RSA

EXPERIENCES IN MANAGING RISK TO THE BULK ELECTRIC SYSTEM

michael.deloach@rsa.com

Michael Deloach

Executive Director - Risk Transformation Office

https://www.linkedin.com/in/mikedeloach/

Michael DeLoach is a thought leader in the utility space. His holistic risk perspective is grounded in over 25 years of leadership in areas of the business including engineering, information technology, cybersecurity, reliability, security and regulatory compliance.

- Senior executive at two major utilities leading reliability and security compliance organizations
- Former member of the NERC Compliance and Certification Committee
- led Integrated Risk Management transformation to improve adherence and visibility of compliance posture
- Implemented a standardized method for assessing and ranking risks to the North American Bulk Electric System to help organizations prioritize investments and scale responses to control deficiencies

Michael holds a bachelor's degree in Electrical Engineering from Clemson University and an MBA from Ohio University.

Michael leads **Utilities** and **Telecommunications** for the Risk Transformation Office.

RSA

RISK PERSPECTIVES

- Definitions Vary…
  - Something that might happen that would **adversely affect** your organization's ability to achieve its **objectives**
  - (**Probability** something bad will happen) x (**Consequences** if it does happen)
  - Sometimes confused with other concepts (e.g., spear phishing = threat, cloud computing platform = asset)
- Should be expressed **in context** – e.g., defined with respect to a particular asset
- Best when based on **objective data** (but this is not always possible)
- Can be assessed **retrospectively** and **prospectively**
- Key challenge: **measuring and communicating** risk in a **consistent, repeatable** manner such that effective **comparisons** can be made for improved **decision making**

