TALKING ABOUT RISK FOR FUN AND PROFIT

SPOILERS - it's ALL about the business!

CyberFace says "Wordz matter!"

CRob, n, adj, and v

Who is *this* jerk?

- **Pronunciation: U.S. (K-robe)**
- Over 25 years of Enterprise-class Architecture, Engineering, Operations, and Security experience
- Ambassador For Intel Product Assurance and Security – *I help manage brand reputation around security*
- Working Group lead for the OpenSSF Dev Best Practices & Vuln Coordination WGs, FIRST PSIRT TPC WG, and others
- Co-Author FIRST PSIRT Services Framework & others
- Pirate-enthusiast & hat-owner

CyberFace says “Don’t worry, it’s almost time for the Exceptional Reception, we can all make it through this!”

AGENDA

01 **WHY MANAGING RISK MATTERS**
WHY

02 **DEFINING RISK**
WAT

03 **RISK MANAGEMENT TECHNIQUES**
HOW

04 **CALL TO ACTION**
WHERE

It may seem strange.
It may make you uncomfortable.
This may seem like a whole new language or way of thinking

It is.

Don’t worry, we’ll all get through this together.

WHY MANAGING RISK MATTERS

01

What’s the worst that could happen?

CyberFace says “We should ONLY focus on things that matter!”

WE ARE OUR CUSTOMER’S SUPPLY CHAIN

As a supplier of goods or services, we affect our customers with delays in opertations and remediation (THEIR compliance). Poor quality in our deliverables impacts THEIR reputation, businesses, and lives. The customers’ projects/initiatives are dependant upon OUR delivery.

Reputation is the most valuable asset an organization possesses. It is **hard** to earn, It is **easy** to lose, it is **nearly impossible** to regain.

CyberFace says “The more effective we are at talking to the business, the more likely we are to achieve our business goals!!”

YO DAWG I HERD YOU LIKE BUSINESS
SO I PUT BUSINESS IN YOUR BUSINESS, SO YOU CAN BUSINESS WHILE YOU BUSINESS
quickmeme.com

ULTIMATELY, IT IS ALL ABOUT THE BUSINESS

Risk Management’s purpose is ensure *effective* & *efficient* strategy & strategic decisions so that the organization can deliver on their desired outcomes. The primary tool for providing this input to the strategy is risk assessments.

Risk-taking is an intrinsic component of business.

CyberFace says “We all contribute to that risk management culture!”

RISK MANAGEMENT GOALS

IDENTIFY

Identify KNOWN risks; explore UNKNOWN risks

DOCUMENT

Collect all relevant data around the potential problem

ASSESS

Following your RMF, analyze and score the severity of the problems - in BUSINESS TERMS

RECOMMEND

Following your org's Risk Strategy, provide the business calm, trusted advice on possible courses of action

MONITOR

Set targets for periodic review and monitor progress as old risks are resolved and as new risks evolve

Defining Risk

02

What luminaries like Merriam Webster have to say on this matter…

CyberFace says “It is important to be talking about the same things!”

WAT is RISK?

A **risk** is a possibility of damage or harm. A risk is described by a **threat** and a **vulnerability**. It is often documented as:

RISK = Threat x Vulnerability

*A **threat** is the potential cause of an incident that may result in harm to a system or organization.*

*A **vulnerability** is a weakness of software, hardware, or online service that can be exploited has security implications.*

It can also be described in terms of Impact and Likelihood

RISK = Likelihood x Impact

FIRST PSIRT Lexicon

Measuring Risk

Qualitative Assessment - relies upon trends, written language, or feelings about the size of a particular issue.

Quantitative Assessment - based off of measurable and observable data

Since you said Quantitative....

Exposure Factor

How much % loss do you expect on your asset?

SLE – Single Loss Expectancy

How much do you think one problem cost?

Asset Value X Exposure Factor = SLE

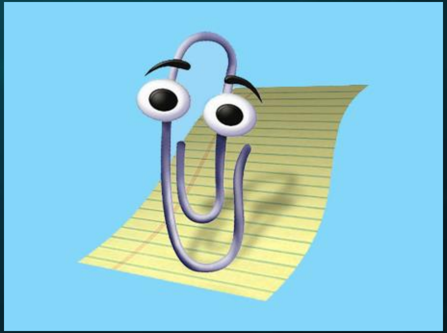
ARO – Annualized Rate of Occurrence

How often does this bad thing keep happening?

