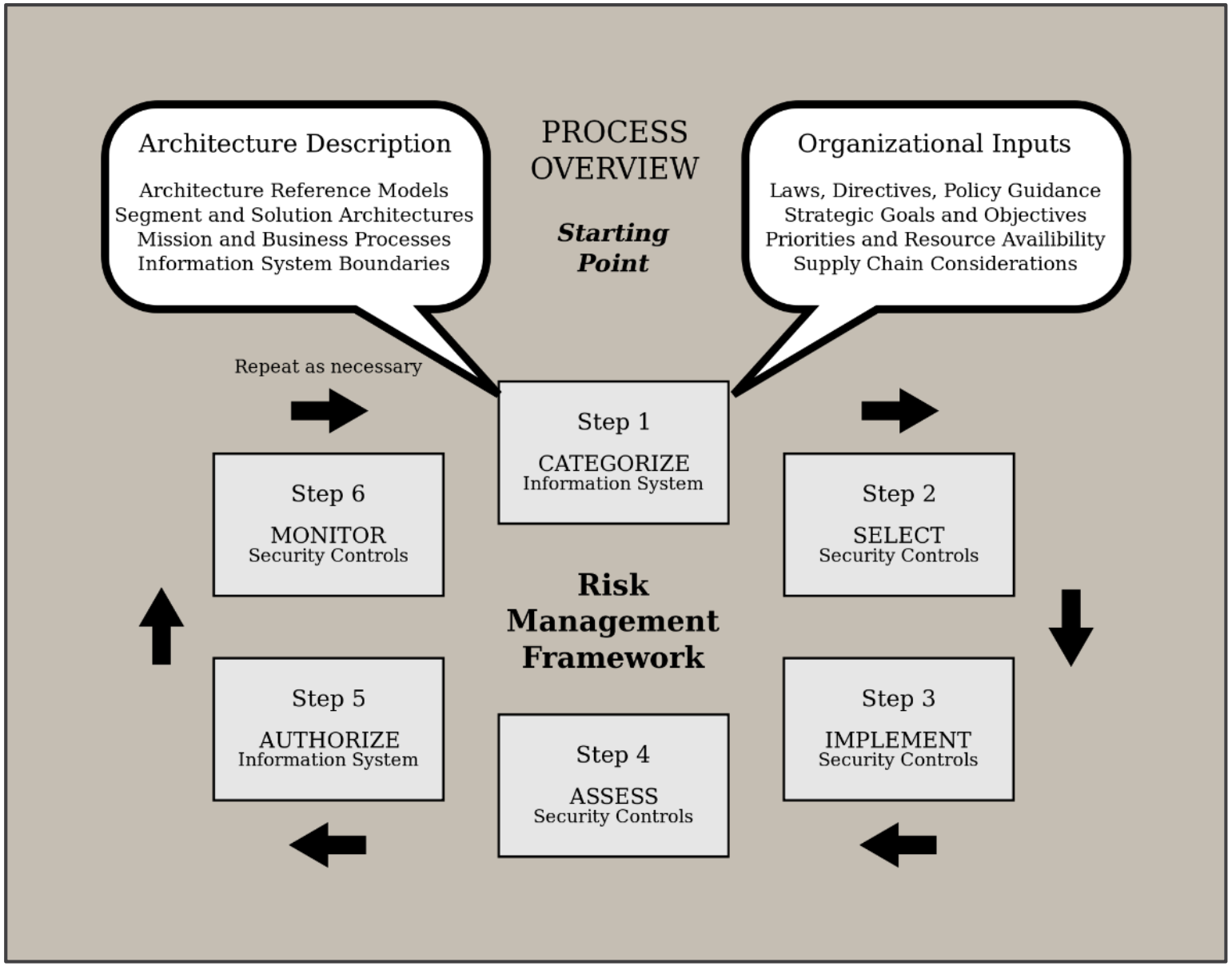
Over Promising

- Ensure that implementation plan scope is reasonable

Failing to Accept Constructive Comments

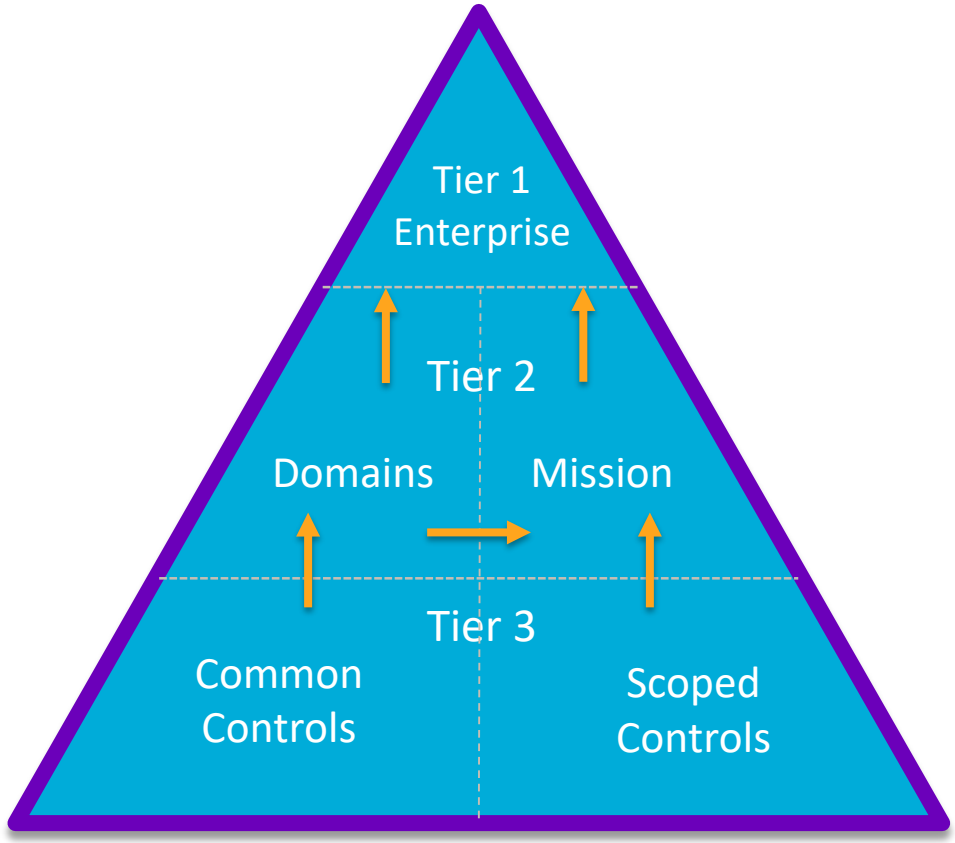
- Be open to different approaches to continuous risk management

NIST Risk Management Framework



Implementing Continuous Monitoring

- Identify gaps via the assessment process and ongoing monitoring
- Identify criteria & implement
  - Select metrics that determine continual effectiveness of controls
  - Evaluate security posture at different levels of the enterprise
- Feed effectiveness of controls into risk management and analysis



