Using Threat Vulnerability Asset (TVA) Methodology to Determine Cyber Security Risk Strategies

Dr. Roberto J. Mejias, Colorado State University-Pueblo,
Pueblo, Colorado, U.S.A.

Dr. Morgan M. Shepherd, University of Colorado Colorado Springs, Colorado Springs, Colorado, U.S.A.

Dr. Joseph E. Gersch, Colorado State University-Fort Collins,
Fort Collins, Colorado, U.S.A.

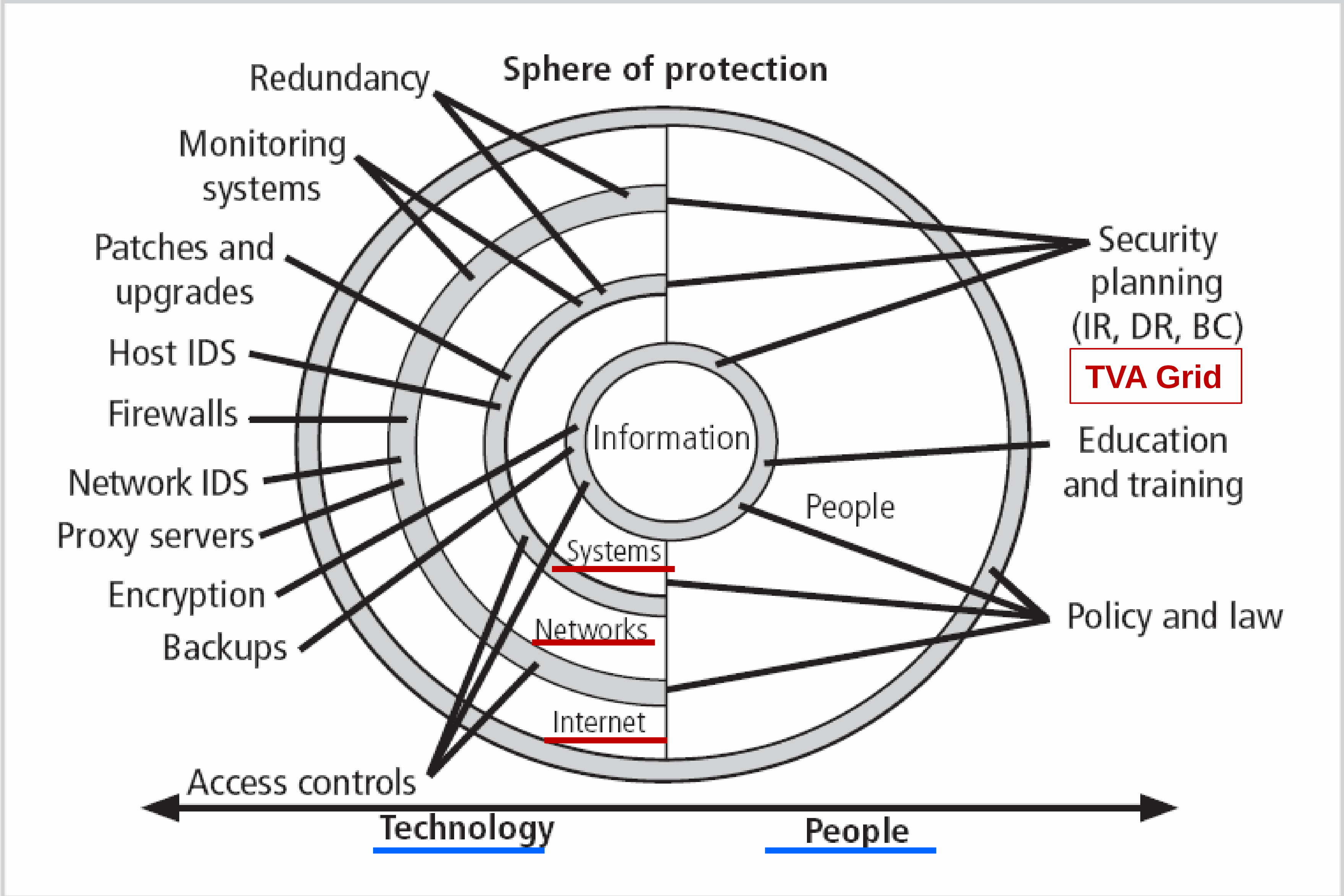
Background

Complex I.S. Architectures = require access by
➔ other External Networks / entities
➔ authentication by users outside of Orgnzl NWs

I.T. Mgmt = have limited time / capability
➔ to assess cyber threats, IS Vulnerabilities
➔ keeping Ops ongoing = 1st priority