ALE – Annual Loss Expectancy

How much are you expecting to lose each year around this problem?

SLE X ARO = ALE



Clippy says "It looks like you're trying to measure some risk. Do you want help with that?"

WHAT TYPES OF RISK could you SEE?

Technical	Business	Project
Something impacts technology (typically software vulnerabilities)	Something impacts your ability to execute on your strategy	Something impacts the delivery or execution of a project

Strategic	Tactical	Operational	Compliance
Something impacts your long-term goals	Something impacts your short-term ability to deliver your goals	Something impacts the infrastructure/operations of the organization	Something impacts your ability to execute your legal/regulatory/compliance obligations

Inherent Risk - level of risk prior to mitigation actions. The uncontrolled level of risk

Residual Risk - (current risk) level of risk **after** applying controls/mitigations.

Boy-howdy, That's A LOT of Risks

CyberFace says "You don't know the HALF of it, brother!!"

BUT CROB.....

My lizard brain

Tells me that risks are scary

Scary things are bad...

So isn't all risk bad?

FALSE!

INTOLERABLE APPETITE

Two more concepts that will be important to us later:

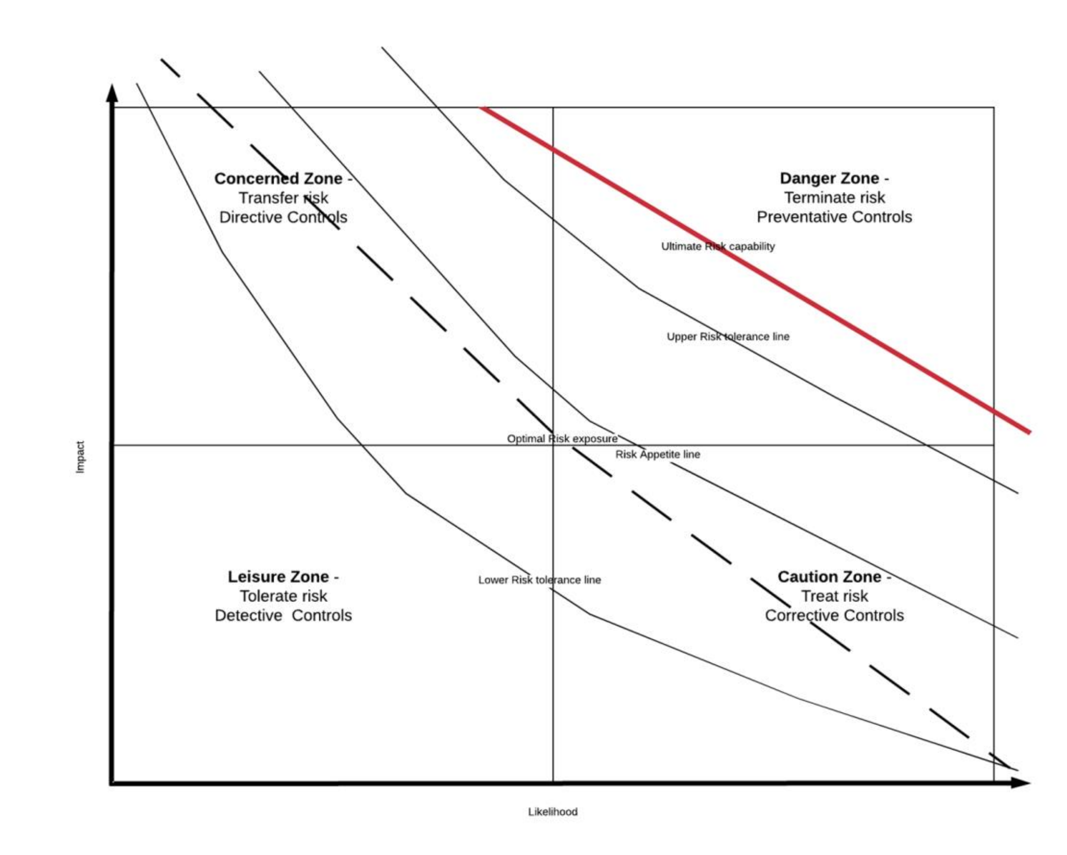
Risk Appetite is the immediate or short-term willingness of an org to undertake an activity that involves risk

