Justifying Investment Risk Mitigation to the Business

Todd Wagner, Energy & Transportation CISO

Caterpillar. Inc.

CISSP | CIPM | CDPSE

May 2022

Presentation Disclaimer

Thoughts, content, and views expressed in this presentation are that of the presenter, personally, and not of the company at which he works.

Setting the Expectations / Ground Rules

- *This is "A Way", Not the "Only Way"!*
- *This will not be Rocket Science… We are going to go "Back to the Basics"*
- *This presentation will be high-level and will not get into specific "Risk Models" or specific calculations / formulas.*
- *Material based on what has worked for me!*
- *My Goal is to just give you high-level concepts to think about.*
- *Please Participate – Offer Additional Suggestions. There will be a prize!*

Agenda

- Foundation & Level Set
- Modified Risk Management Process - The Business
- High-level 5 Step Identification & Prioritization Process
- Simplified Presentation Format for the Business
- Risk Calculation Considerations
- Summarization of Critical Success Factors

Reminder: Back to the Basics

Risk – Basic Foundational Definitions

Often Unknown or Confused

Cybersecurity

Cybersecurity is understanding, managing, and mitigating the risk of critical data being disclosed, altered, or denied access to.

Risk

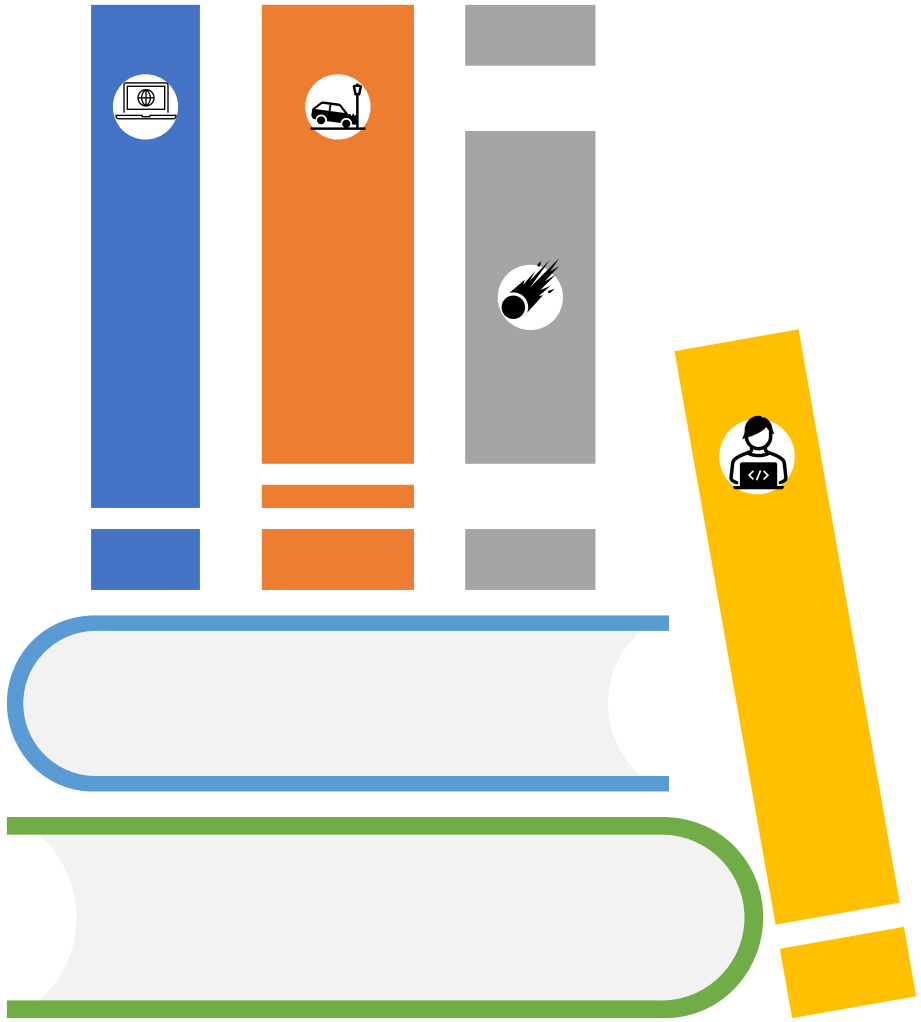
Risk is the probability of something bad happening in the future. “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Risk is uncertain.”*

Threat

Threat is any circumstance or event with the potential for harm.