TVA Methodology:
➔ effective 1st step to assess I.S. Vulnerabilities
➔ Excellent ID of Logical Vulnerabilities before
….Pen Testing

Sphere of Security



Source: Whitman and Mattord, 2019

2 Basic Types of Vulnerability Analyses

* Vulnerability Assessment

* Penetration Testing

Focus of this Presentation:

Use of TVA (*Threat Vulnerability Asset)* Methodology to

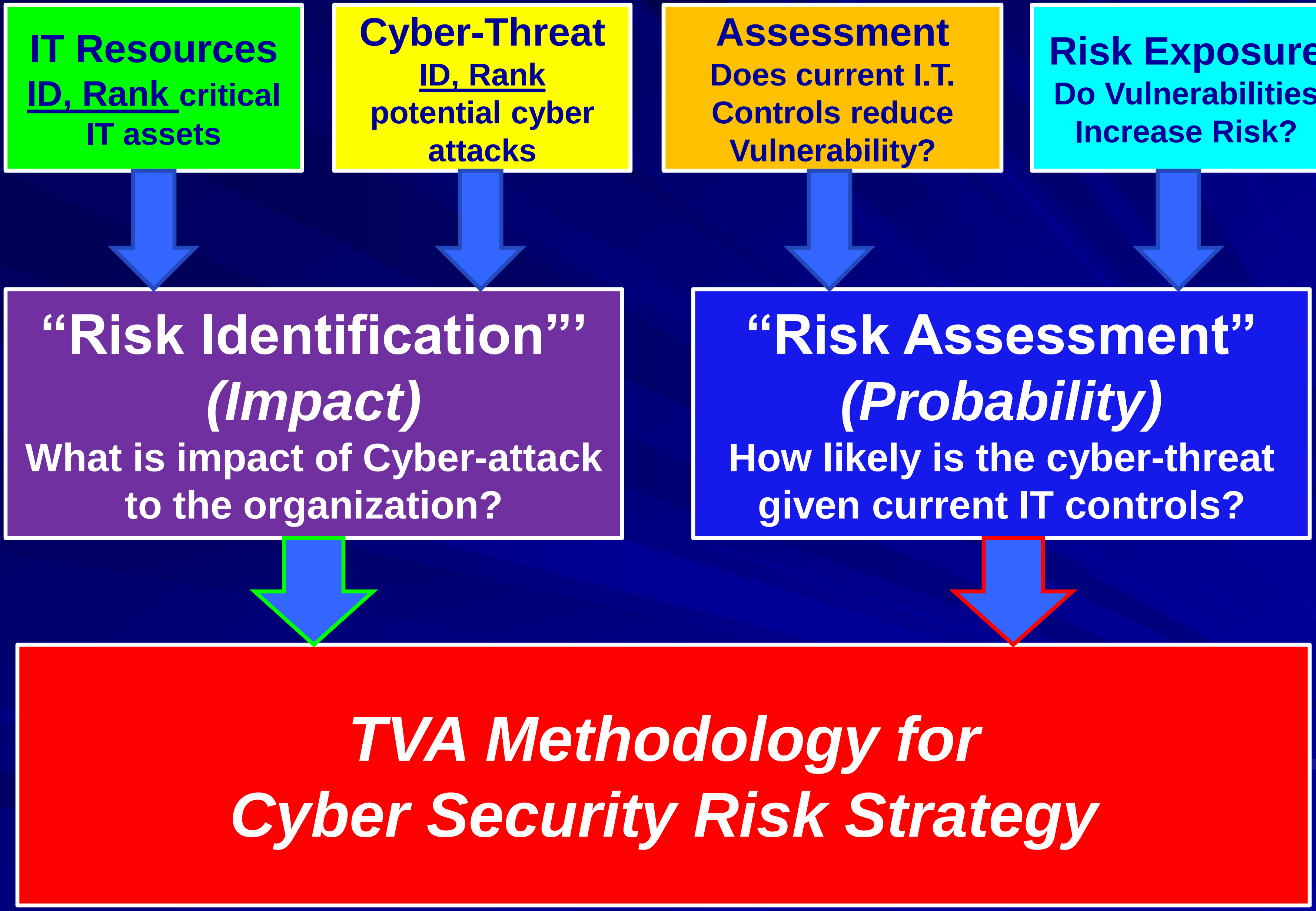
➔ I.D. System Vulnerabilities

➔ Determine Cyber Security Risk Strategies

Vulnerability Analysis

= the analysis of existing I.S. safeguards
to identify any weaknesses in…

- ➔ *detection of a cyber threats / attempted exploits*
- ➔ *inadequate responses to Cyber threats that may “trigger” a system vulnerability*
- ➔ *I.S.’s ability to recover and continue from a Cyber threat / Cyber breach (“robustness”)*
- ➔ *Are current Info Sec investments cost effective …*
  = at detecting / preventing cyber attacks?