Continuous Monitoring Metric Selection

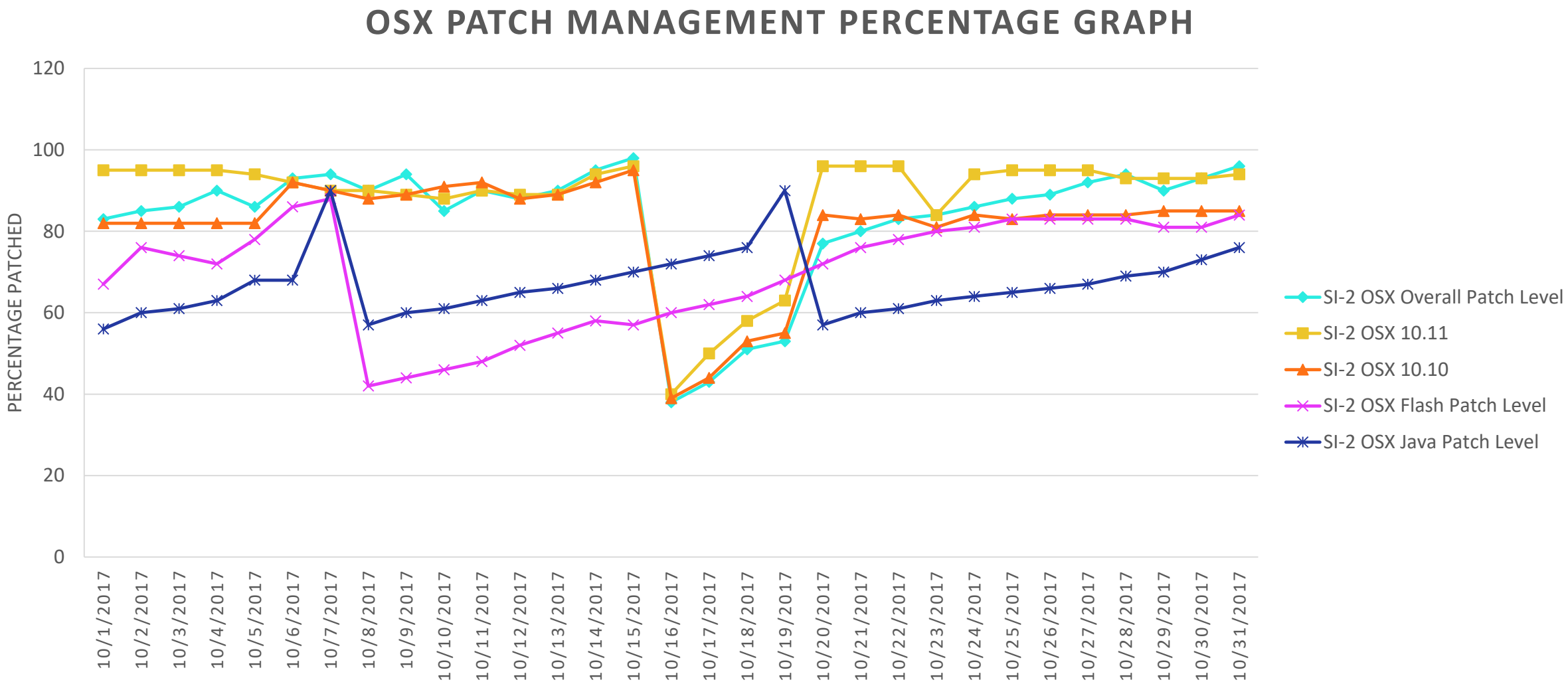
- Select metrics based on program maturity, available data, and organizational areas of value and criticality

Business Unit – e.g. Finance, IT

IT Process – e.g. Change Management, Account Management

Application or Technology – e.g. Active Directory, Critical Applications

Tier 3 – Analyst Level Reporting



Tier 3 – Analyst Level Reporting

Control Number	Control Name	Measure	Criticality	Current State	Alert Level	Weighted	Ideal
CM-3	Configuration Change Control	Time to implement change	High	93.00		279.00	300
MA-2	Controlled Maintenance	Time to resolve unscheduled maintenance	Low	97.00		97.00	100
RA-5	Vulnerability Scanning	% of scan population that is vulnerable	Very High	54.60		218.40	400
SI-2	Patch Management	% patched	High	39.80		119.40	300
Total Vulnerability & Patch Management	**Total Vulnerability & Patch Management**			**64.89**		**713.80**	**1,100**

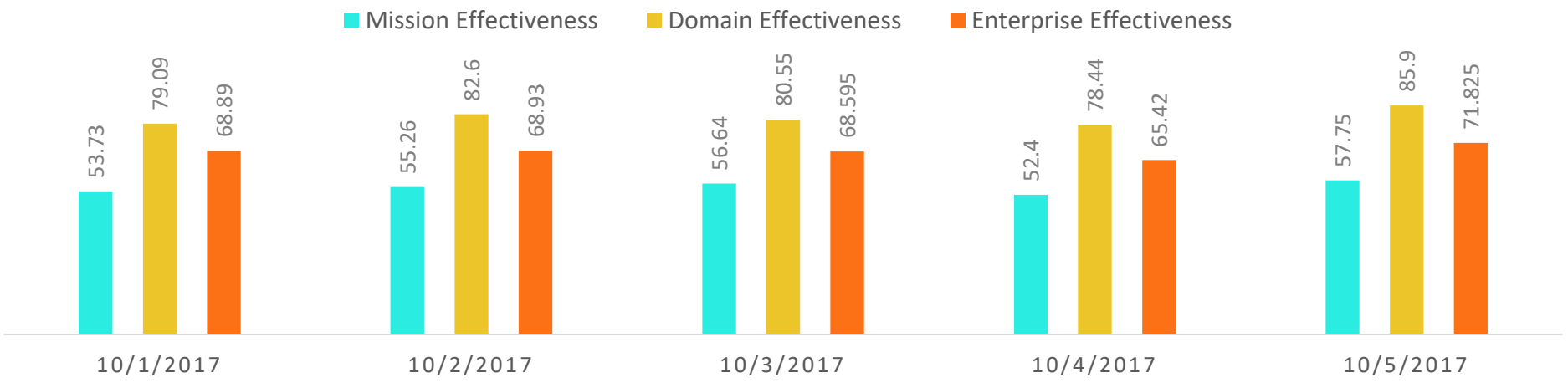
Tier 2 – Management Level Reporting

Domain	Percentage	Alert Level	Weighted	Ideal
Vulnerability and Patch Management	79.40		873.35	1,100
Configuration Management	57.82		1,214.16	2,100
Asset Management	83.63		752.64	900
Event and Incident Management	85.93		945.27	1,100
Domain Total	72.80		3,785.42	5,200