Vulnerability

Vulnerability is the weakness that allows a threat to manifest itself.



* NIST SP 800-37

Foundational Understanding

Risk Management

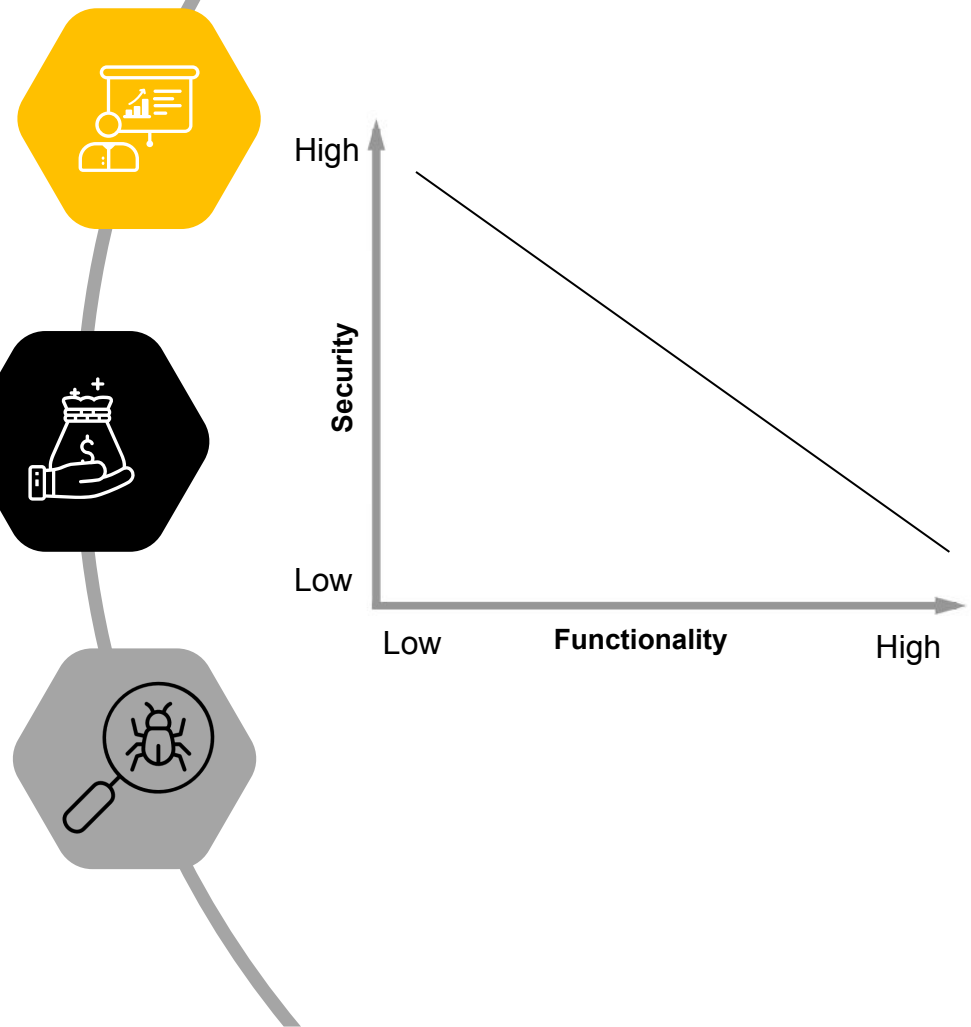
Cybersecurity Risk Management is the on-going process of identifying, analyzing, and addressing the cyber threats to the confidentiality, integrity, and availability of critical assets, processes, and data within your organization.