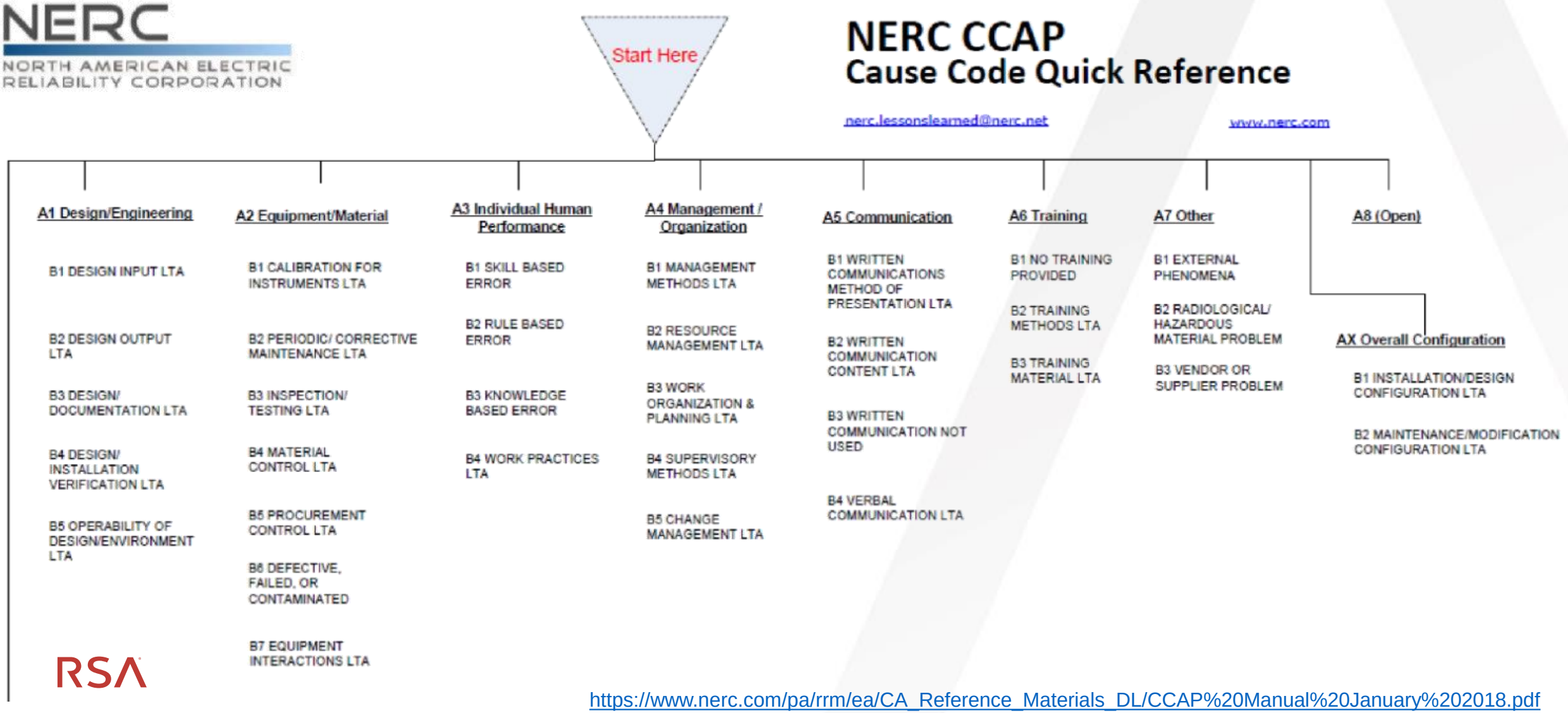
RISK-HARM ASSESSMENT REVIEW

RSA

RISK-HARM METHODOLOGY

- Based on ReliabilityFirst's risk assessment methodology
- Focused on risk to the Bulk Electric System (BES)
- Integrated into the incident management process at AEP and Duke (started)
- Introduced a consistent, repeatable approach to assessing potential compliance issues
- Performed by teams of risk assessors who were trained and calibrated
- Leveraged NERC's Cause Code Assignment Process (CCAP) as a means of identifying and trending causes ranked by risk

CAUSE ANALYSIS



RSA

https://www.nerc.com/pa/rrm/ea/CA_Reference_Materials_DL/CCAP%20Manual%20January%202018.pdf

RISK-HARM QUESTIONS

Methodology involves asking and answering (5) questions (each with a 90% confidence level):

Question 1: Probability of Recurrence

Estimate the likelihood of the violation occurring again or continuing to occur if the root cause remains.

Statement	Vote	Odds
High	1	1 in 1
High	2	1 in 3
Serious	3	1 in 8
Serious	4	1 in 20
Unlikely	5	1 in 80
Unlikely	6	1 in 400
Unlikely	7	1 in 1,000
Minimal	8	1 in 15,000
Minimal	9	1 in 150,000
Not Likely	10	< 1 in 1,500,000

RISK-HARM QUESTIONS

Methodology involves asking and answering (5) questions (each with a 90% confidence level):

Question 2: Likelihood of Detection
Estimate the likelihood the control environment and related activities would detect the violation.

Statement	Vote	Likelihood of Detection
Almost Impossible	1	50.0%
Very Remote	2	80.0%
Remote	3	82.0%
Very Low	4	85.0%
Low	5	87.5%
Moderate	6	90.0%
Moderately High	7	92.5%
High	8	95.0%
Very High	9	97.5%
Almost Certain	10	99.5%

RISK-HARM QUESTIONS

Methodology involves asking and answering (5) questions (each with a 90% confidence level):

Question 3: Probability of Side Effects

Estimate the likelihood of a different violation occurring if the root cause remains.

Statement	Vote	Odds
High	1	1 in 1
High	2	1 in 3
Serious	3	1 in 8
Serious	4	1 in 20
Unlikely	5	1 in 80
Unlikely	6	1 in 400
Unlikely	7	1 in 1,000
Minimal	8	1 in 15,000
Minimal	9	1 in 150,000
Not Likely	10	< 1 in 1,500,000

RISK-HARM QUESTIONS

Q4 - Estimate the potential harm to the reliability of the bulk electric system caused by the violation.