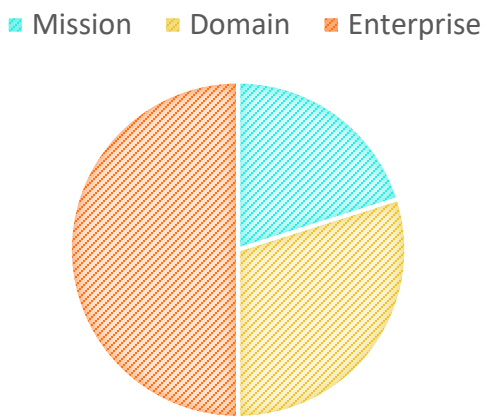
Tier 1 – Executive Level Reporting

Enterprise Entity	Percentage	Alert Level	Weighted	Ideal
Mission Total	53.73		1,880.57	3,500
Domain Total	79.09		4,112.81	5,200
Enterprise Total	**68.89**		**5,993.38**	**8,700**

ENTITY EFFECTIVENESS



ENTITY IMPACTS



From Monitoring to Risk Quantification

Using Continuous Monitoring data, we can determine our risk exposure

Once quantified, these risks can be prioritized

Multiple methods of risk analysis - qualitative, semi-quantitative, quantitative

Hybrid approaches can garner more buy-in without a major culture shock

Evolution of Risk Analysis

IMPACT	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

LIKELIHOOD

LIKELIHOOD	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

High ↑ Low; CONSEQENCES; Low ← → High

Risk
High
Medium
Low

Figure 4

Risk Assessment Matrix

Frequency (likelihood of occurrence)	Severity (consequences of incident)				
	Incidental < $10K	Minor $10 to 25K	Serious $25 to 100K	Major $100 to 500K	Catastrophic $500K >
Every year	5	10	15	20	25
1 to 5 years	4	8	12	16	20
5 to 10 years	3	6	9	12	15
> 10 years	2	4	6	8	10
Almost never	1	2	3	4	5

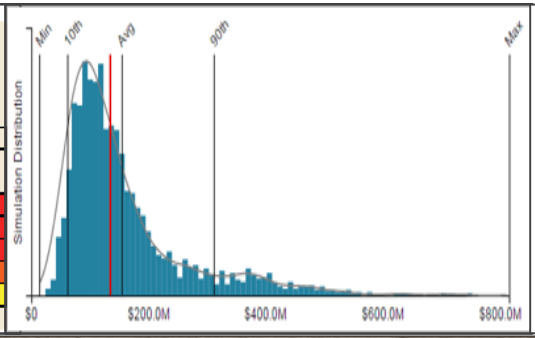
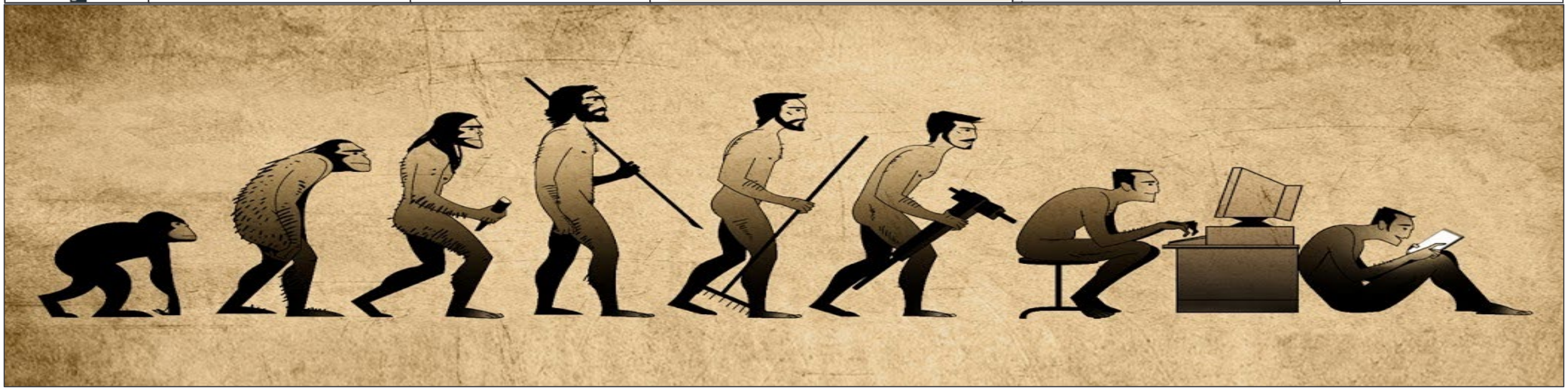