Business Enabler

Cybersecurity is a business enabler. Help “the business” by reducing the risk associated with “functionality”. If cybersecurity is negatively impacting the business, cybersecurity is wrong.

Risk Based Decisions

If you want business functionality, you can’t have 100% security. Business is all about risk. Business Leaders are taking Risks every day.



A Risk Management Process with “The Business”

Identify

Identification must be focused on risks to critical assets, processes, and data and must be done through business relationships, aligning to Business priorities.

Assess

Assessing the identified risks to determine potential solutions can be done by the Cybersecurity team; however, prioritization must be done with the business, aligning with available resources in Cybersecurity, IT, and the Business.

Monitor & Report

Monitor & Report to other stakeholders, including the Board of Directors on status of projects as well as overall Risk Program - include your Business partners.

Treat

Treat through an organized project management process with a well-defined roadmap and project updates to Cybersecurity Team, IT, and the Business.

High-Level Risk Identification and Prioritization

5 STEP PROCESS

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Identify Business Priorities	Identify Cyber Risks to Business Priorities	Determine the Likelihood of the Risk Manifesting	Determine the Cost of Addressing each Risk (Cost to Fix)	Determine the Cost to Organization if it Occurs

Foundational – Develop Relationship with “The Business” and be able to translate technical to business & business to technical

Building that Foundation with The Business

Personal Relationships – Relationship Development

Some Basic Keys to Good Relationships

- Open Communication – Communication, Communication, Communication…
- Schedule Time to Develop the Relationship
- Be Genuine, Honest, Humble, Trustworthy, Positive, Confident, and Fun
- Be a Great Listener
- Pay Attention – Be Present
- Be a Giver – Offer Assistance
- Don’t Ever Play the Blame Game
- Bring Solutions to the Table
- Your Verbal & Non-Verbal Communication Matters
- Share Credit for Accomplishments
- Put Other Person First
- Use Person’s Name

High-Level Risk Identification and Prioritization

STEP 1: Understanding of Business Priorities & Critical Assets, Processes, & Data

Enterprise Business Priorities

AND/OR

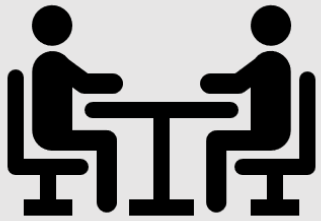
Business Unit Business Priorities

Determine the 5 – 7 Critical Processes, Data, and Systems that support / feed these Priorities

Why… is it important for Cybersecurity Team to understand the Business Priorities?

- "Enable The Business" by addressing the most important Risk…TO THE BUSINESS
- By Understanding:

How can you determine how your Company / Business makes money and what are the Business Priorities?



High-Level Risk Identification and Prioritization

Business Relationship Development – Recommended Agenda & Questions

AGENDA*

- Introductions
- Business Enabler Discussion
- Financial Discussion
- Strategy of the business Discussion – R&D efforts / focus
- Business Priorities Summary
- Critical Assets, Processes, and Data that supports Priorities
- Begin Discussion of Location of Critical Assets and Data
- Schedule Follow-up / On-going Conversations

*Description of meeting goals with questions should be provided to business partner prior to the meeting.

QUESTIONS

- What makes the business money?
- What is the current business strategy?
- What are your R&D efforts focused on?
- What are your top 5 Business Priorities?
- What Critical Assets, Processes, and Data supports those Priorities?
- Where are those Critical Assets and Data located?
- How can I help support your Priorities?

High-Level Risk Identification and Prioritization

STEP 2: Identify Cyber Risks to the "Business Priorities"

What are the Cyber Risks that <u>could</u> negatively impact our ability to make money (Affect Priorities)?

Again, not going to get into Specific Risk Calculations or Formulas.

What are the Cyber Risks to the Critical Processes, Data, and/or Systems supporting those Business Priorities?

