Applying Physical Discipline to Cybersecurity Challenges

David Shinberg, MS, MBA, CISSP, GSTRT, GREM, GCFA, GMON, GPEN, GCIH, GSEC

Senior Manager ISO, Capital One

If builders built buildings the way programmers write programs, the first woodpecker that came along would destroy civilization.

Solution Motivation

We work in an industry that is driven by threat actors

Cybersecurity can benefit from engineering and processes discipline

But we have ……

- Threat Modeling
- Attack Graphs

Still not enough formality, especially about **failures**

Cybersecurity Is Not Alone when it comes to Failures

- Tacoma Narrows Bridge
- Challenger

SUBSAFE – A Real Safety Program

- The purpose of the SUBSAFE Program is to provide maximum reasonable assurance of watertight integrity and recovery capability of a Submarine.
- A culture of Safety is central to the entire Navy submarine community.

Admiral Rickover Insights

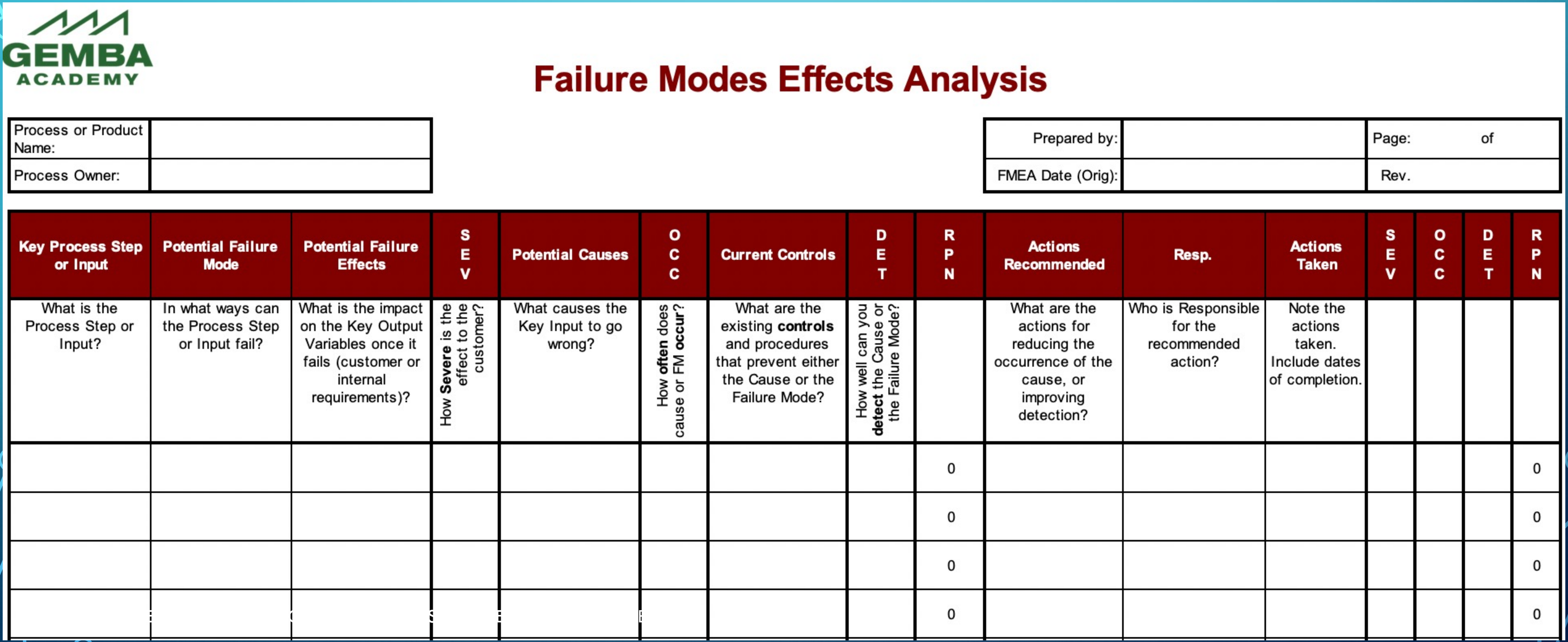
- I made one man responsible for his entire area of equipment—for design, production, maintenance, and contracting. If anything went wrong, **I knew exactly at whom to point.**
- The man in charge must concern himself with details. If he does not consider them important, neither will his subordinates. Yet **"the devil is in the details."**

What Is Failure Mode And Effects Analysis (FMEA)?