Figure 4 - Example Risk Heat Map

Likelihood \ Impact	1	2	3
3			
2			
1			



Risk Matrices: What Not to Do

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Risk Matrix Goals

Easily Understood → Defensible → Actionable

Mathematically-Sound Risk Matrix

Likelihood				
5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5
		Impact		

Qualitative Risk

- No Definition for Each Value
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Subjective, but Simple

Mathematically-Sound Risk Matrix

Likelihood				
5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5
	Impact			

Common Questions

- What does a 12 mean?
- What's the difference between an impact of 3 and an impact of 4?
- Do we prioritize likelihood or impact?

Semi-Quantitative Risk Matrix

	1	2	3	4	5	6	7
5	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00	$ 1,000,000,000.00
4	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00
3	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00
2	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00
1	$ 0.10	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00

Semi-Quantitative Risk

- Definition for Each Risk Value
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Useful for Mitigation Selection

Semi-Quantitative Risk Matrix

	1	2	3	4	5	6	7
5	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00	$ 1,000,000,000.00
4	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00
3	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00
2	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00
1	$ 0.10	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00

Common Questions

- How did you select values?
- What if I'm unsure about the likelihood or impact score?
- Do we prioritize by expected loss?

Quantitative Risk Method

Risk	LEF	TEF	Vulnerability	Tcap	RS	LM	Productivity Loss	Other Loss
$ 15,328.00	2.5	25	0.1	0.85	0.8	6131.2	$ 6,131.20	0
Sample	Risk		Average	$ 558,725.46				
1	$ 15,328.00		standard	$ 1,565,137.07				

	Productivity Loss	Other Loss	Avail Loss	Confidentiality Loss	Tcap	RS	TEF
Low	$ 2,295.54	Availability	$ 1,000.00	$ 2,745,500.00	85%	75%	15
Most Likely	$ 4,213.37	$ -	$ 9,600.00	$ 9,754,005.00	95%	80%	25
High	$ 6,131.20	Confidentiality	$ 10,000.00	$ 16,314,050.00	100%	85%	40

Quantitative Risk

- Incorporates Continuous Monitoring and Threat Information
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Useful for Mitigation Selection
- Utilizes simulation to build a range of risk, given inherent uncertainties

Quantitative Risk Method

Risk	LEF	TEF	Vulnerability	Tcap	RS	LM	Productivity Loss	Other Loss
$ 15,328.00	2.5	25	0.1	0.85	0.8	6131.2	$ 6,131.20	0
Sample	Risk		Average	$ 558,725.46				
1	$ 15,328.00		standard	$ 1,565,137.07				

	Productivity Loss	Other Loss	Avail Loss	Confidentiality Loss	Tcap	RS	TEF
Low	$ 2,295.54	Availability	$ 1,000.00	$ 2,745,500.00	85%	75%	15
Most Likely	$ 4,213.37	$ -	$ 9,600.00	$ 9,754,005.00	95%	80%	25
High	$ 6,131.20	Confidentiality	$ 10,000.00	$ 16,314,050.00	100%	85%	40