<u>Example</u>:

- Business Priority: Manufacturing of Widget "A" of which multiple manufacturing processes (Process Group 1) use "Critical Data 2" stored on Critical "Server 3"
- Risk: Loss or destruction of Data caused by Cyber Attack (External)

What are the Threats & Vulnerabilities associated with those Cyber Risks from External "Actors"?

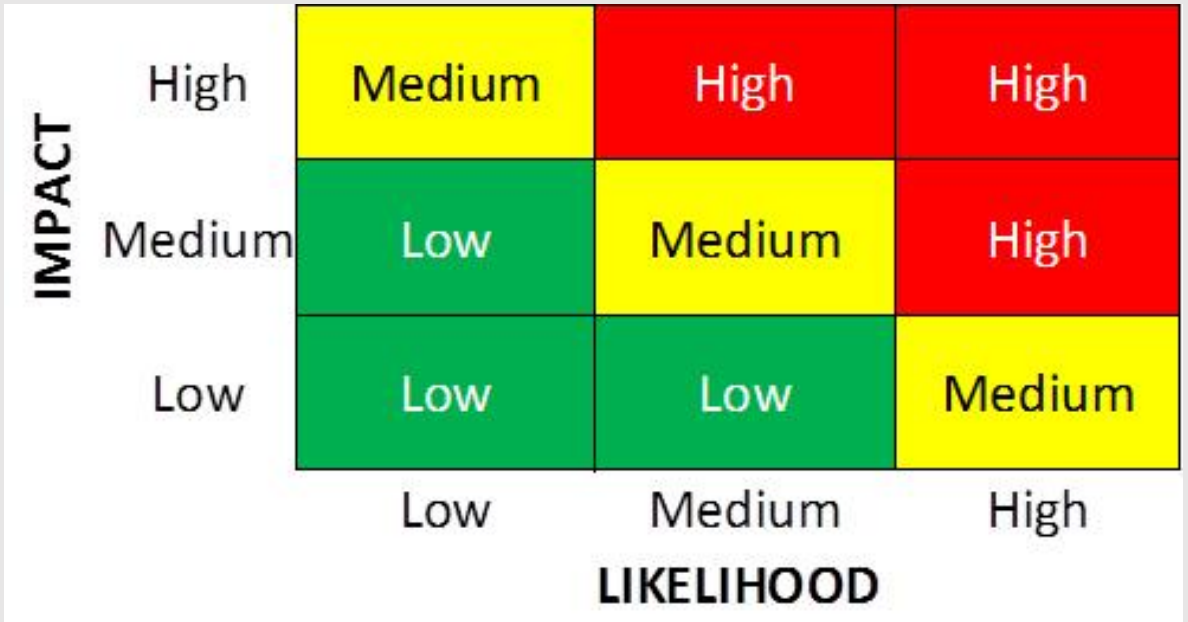
- Threats: Foreign Adversary using Virus / Ransomware or DoS to make data or system unavailable.
- Vulnerabilities: Unpatched System, Application, OS, etc.; Unencrypted Data exposed on Internet; Issues with Back-ups; Fragile Internet Connection; etc.

High-Level Risk Identification and Prioritization

STEP 3: Determine Likelihood of Risk Event and Rough Impact

What is the Likelihood of the Risk Event Occurring?	
What is the Potential Impact?	
High	7
Medium	5
Low	3
	1

Example:



May be different for each Business Unit

High-Level Risk Identification and Prioritization

STEP 4: Calculate the "Cost to Fix"

What is the cost to fix this issue?

- Not likely to eliminate entire Risk
- May be multiple solutions
- Don't look at specific tools / technologies
- Include Total Cost of Ownership (TCO)

Example Solution 1: Off-line back-ups and DDoS Protection
Example Solution 2: Off-line back-ups and Segmentation ("Choke" Points)

Estimated Costs must Include (Yearly Capital & Expense of both IT & Security):

- Hardware Costs
- Software Costs
- Storage Costs
- Costs to Set-up (Configuration: IT & Security FTEs)
- On-going Support Costs (IT & Security FTEs)

High-Level Risk Identification and Prioritization

STEP 5: Calculate the "Cost if it Occurs"

What will it cost the company if Risk materializes?