Name	Rank	Loss of Equipment	Loss of Generation/Load	Loss of Visibility	System Restoration
Extreme	1	Loss of more than three (3) pieces of BES equipment of > 200 kV. Loss of more than three substations ≤ 200 kV	Unintended loss of load and/or generation > 10,000 MWs	EMS, ICCP, SCADA - 100% Data Affected -or- Loss of visibility of multiple Utilities' (or TOs) transmission and generating substations	System Restoration Time greater than 24 hrs following an event
Substantial	2	Loss of up to three (3) pieces of BES equipment > 200 kV. Loss of up to three (3) substations ≤ 200 kV	Unintended loss of load and/or generation from 5,000-to-10,000 MWs	EMS, ICCP, SCADA - 75% Data Affected -or- Loss of visibility of a single utility's (or TO) transmission and generating substations	System Restoration Time from 18-24 hrs following an event
Intermediate	3	Loss of a single piece of BES equipment > 200 kV. Loss of up to three (3) pieces of BES equipment ≤ 200 kV	Unintended loss of load and/or generation from 999-to- 4,999 MWs	EMS, ICCP, SCADA - 50% Data Affected -or- Loss of visibility of multiple transmission or generating substations (or RTUs)	System Restoration Time from 12-16 hrs following an event
Minor	4	Loss of a single piece of BES equipment ≤ 200 kV	Unintended loss of load and/or generation from 300-to-999 MWs	EMS, ICCP, SCADA - 50% Data Affected -or- Loss of visibility of one transmission or generating substation (or RTU)	System Restoration Time from 6-12 hrs following an event
None	5	No loss of any BES equipment	Unintended loss of load and/or generation < 300 MWs	EMS, ICCP, SCADA - less than 25% Data Affected	No impact on system recovery following an event

RSA

RISK-HARM QUESTIONS

Methodology involves asking and answering (5) questions (each with a 90% confidence level):

Question 5: Probability of Harm
Given your answer to question four, estimate the likelihood of potential harm actually occurring.

Statement	Vote	Odds
High	1	1 in 1
High	2	1 in 3
Serious	3	1 in 8
Serious	4	1 in 20
Unlikely	5	1 in 80
Unlikely	6	1 in 400
Unlikely	7	1 in 1,000
Minimal	8	1 in 15,000
Minimal	9	1 in 150,000
Not Likely	10	< 1 in 1,500,000

SAMPLE RISK-HARM ANALYSIS

Scenario:

- While **commissioning** a new generating station **control system**, a **network switch** was **misconfigured** to have an **overly permissive ruleset**.

- **Violation of NERC CIP-007 R1.1**, which requires that **only ports and services that are needed** for reliable operation **shall be opened / enabled**.

- Cause was found to be: A3 > B4 > C05:
  Mgmt Methods LTA > Supervisory Methods LTA > **Emphasis on Schedule Exceeded Emphasis on Methods** (Doing a good job)

SAMPLE RISK-HARM ANALYSIS

- Background Information
  - XYZ generating station has a **combined generating capability of 612 MW**. It has two generating units that are both controlled by a **common control system**.
  - This issue was **discovered while reviewing evidence** that was pursuant to an **upcoming SERC NERC CIP audit**.
  - Our company has been replacing control systems across our whole fleet. They have **completed control system replacements at 4 stations** and there are 2 more remaining to be completed. Total generating capacity at the 4 stations that have been completed is **3,450 MW**.