IT Resources
ID, Rank critical
IT assets

Cyber-Threat
ID, Rank
potential cyber
attacks

Assessment
Does current I.T.
Controls reduce
Vulnerability?

Risk Exposure
Do Vulnerabilities
Increase Risk?

“Risk Identification”’
(Impact)
What is impact of Cyber-attack
to the organization?

“Risk Assessment”
(Probability)
How likely is the cyber-threat
given current IT controls?

TVA Methodology for
Cyber Security Risk Strategy

Source: Whitman and Mattord, 2019, modified by Roberto Mejias, 2020

Undertanding Threat Vulnerability ➔ Cyber Security Risk Mgmt

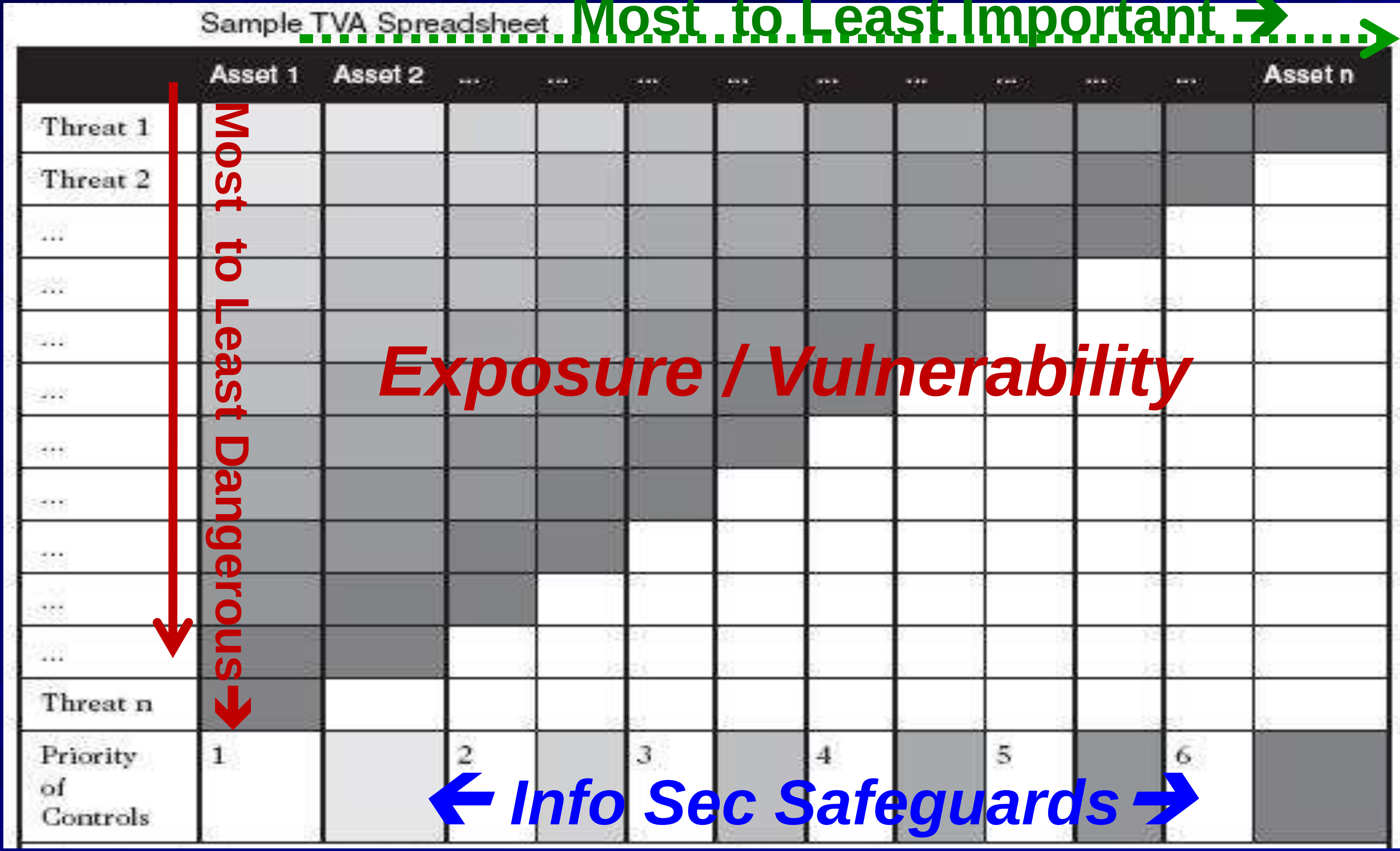
I. (Cyber) Risk Identification

II. (Cyber) Risk Assessment

III. (Cyber) Security Risk Strategies

…via the TVA Methodology

TVA Grid Template



Sample TVA Spreadsheet

	Asset 1	Asset 2	...	...	...	...	...	...	...	...	...	Asset n