- Disciplined method to design reliable and robust systems and processes
- Originated with the US Military in 1940
- Step-by-Step approach for identifying all possible failures
  - Not eliminating all failures
- **Failure modes** - ways, or modes, in which something might fail
- **Effects analysis** - studying the consequences of those failures

Note: Sourced from https://asq.org/quality-resources/fmea

Applying FMEA – Sample Spreadsheet



GEMBA ACADEMY

Failure Modes Effects Analysis

Process or Product Name:	
Process Owner:	

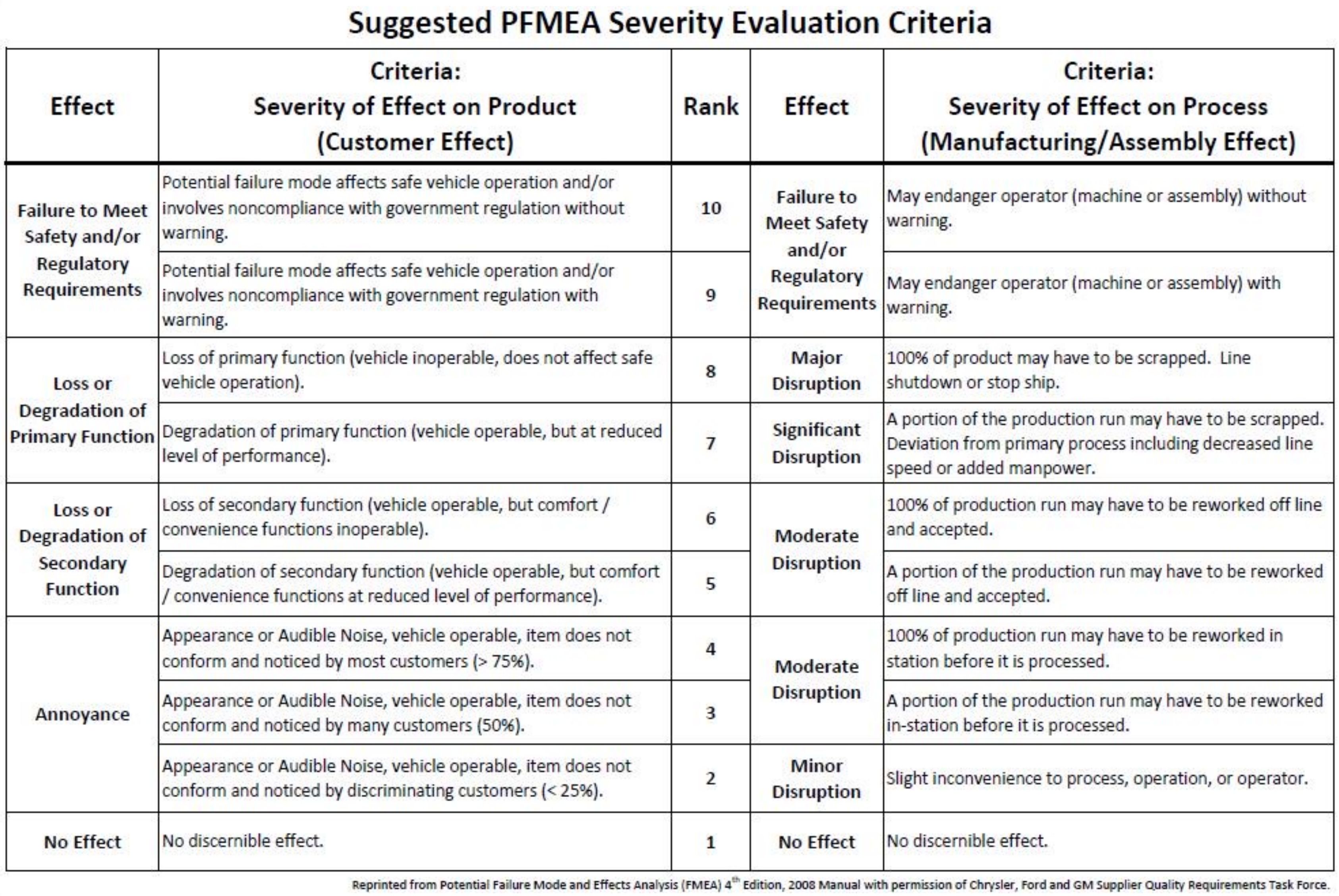
Prepared by:		Page: of
FMEA Date (Orig):		Rev.