ASSESSMENT RESULTS (ROUND 1)

Question 1: Estimate the likelihood of the violation occurring again or continuing to occur if the root cause remains.				
Voter 1	1	1.0	0	I'm certain we have this issue elsewhere on the network. Granted, this was a rushed implementation, but it seems we're always in a rush. We've reduced the number of personnel who do this work and they are stretched super thin. Additionally, it appears that we lack the controls (e.g., checklists) that would help lower the likelihood of human errors when these rulesets are changed.
Voter 2	1 2	1.5	1	While I suspect we have this problem elsewhere, more research is needed to ensure that is the case. This may be limited to the Generation business unit.
Voter 3	1 2	1.5	1	I'm almost certain this problem exists elsewhere. More assessments should be performed at other locations.
Voter 4	2 4	3.0	2	I'm not convinced that this is not a one-off issue. The commissioning of this facility was rushed and I believe that is why this error occurred. Still, we need to look more broadly at our rulesets to make sure this is not a pervasive issue.
	Average	**1.8**	**57%**	**Consensus Level**

ASSESSMENT RESULTS (ROUND 1)

Question 2: Estimate the likelihood the control environment and related activities would prevent and/or detect the violation.				
Voter 1	1 3	2.0	2	Historically, we have not had a program whereby we review our rulesets, so I rated the detection rather unlikely. The only reason we found this one is because it was part of the data request for the upcoming audit by SERC.
Voter 2	1 2	1.5	1	We really need to be reviewing these rulesets as part of a program. Perhaps we should consider technology to help us detect situations where we depart from our baseline configurations.
Voter 3	1	1.0	0	Only found this one because of upcoming audit.
Voter 4	6 8	7.0	2	In Transmission, we have a configuration monitoring solution that would detect these kinds of issues, so I rated the likelihood of detection somewhat high. Of course, the answer to this question may be different if we're talking about an enterprise-wide perspective...
	Average	**2.9**	**16%**	**Consensus Level**

ASSESSMENT RESULTS (ROUND 1)

Question 3: Estimate the likelihood of a different violation occurring if the root cause remains.				
Voter 1	1 4	2.5	3	This is likely due to the rushed implementation performed by people who didn't really understand or take into account the compliance and security implications. Further, the lack of integration between IT and OT organizations and processes contributed to the situation.
Voter 2	1 3	2.0	2	The commissioning of XYZ was rushed for myriad reasons. Such rushed efforts frequently result in human errors being made. These errors can cause many issues -- beyond what happened in this situation.
Voter 3	1 2	1.5	1	People rushing, coupled with lack of tools / job aids to lower likelihood of human error could cause all kinds of problems.
Voter 4	1 2	1.5	1	Broadly speaking, we need to invest in more controls to help protect against human errors.
	Average	**1.9**	**78%**	**Consensus Level**

RSA

ASSESSMENT RESULTS (ROUND 1)

Question 4: Estimate the potential harm to the reliability of the bulk electric system caused by this violation.				
Voter 1	3 5	4.0	2	I based my harm rating on the fact that we have performed control system replacements at (4) stations with a combined generating capability of 3,450 MW. I expressed it as a range because it's possible errors were not made at other stations.
Voter 2	4 5	4.5	1	While we have not completed assessment of rulesets at the other (3) stations, those efforts were not as rushed as XYZ, so I rated harm based on impact to XYZ only.
Voter 3	2 4	3.0	2	Seems rushed implementations are becoming a more normal occurrence, so I rated harm based on potential that it could also impact EMS / SCADA implementations as well.
Voter 4	1 4	2.5	3	The potential harm of misconfigured switches and firewalls could have a huge impact. Note: this is not to say that it is likely (see my answer to question 5).
	Average	**3.5**	**77%**	**Consensus Level**

RSA

ASSESSMENT RESULTS (ROUND 1)