Threat 1												
Threat 2												
...												
...												
...												
...												
...												
...												
...												
...												
...												
Threat n												
Priority of Controls	1		2		3		4		5		6	

Most to Least Important →

Most to Least Dangerous →

Exposure / Vulnerability

← Info Sec Safeguards →

Source: Whitman and Mattord, 2019

ID and Ranking of Most Critical Assets

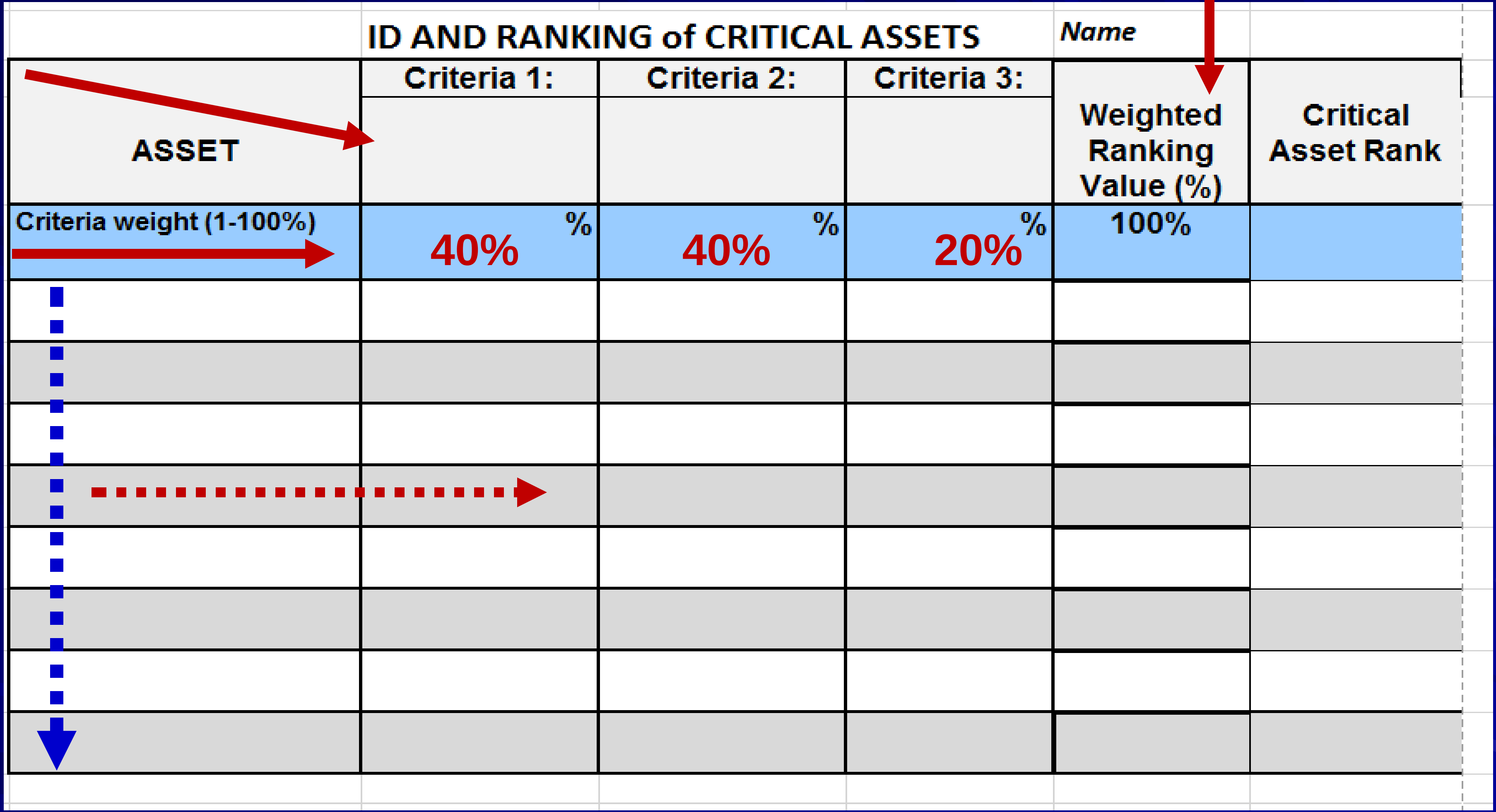
Possible “Value” Categories for Prioritization

- Economic Value
- Operational Value
- Strategic Value

Additional Ranking Criteria :

- Are most critical to success of Orgzn?
- Generate the Most Revenue?
- Has the highest profitability?
- Would be the most expensive to replace?
- Would be the most expensive to protect?