Key Process Step or Input	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes	OCC	Current Controls	DET	RPN	Actions Recommended	Resp.	Actions Taken	SEV	OCC	DET	RPN
What is the Process Step or Input?	In what ways can the Process Step or Input fail?	What is the impact on the Key Output Variables once it fails (customer or internal requirements)?	How **Severe** is the effect to the customer?	What causes the Key Input to go wrong?	How **often** does cause or FM **occur?**	What are the existing **controls** and procedures that prevent either the Cause or the Failure Mode?	How well can you **detect** the Cause or the Failure Mode?		What are the actions for reducing the occurrence of the cause, or improving detection?	Who is Responsible for the recommended action?	Note the actions taken. Include dates of completion.				
								0							0
								0							0
								0							0
								0							0

Note: Sourced from: https://blog.gembaacademy.com/2007/06/28/10-steps-to-creating-a-fmea/

FMEA Scoring

- Choose a scoring that works for your team.
- Severity
  - 10 Highest
  - 1 Lowest
- Occurrence
  - 10 Highest
  - 1 Lowest
- Detection
  - 10 Worst
  - 1 Best

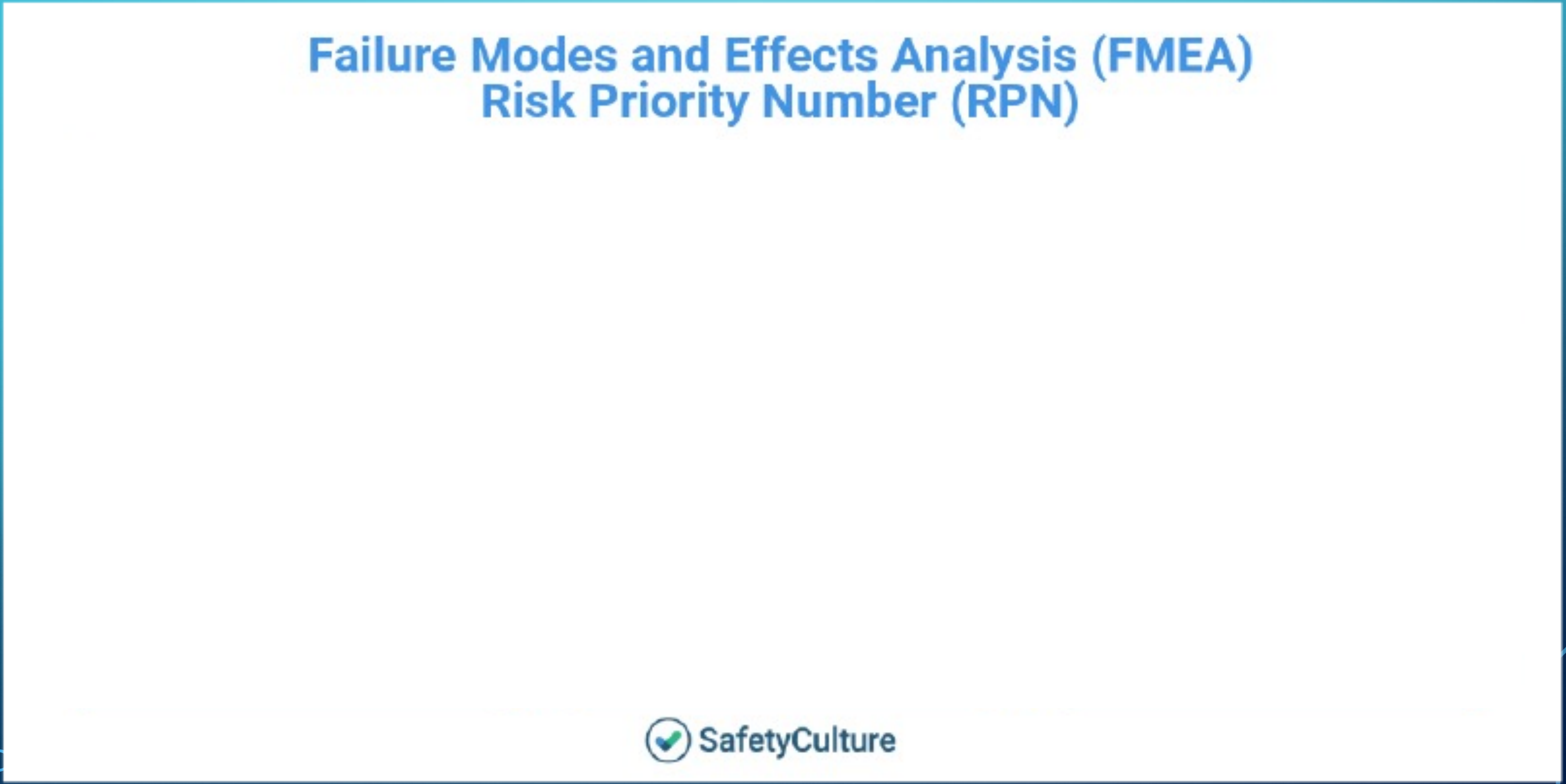


Suggested PFMEA Severity Evaluation Criteria

Effect	Criteria: Severity of Effect on Product (Customer Effect)	Rank	Effect	Criteria: Severity of Effect on Process (Manufacturing/Assembly Effect)
Failure to Meet Safety and/or Regulatory Requirements	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	10	Failure to Meet Safety and/or Regulatory Requirements	May endanger operator (machine or assembly) without warning.
	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	9		May endanger operator (machine or assembly) with warning.
Loss or Degradation of Primary Function	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation).	8	Major Disruption	100% of product may have to be scrapped. Line shutdown or stop ship.
	Degradation of primary function (vehicle operable, but at reduced level of performance).	7	Significant Disruption	A portion of the production run may have to be scrapped. Deviation from primary process including decreased line speed or added manpower.
Loss or Degradation of Secondary Function	Loss of secondary function (vehicle operable, but comfort / convenience functions inoperable).	6	Moderate Disruption	100% of production run may have to be reworked off line and accepted.
	Degradation of secondary function (vehicle operable, but comfort / convenience functions at reduced level of performance).	5		A portion of the production run may have to be reworked off line and accepted.
Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by most customers (> 75%).	4	Moderate Disruption	100% of production run may have to be reworked in station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by many customers (50%).	3		A portion of the production run may have to be reworked in-station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by discriminating customers (< 25%).	2	Minor Disruption	Slight inconvenience to process, operation, or operator.
No Effect	No discernible effect.	1	No Effect	No discernible effect.

Reprinted from Potential Failure Mode and Effects Analysis (FMEA) 4th Edition, 2008 Manual with permission of Chrysler, Ford and GM Supplier Quality Requirements Task Force.

Risk Priority Number (RPN)



Failure Modes and Effects Analysis (FMEA)
Risk Priority Number (RPN)

SafetyCulture

Note: Sourced from https://safetyculture.com/checklists/fmea-template/