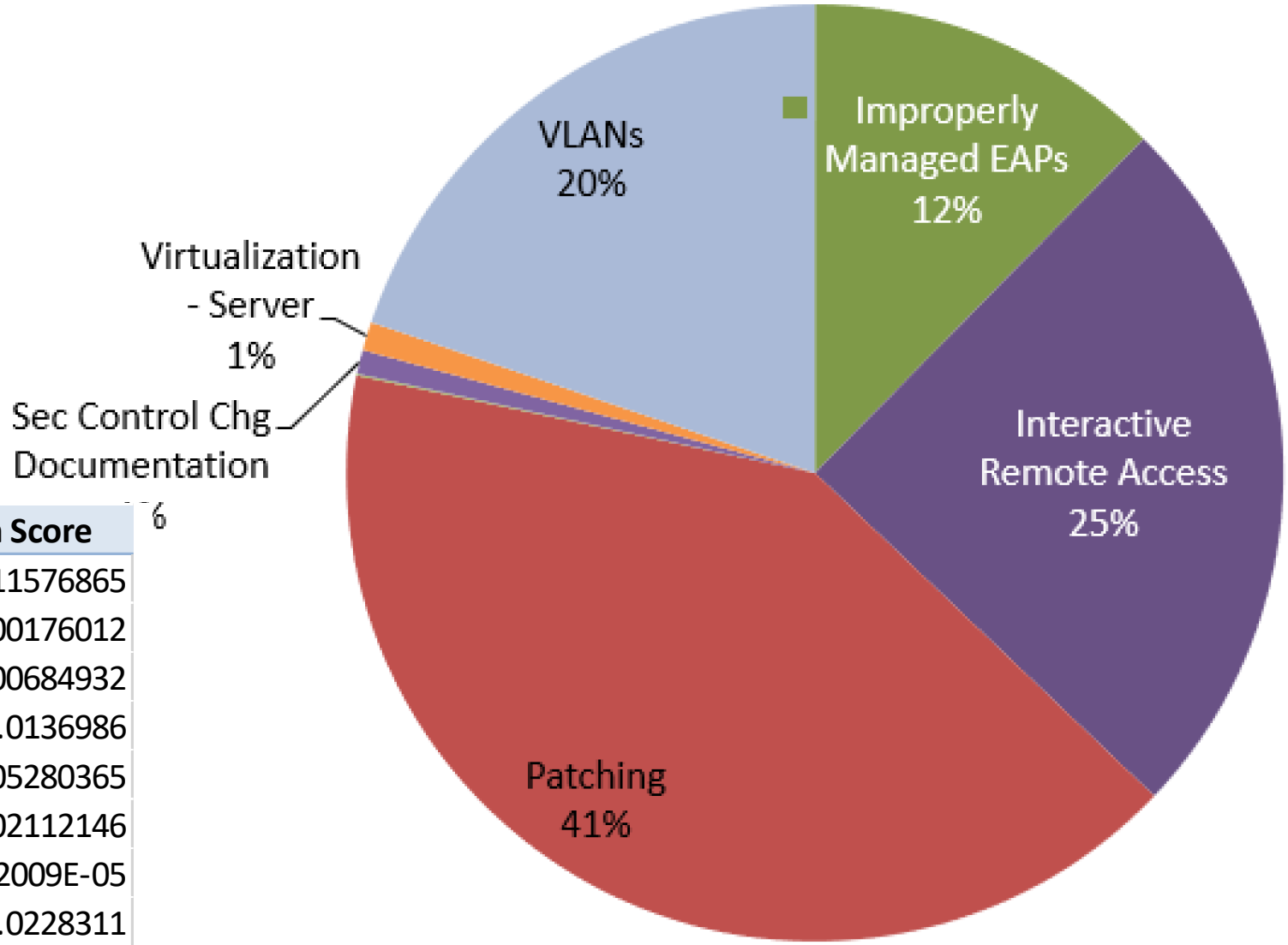
Question 5: Given your answer to question 4, estimate the likelihood of potential harm actually occurring.				
Voter 1	1 4	2.5	3	Depends on the threat actor. If a nation state, there is a higher probability they would be able to take advantage of this deficiency. It is worth noting that it really would not require an extrmely advanced adversary to use this vulnerability to their advantage.
Voter 2	2 6	4.0	4	Hard to say what the probability is precisely. Depends on the nature of the threat. It is worth noting that this was an internal switch that was misconfigured -- not one that is facing the internet -- so it would require a threat actor capable of getting past our outer perimeter.
Voter 3	7 10	8.5	3	Our outer perimeter would have to be compromised and we have solid controls there to ensure threat actors are deterred.
Voter 4	7 9	8.0	2	I rated the likelihood of actual harm low because when it comes to EMS/SCADA, we have detective controls in place that would alert us to the problem and we would close whatever holes we have in short order -- thus lowering likelihood of an actual external compromise.
	Average	**5.8**	**55%**	**Consensus Level**