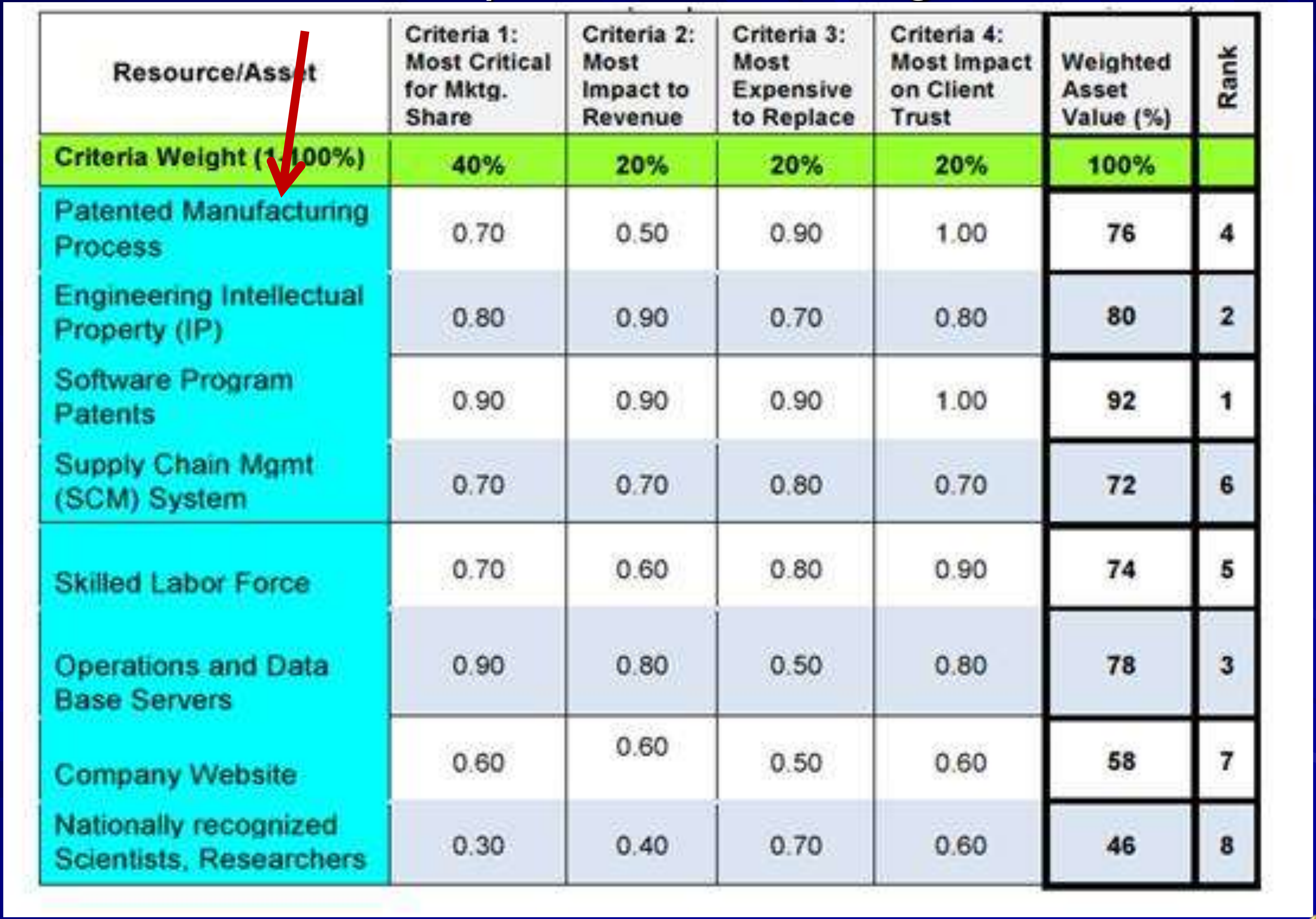
Matrix for Ranking Critical Assets



	ID AND RANKING of CRITICAL ASSETS			*Name*	
ASSET	Criteria 1:	Criteria 2:	Criteria 3:	Weighted Ranking Value (%)	Critical Asset Rank
Criteria weight (1-100%)	% 40%	% 40%	% 20%	100%	