Common Questions

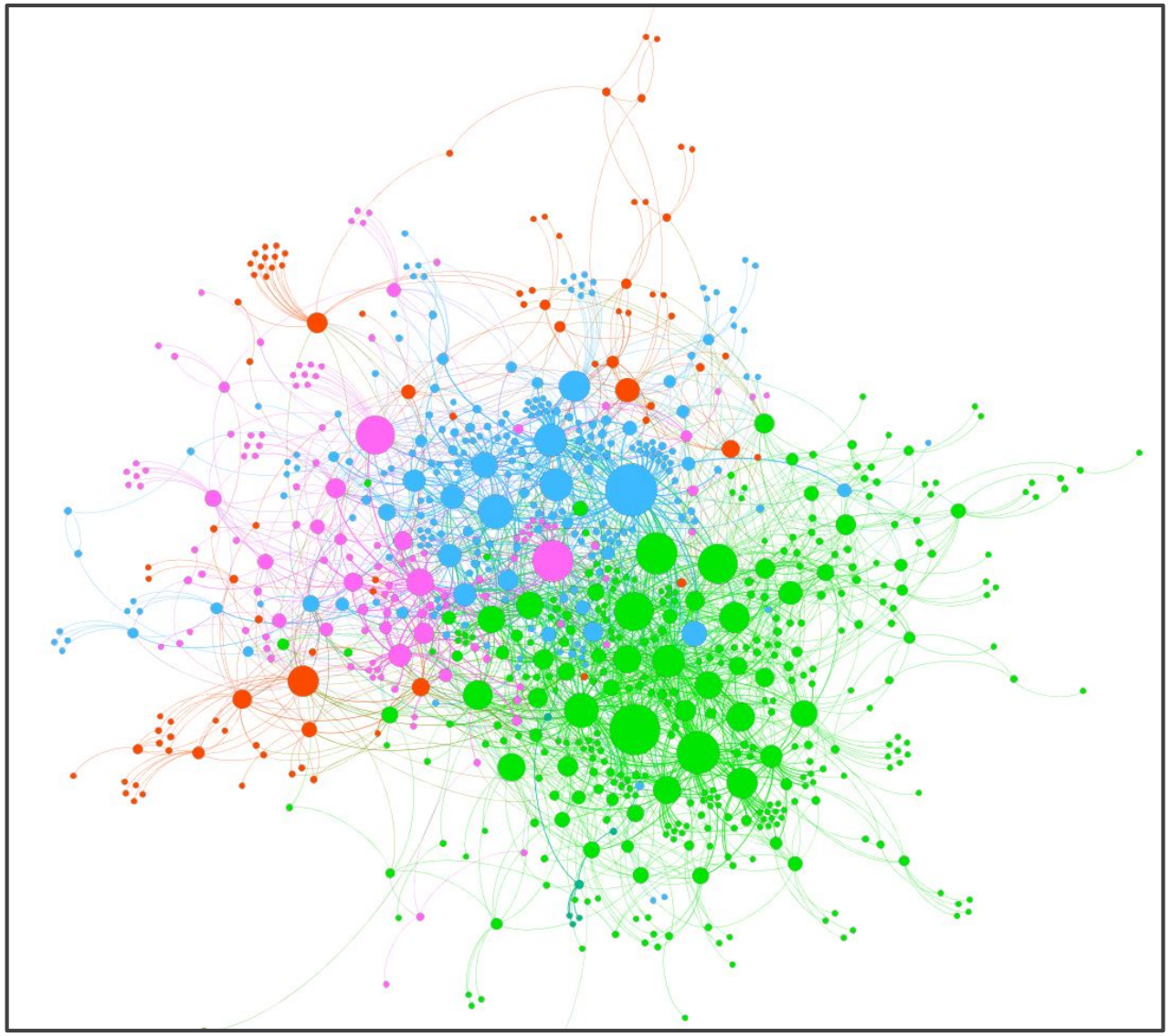
- Why is there so much uncertainty?
- This seems overly complicated. Why would we not do something simple?
- Does this mean we have a “yellow” risk?
- That number seems off. How can I trust any of this?