ASSESSMENT RESULTS (ROUND 1)

	Risk-Harm Score is:	0.004870624049	**The RAC determination of the Risk-Harm is: Low Minor**

	Risk	Harm	Internal Rfirst Levels
1	Low	Minor	0.00000
2	Moderate	Minor	0.00500
3	High	Minor	0.00750
4	Low	Intermediate	0.01250
5	Moderate	Intermediate	0.02222
6	Low	Substantial	0.03030
7	High	Intermediate	0.03750
8	Moderate	Substantial	0.05000
9	Low	Extreme	0.06250
10	High	Substantial	0.07500
11	Moderate	Extreme	0.10000
12	High	Extreme	0.15000

RISK IN CONTEXT



Row Labels	Sum of Risk-Harm Score
AIC Ownership	0.011576865
Backdating Terms	0.000176012
Improperly Managed EAPs	99.00684932
Interactive Remote Access	198.0136986
Malicious Code Prevention	0.005280365
Multinet TFE	0.002112146
PACs Entitlements	1.32009E-05
Patching	330.0228311
Physical BCSI	0.478767123
Sec Control Chg Documentation	6.600456621
Segmentation	0.000638356
Virtualization - Server	7.920547945
VLANs	158.4109589

MORE ADVANCED RISK ASSESSMENT TECHNIQUES

FACTOR ANALYSIS OF INFORMATION RISK (FAIR) METHODOLOGY

RSA

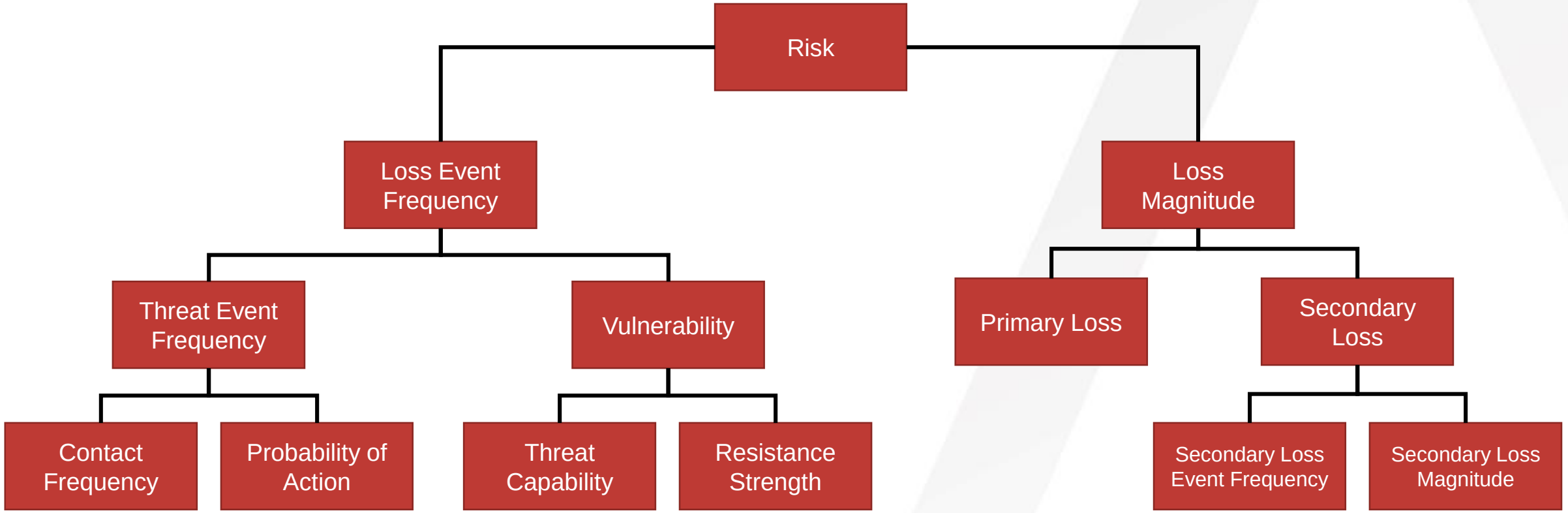
FAIR

- Well-defined framework to identify all factors of a risk
- Measurement of various risk factors
- Calculation of risk (Monte Carlo Simulation)
- Communication of risk to business managers in a form they understand
- Quantitative values can be translated into Qualitative values – if necessary

WHAT IS RISK (PER FAIR)?

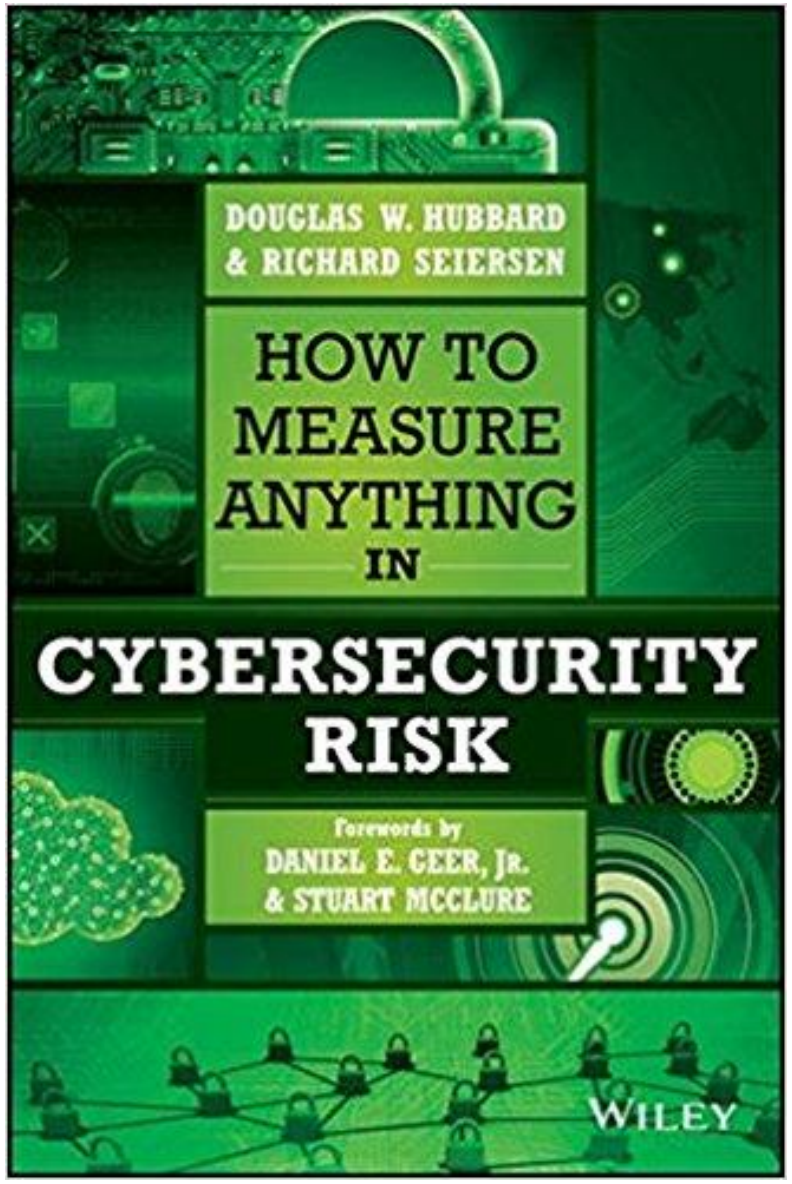
Risk is the measurement of the probable frequency and probable magnitude of future loss