Adapted from : Whitman and Mattord, 2019

Real Example: Asset Ranking Matrix



Resource/Asset	Criteria 1: Most Critical for Mktg. Share	Criteria 2: Most Impact to Revenue	Criteria 3: Most Expensive to Replace	Criteria 4: Most Impact on Client Trust	Weighted Asset Value (%)	Rank
Criteria Weight (1-100%)	40%	20%	20%	20%	100%	
Patented Manufacturing Process	0.70	0.50	0.90	1.00	76	4
Engineering Intellectual Property (IP)	0.80	0.90	0.70	0.80	80	2
Software Program Patents	0.90	0.90	0.90	1.00	92	1
Supply Chain Mgmt (SCM) System	0.70	0.70	0.80	0.70	72	6
Skilled Labor Force	0.70	0.60	0.80	0.90	74	5
Operations and Data Base Servers	0.90	0.80	0.50	0.80	78	3
Company Website	0.60	0.60	0.50	0.60	58	7
Nationally recognized Scientists, Researchers	0.30	0.40	0.70	0.60	46	8

Mejias, Shepherd, Fronmueller, Huff, 2109

	Resources & Assets *(Most Critical ===> Least Critical)*					
Ranked Threat Agents	**1. SW Program Patents**	**2. Engin’g Intellectual Property (IP)**	**3.Operation and DB Servers**	**4. Patented Mfg. Process**	**5. Skilled Labor Force**	**6. Supply Chain Mgmt. (SCM)**
		TVA	**GRID**			
Current IT Safeguards ***(Unranked)***						

Mejias,2019

ID and Ranking of Most Probable Threats

Threat ID and Ranking

All Organizations = face a wide variety of threats

It is operationally, financially infeasible to try to guard all *critical assets* against all *cyber threats*

If every threat were assumed to be successful….