Applying FMEA to a Phishing Attack

Identification of Failure Modes

Key Process Step		
Potential Failure		
Potential Failure Effect		
Severity		
Potential Causes		
Occurrence		
Current Controls		
Detection		
Risk Priority Number (RPN)		

DATA FOR ILLUSTRATIVE PURPOSES ONLY

Based on *CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks* (Product ID: AA23-059A)

Applying FMEA to a Phishing Attack

Recommend Actions

Key Process Step		
Potential Failure		
Recommended Actions		
Responsible Party		
Actions Taken		
Revised Severity		
Revised Occurrence		
Revised Detection		
Revised Risk Priority Number		

DATA FOR ILLUSTRATIVE PURPOSES ONLY

Based on *CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks* (Product ID: AA23-059A)

Applying FMEA to Ineffective Separation of Privilege

Identification of Failure Modes

Key Process Step	Lateral Movement
Potential Failure	Excessive permissions granted to standard user accounts
Potential Failure Effect	Facilitation of lateral movement and domain compromise by attackers
Severity	9
Potential Causes	Misconfiguration and inadequate access control policies
Occurrence	4
Current Controls	Weak configuration and poor IAM
Detection	6
Risk Priority Number (RPN)	216

DATA FOR ILLUSTRATIVE PURPOSES ONLY

Based on *CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks* (Product ID: AA23-059A)

Applying FMEA to Ineffective Separation of Privilege

Recommended Actions

Key Process Step	Lateral Movement
Key Process Step	Permissions granted to standard user accounts
Potential Failure	Excessive permissions granted to standard user accounts
Recommended Actions	1. Enforce the principle of least privilege 2. Conduct regular audits of user permissions 3. Implement robust monitoring for unusual access patterns
Responsible Party	1,2. IAM, 3. CSOC
Actions Taken	1,2. Create standard limiting privileges and requiring audits 3. Implement additional detection agents and alerts
Revised Severity	9
Revised Occurrence	3
Revised Detection	4
Revised Risk Priority Number	108

DATA FOR ILLUSTRATIVE PURPOSES ONLY

Based on *CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks* (Product ID: AA23-059A)

FMEA Summary

- Failure Mode and Effects Analysis (FMEA) is a disciplined method to design reliable and robust systems and processes that can be applied to Cybersecurity
- Benefits of FMEA
  - Formal Approach
  - Documented Mitigations
  - Scoring mechanism
- Potential Issues with FMEA
  - Adoption
  - Detection score

Back To The Beginning

- Early stages of computers
  - Computer failures were not a big issue
  - If the program compiles it must work
  - The Internet didn’t exist
- Current life
  - Everything is connected
  - Failures matter and have consequences

Conclusion

- We need to do better and can learn from the the Physical World
- FMEA when done properly can identify almost all failure modes
  - Bringing discipline to Cybersecurity
- Not all failure modes need to be addressed, but knowing failure modes allows:
  - Better prioritization of remediations
  - Adjusting to changing environment be rescoring failure modes (i.e., Threat Modelling)
  - Understanding relationship between failure modes (i.e., Attack Graphs)
- FMEA includes detection probability aiding in understanding impact of failures

A FAVORITE QUOTE

”*Why are there so many failures* - **its because despite the best advice of people who know what they are talking about, other people insist on doing the most massively stupid things"** – Galen