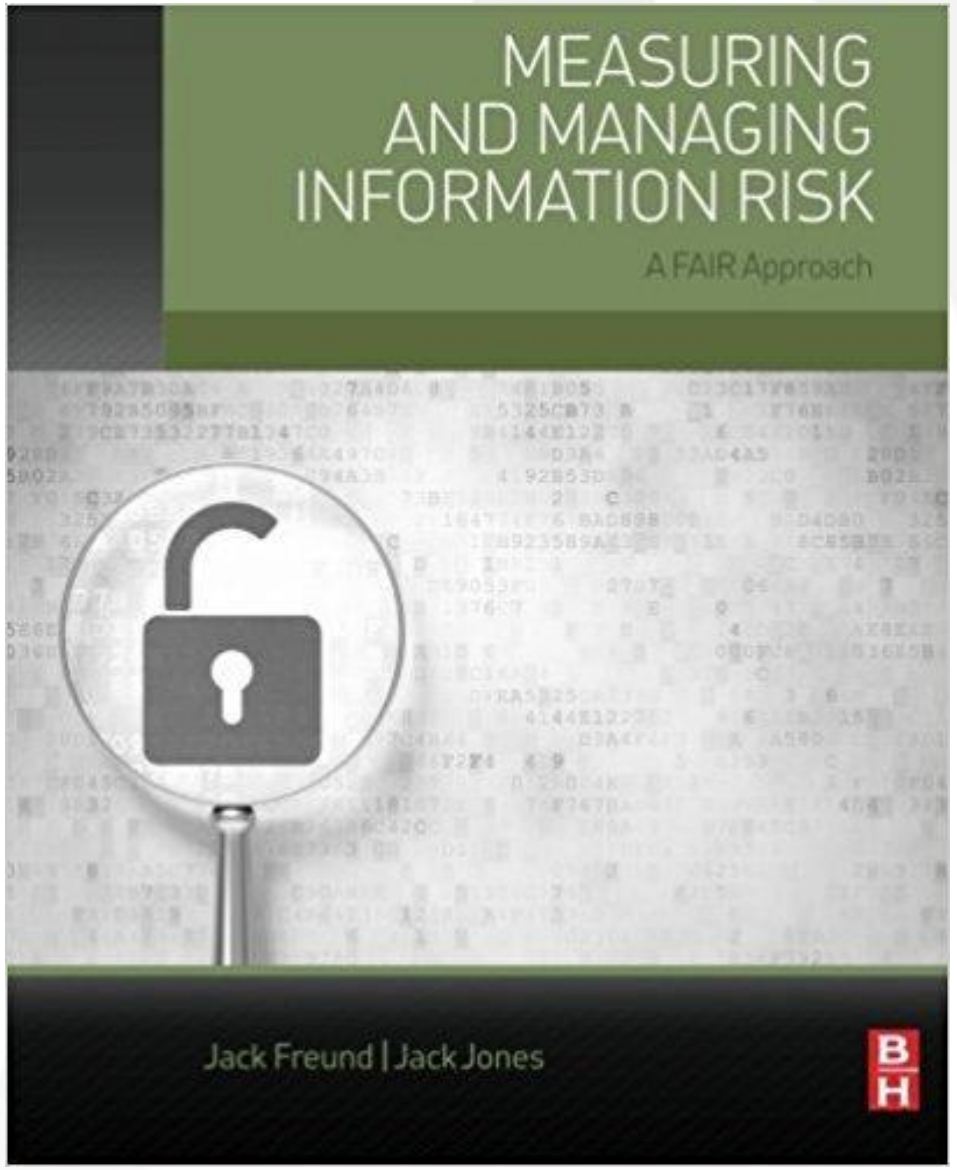
FAIR RISK MODEL



RSA

RECOMMENDED READING





THANK YOU

MICHAEL DELOACH

MICHAEL.DELOACH@RSA.COM

HTTPS://WWW.LINKEDIN.COM/IN/MIKEDELOACH