→ *Info Security program*

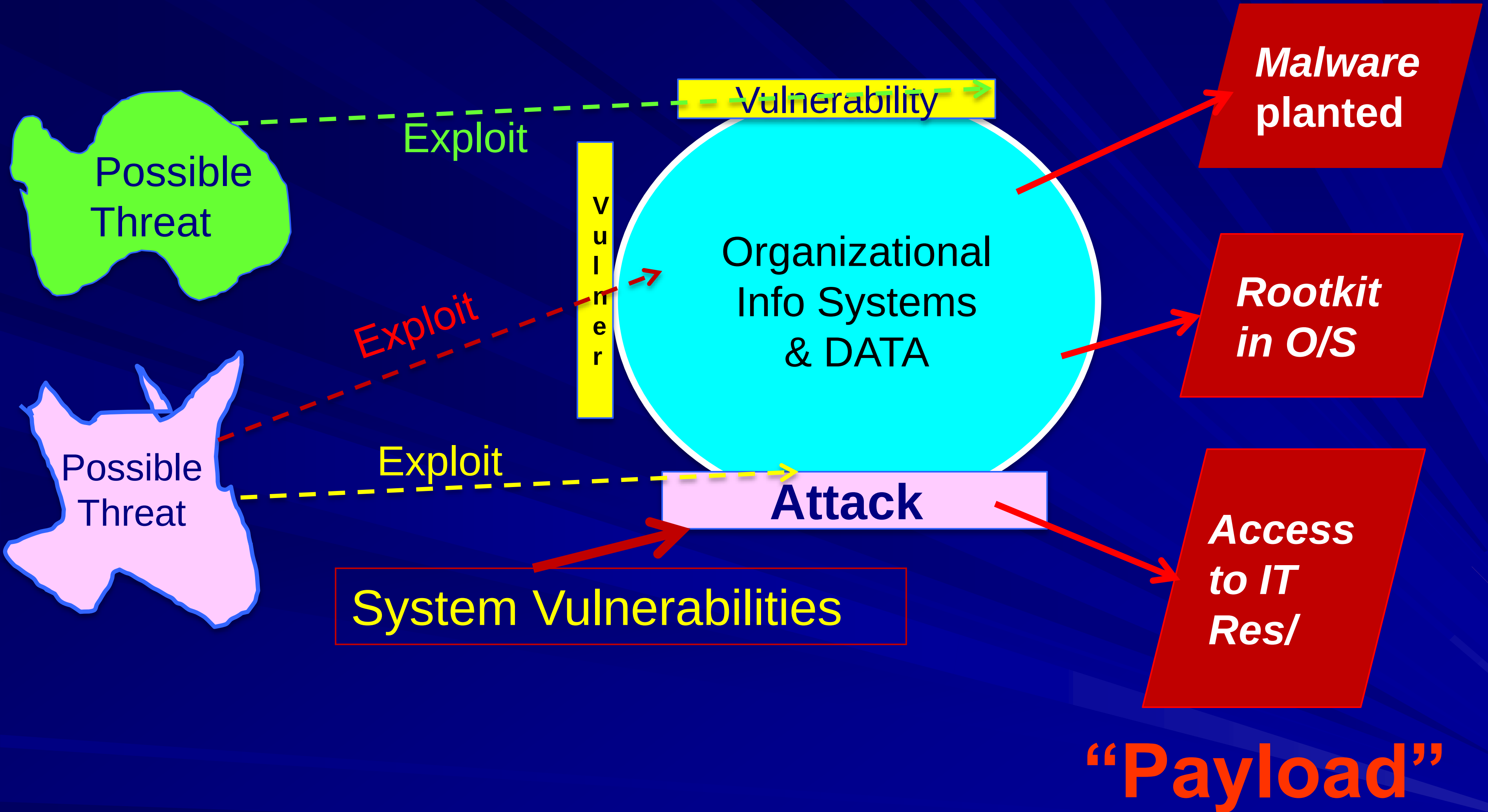
…. becomes too complex

ID, Ranking of THREATS

→ considers only most damaging cyber-attacks

→ that affect Survivability, Continued Ops

Cyber Threats, Exploits, Vulnerabilities and Cyber-Attacks



R.J. Mejias© 2018

Threat Prioritization Matrix-3 factors

Threat Agent	Estimated Impact of Threat Agent	Likelihood of Attack	Est. Loss if Exploit is Successful	Threat Rating Factor	Threat Ranking
1.Theft of Intellectual Property (IP)	94	30%	95%	26.8	**1**
2. Sabotage to Mfg. or SCM Process	74	40%	90%	26.6	**2**
3. Loss of SCM System, Loss of SCM Vendors	80	75%	40%	24.0	**3**
4.Password Cracking of I.S.	59	60%	53%	18.8	**4**
5. Social Engineering of Employees	70	60%	40%	16.8	**5**
6. Website Outage DoS Attack	74	20%	53%	7.8	**6**
7. Software Design Vulnerability Error	57	20%	65%	7.4	**7**
8. Loss of Key Vendors, Contractors	66	15%	45%	4.5	**8**
9. Eavesdropping on Corp. Network, IS	66	15%	45%	4.5	**9**
10.Physical Damage to the PCs, Hard Drives	89	10%	40%	3.6	**10**
11. Open Ports on Routers and Firewalls	53	10%	44%	2.3	**11**
12. Human Error in Software or Mfg.	30	10%	15%	0.5	**12**
13. SQL Injection to databases	45	1%	67%	0.3	**13**

*   94 x .30 x .95 = 26.8

	Resources & Assets *(Most Critical ===> Least Critical)*					
Ranked Threat Agents						
1.Theft of Intellectual Property (IP)						
2. Sabotage to Mfg. or SCM Process						
3. Loss of SCM System, SCM Vendors		**TVA**	**GRID**			
4. Password Cracking of IS						
5. Social Engineering of Employees						
6. DoS Attack / Website Outage						

Mejias,2019

ID of Current I.T. Safeguards and Controls

	Resources & Assets ***(Most Critical ===> Least Critical)***					
Ranked Threat Agents						
		TVA	**GRID**			
Current IT Safeguards ***(Unranked)***	**S1 Firewalls**	**S2 Intrusion Protection**	**S3 Anti-Virus SW**	**S4 Double Authenticate**	**S5 Encryption**	**S6 SETA, Policies, Procedures**

Mejias,2019

➔ Populated TVA Grid to Analyze

	Resources & Assets *(Most Critical ===> Least Critical)*					
Ranked Threat Agents	**1. SW Program Patents**	**2. Engin'g Intellectual Property (IP)**	**3.Operation and DB Servers**	**4. Patented Mfg. Process**	**5. Skilled Labor Force**	**6. Supply Chain Mgmt. (SCM)**
1.Theft of Intellectual Property (IP)						
2. Sabotage to Mfg. or SCM Process						
3. Loss of SCM System, SCM Vendors		**TVA**	**GRID**			
4. Password Cracking of IS						
5. Social Engineering of Employees						
6. DoS Attack / Website Outage						
Current IT Safeguards *(Unranked)*	**S1 Firewalls**	**S2 Intrusion Protection**	**S3 Anti-Virus SW**	**S4 Double Authenticate**	**S5 Encryption**	**S6 SETA, Policies, Procedures**