(Issue Occurs)

- **Be sure to include ALL costs**
- **Don't get hung up on numbers**
  (How many "zeros"? – If needed, create multiple choice based on answers)

Some Example Costs to Include:

- Value of Data
- Cost of Resources to Respond (Internal & External)
- Cost of "Downtime"
- Regulatory Fines
- Cost of Not Meeting SLAs
- Cost of Resources to Recover (Restore Data, Damage to Hardware / Software, etc.)
- Cost of Brand & Reputation Impact
- Cost to Increase Protection to Prevent Re-occurrence

Note: Beneficial to include Business Representatives in discussion!

Presenting to "The Business"

SIMPLIFICATION – DESCRIBE RISK & SOLUTION IN NON-TECHNICAL TERMS

Business Priority & Critical Data	Cyber Risk	Likelihood	Cost to Fix* (May be multiple Options)	Cost if Occurs
CYBERSECURITY PRIORITY 1: Critical Data stored on Critical Server supporting Critical Process to execute on Business Priority A	Risk 1A	HIGH	$1.0M	$2.0M
	Risk 1B	HIGH	$2.5M	$1.5M
	Risk 1C	MEDIUM	$1.0M	$1.0M
	Risk 1D	LOW	$8,000	$10,000

Likelihood of Occurrence should be High or Medium Unless Business Reason

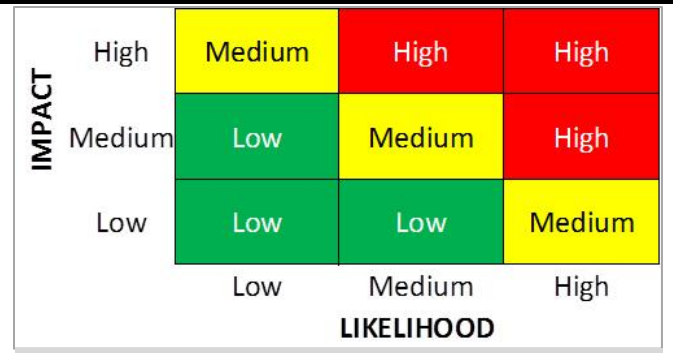
Cost to Fix ≤ Cost if Occurs Unless Business Reason

Basic Risk Calculation Considerations

Four components: Threats, Vulnerabilities, Likelihood, and Impact

Risk = (Threat x Vulnerability)

- Vulnerabilities are the only thing we can control / influence



Where Risk falls on chart may be different for each Business Unit

Because things may happen more or less than once a year

When Calculating “Cost if it Occurs”, build in:

✔ Single Loss Expectancy (SLE): Loss ($) if it happens once
- SLE = Asset Value (AV) x Exposure Factor (EF)
  - AV: Asset Worth
  - EF: How much of that asset will be lost?

✔ Annualized Loss Expectancy (ALE): Expected Loss ($) per year
- ALE = SLE x Annual Rate of Occurrence (ARO)
  - ARO: How often does it occur in a year?

Critical for Success

Relationships with the Business and its Leaders are Critical!

The CISO needs to understand where the critical data / systems are in an organization.

CISO must understand “The Business” and its priorities - focus on enabling the Business through Cybersecurity.

Cost benefit analysis must be conducted. Security spend can’t cost more than accepting the risk.

Prioritize Cybersecurity around critical processes, data, and systems. The CISO must understand what is critical in order to protect it.

Simplify final presentation of Cybersecurity Risk so “The Business can understand”.

Thank You!

Todd Wagner, CISSP | CIPM | CDPSE

wagners1221@gmail.com

(309) 840-2908

A proud member of:

INFRAGARD MEMBERS ALLIANCE SPRINGFIELD