Quantitative Example

AVAILABILITY

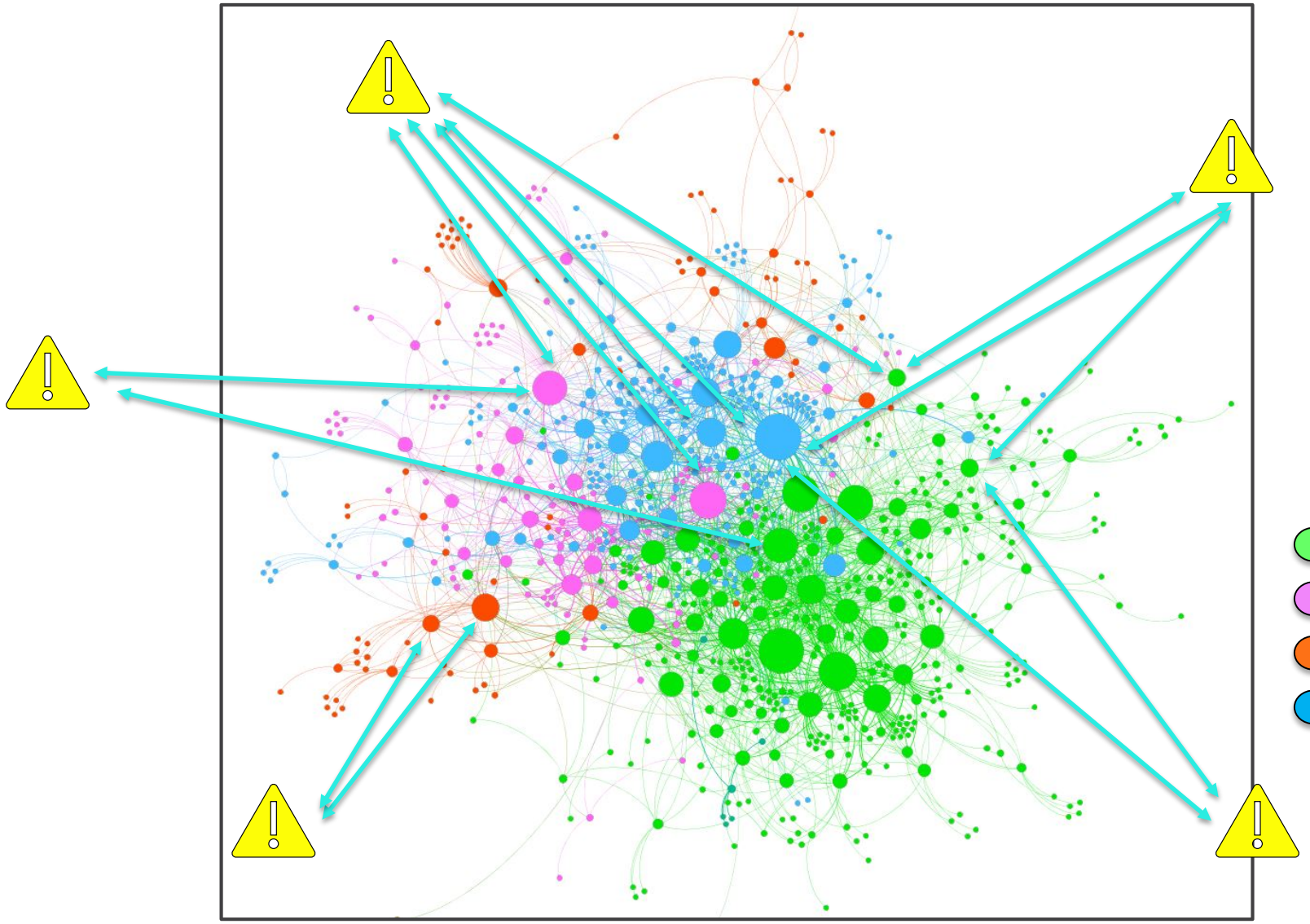
- Assume a 10,000 employee organization has a target uptime of 99.8% for their core network. The average fully-loaded cost/employee is $200/hr and works 2000hrs/year (40hrs/wk x 50wks/yr)
- 99.8% uptime = network is down for 4 hours/year.
- Estimate that between 1,000 and 10,000 employees affected by that 4hr of downtime = $800k to $8mil in lost productivity
- If uptime can be increased to 99.9%, then expected productivity loss is halved

Control Mapping for Gap Analysis



- Configuration/Asset Management
- Vulnerability/Patch Management
- Physical/Environmental Management
- Event/Incident Management

Threat-Centric Gap Analysis



- Configuration/Asset Management
- Vulnerability/Patch Management
- Physical/Environmental Management
- Event/Incident Management

Quick Start Guide to Risk Management

Take initial steps to foster buy-in with applicable use-cases and proof-of-concepts

During implementation, map applicable policies to identify areas of focus and potential gaps

Use manual and automated monitoring of individual policies to measure ongoing effectiveness

Create reports at multiple tiers to identify effectiveness at different levels of the enterprise

Feed continuous monitoring data into risk analysis solutions

Utilize quantitative risk to prioritize weaknesses and determine appropriate mitigations

Apply What You Have Learned Today

Next Week

- Identify partners to foster buy-in with applicable use-cases and proof-of-concepts