Mejias,2019

Actual TVA Grid with Revealed Vulnerabilities

	Resources & Assets *(Most Critical =====> Least Critical)*					
Ranked Threat Agents	1.SW Program Patents	2.Engineer'g Intellectual Property (IP)	3. Operation and DB Servers	4. Patented Mfg. Process	5. Skilled Labor Force	6. Supply Chain Mgmt. (SCM)
1.Theft of Intellectual Property	S1, S5, S6	S1, S4,	S1, S4, S5, S6,	S1, S4, S5, S6	S6	S1, S2, S3, S4, S5, S6
2. Sabotage to Mfg. or SCM Process	✗	✗	✗	S1,S2,S3, S4,S5,S6	N/A	S1, S2, S3, S4, S5, S6
3. Loss of SCM System, SCM vendors	N/A	N/A	✗	S4	N/A	S1, S2, S3, S4, S5, S6
4. Password Cracking of IS	✗	S1, S4	S1, S2, S3, S4, S5	S1, S2, S4, S5	S6	S1, S2, S3, S4, S5, S6
5. Social Engineering of Employees	✗	S6	✗	✗	✗	S1, S2, S3, S4, S5, S6
6. Website Outage / DoS Attack	N/A	N/A	S1, S2, S3, S4, S5	S4, S5,	N/A	S1, S2, S3, S4, S5, S6
Current IT Safeguards *(Unranked)*	S1 Firewall	S2 IDS / IPS	S3 Anti-Virus SW	S4 Double Authenticate	S5 Encryption	S6 SETA Policies, Procedures

Mejias, Shepherd, Fronmueller, Huff, 2109

TVA Methodology:
Do we have the correct Cyber Security strategy for Allocating Cyber Security Safeguards and I.T. Spending?

”the $100 test”

4 Basic Cyber Security Risk Strategies

If Cyber Incident, Breach <u>Anticipated</u>…

<u>Proactive Strategies:</u>

(Risk) Avoidance

(Risk) Transference

If Cyber Incident, Breach <u>Occurred</u>:

<u>Reactive Strategies :</u>

(Risk) Mitigation

(Risk) Acceptance

4 Basic Risk Control Strategies

Proactive Strategies

1. Avoidance

= proactive application of safeguards

→ Actively eliminate all / most risks, vulnerabilities

→ Cost is usually not an issue

2. Transference

= proactive shift of Cyber Sec risk → *to outside Entities*

→Outsourcing their cyber security defenses

→ compensates for own lack of Cyber Sec expertise

4 Basic Risk Control Strategies

Reactive Strategies :

3. Mitigation

= Strategy after System has been attacked

➔ Organization safeguards have been breached!

➔ Must now consider “damage control”

4. Acceptance

= Decision is NOT to protect the info system data

= Acknowledged lack of Info Security control(s)

= Accept related loss when cyber attack occurs

4 Basic Risk Control Strategies

Caveat for “Acceptance” Strategy

➔assumes Cost Analysis has taken place!

➔ level of risk and potential loss of info asset is determined / accepted

➔probability of successful attack is low

Questions?

For further info contact Dr. Roberto Mejias at roberto.mejias@csupueblo.edu

Appendix

References:

Ciampa, Mark, Security+ Guide to Network Security Fundamentals (2018), 6th **Edition**, Course Technology,, Cengage Learning, ISBN-13: 978-1-337-28878-1 and ISBN-10: 1-337-28878-0.

Mejias, R.J. and Balthazard, P. “A Model of Information Security Awareness for Assessing Information Security Risk”, *Journal of Information Privacy and Security,* ***(JIPS).*** Winter, 2014; Vol. 10, pp. 1-26.

Mejias, R.J., Shepherd, M.A. Fronmueller, M., Huff, R. A. “Using Threat Vulnerability Asset (TVA) Methodology to Identify Cyber Threats and System Vulnerabilities: A Student Field Project Case Study”, *Business Education Innovation Journal* ***(BEIJ)***, Vol. 11, No. 1, June 2019.

Shepherd, M.A. and Mejias, R.J. “Non-Technical Deterrence Effects of Mild and Severe Internet Use Policy in Reducing Employee Abuse Frequency”, *International Journal of Human Computer Interaction* ***(IJHCI),*** Vol. 32, Issue 7, pp. 557-567**,** 2016**.**

Whitman, Michael E., Mattford, Herbert J. (2018). Management of Information Security, **6th Edition.** Course Technology, Cengage Learning. ISBN-13: 978-1337405713 and ISBN-10: 133740571X