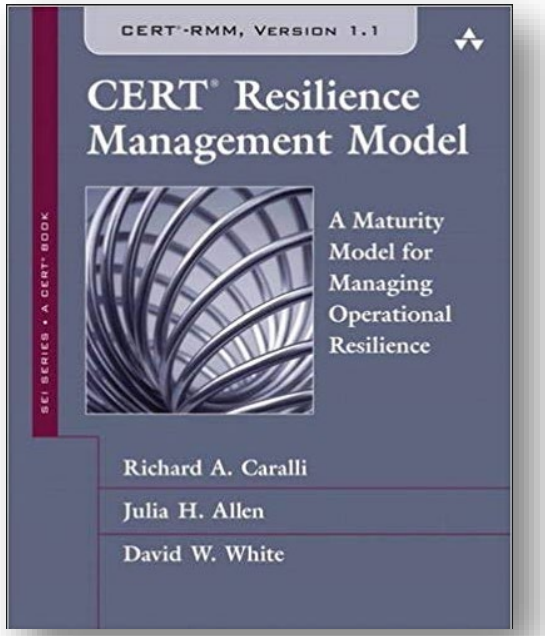
First 3 Months

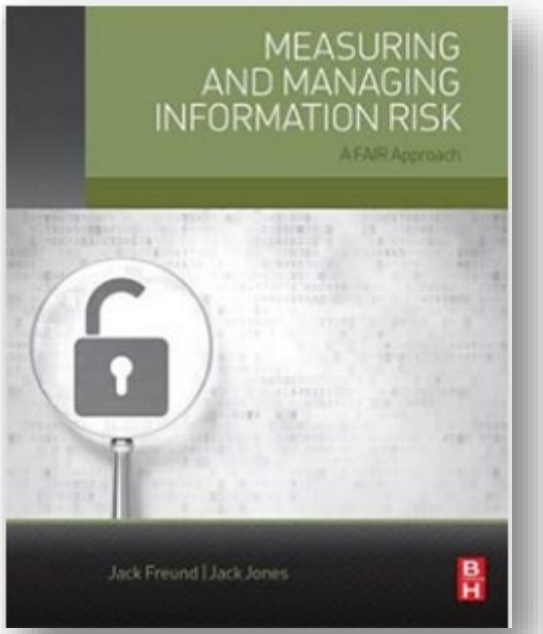
- Understand your current risk management maturity
- Develop a roadmap to implement quantitative risk management

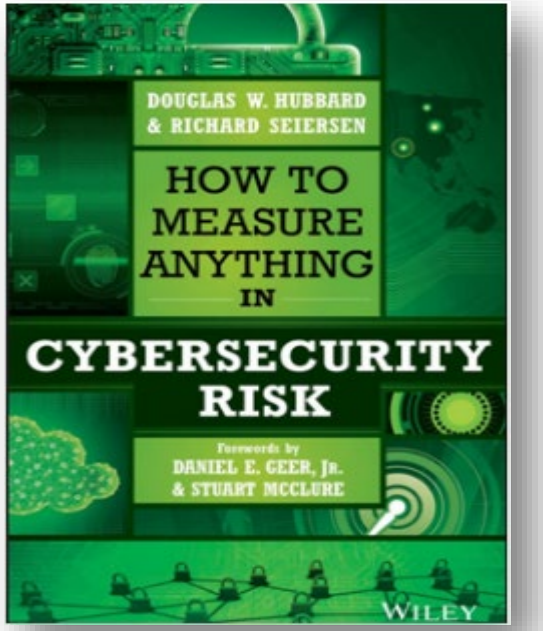
Within 6 Months

- Begin implementation of automated monitoring of control effectiveness
- Utilize quantitative methods to prioritize weaknesses and determine risk

Recommended Reading







Publicly Available Data Sources

- Verizon DBIR
- Ponemon Cost of Data Breach Reports
- ITIC Hourly Cost of Downtime Surveys
- IAPP Data Breach Calculators
- Value of Statistical Life (VSL) estimates
- Court settlements/fines

BETTER.

SESSION ID: GRC-R11

Questions?

Max Blumenthal

Senior Cyber Assurance Architect
Sandia National Laboratories
https://www.linkedin.com/in/maxblumenthal

Christie Gross

Cybersecurity Solutions Engineer Lead
Delta Dental of California
https://www.linkedin.com/in/christiegross