Risk appetite is about identifying the optimal level of risk that will achieve the most favourable outcome for the organization

Risk Tolerance represents the range of risk an organization is willing to carry. Sometimes this may be at levels higher than would normally be accepted

CyberFace has a HUNGER for RISK. nom nom nom

GET IN THE ZONE



Organizations will typically carry enough risk to help them innovate, accelerate, and meet their business objectives (being too conservative will stifle growth or the ability to capitalize on arising opportunities)

The Risk tolerances and appetite of an organization will change over time/economic conditions/market opportunities

RISK MANAGEMENT TECHNIQUES

03

What we can DO about Risk

CyberFace says “Knowing is half the battle!”

WHAT CAN YOU DO WITH A RISK?

Terminate or Eliminate

Treat or Mitigate

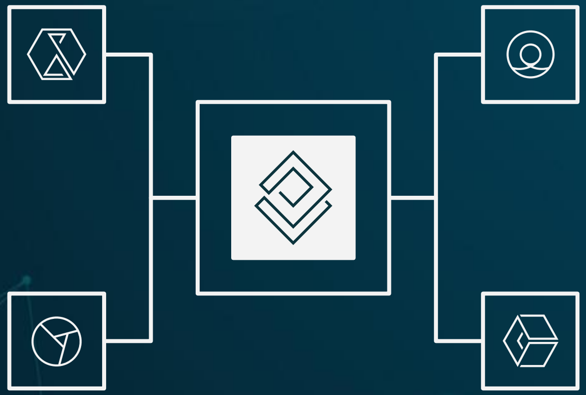
Transfer....meh

Tolerate or Accept

This is “The 4 T’s” of Risk Management

HOW DO YOU MANAGE RISK?

….By applying **CONTROLS** (AKA Mitigations)



Relevant to actions BEFORE an event occurs

PREVENTATIVE

Ex - A Firewall, or SELinux

DETECTIVE

Relevant to circumstances AFTER an event has occurred

Ex - Reviewing Audit logs, an IDS, or network/server scans

Designed to ensure a particular outcome is achieved

DIRECTIVE

Ex - A Policy: “Don’t do that!”

CORRECTIVE

Designed to correct undesirable circumstances or reduce unacceptable risk exposures

Ex - AIDE, or a patch

CyberFace asks “What about COMPENSATING controls?”

Compensating controls are alternatives that can assist in reducing the impact of a risk, oftentimes because a CORRECTIVE control is deemed too expensive.

COOL STORY, BRO

...but HOW do we do that?

Great Value(TM) Risk Analysis

I can't believe it's not Butter!
Original
Great Value
Wow! I totally thought it was "butter"
58% VEGETABLE OIL SPREAD
$3.18

Likelihood X Impact

How often could this happen x How bad could it be?

Let’s put this into concepts we all can relate to in our everyday lives

Werewolves - Cuddly friends?

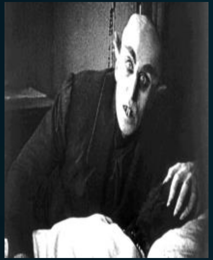
Threat	Likelihood	Impact	Overall Risk
Werewolf	Once every 29.5 days	You are murderfaced	Complete loss of C, I & A

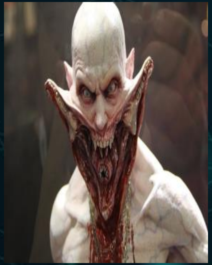
Strengths – speed, agility, heightened senses, and fury. Can break through cement walls, rip people in half, work in groups to bring down their prey, transmit lycanthropy through bites

Weaknesses - Silver is needed to kill a Lycanthrope but most people do not carry a big-assed hunk to defend themselves. Chew toys. The Mailman and/or Amazon guy

Sounds pretty bad if it happens, but it doesn't happen THAT often

Vampires - Gentleman caller from across the sea





Threat	Likelihood	Impact	Overall Risk
Vampire	~12hrs every 24hrs	Varies	Varies
Vampire - feeds	~12hrs every 24hrs	Bad Hickey, tired	C jeopardized, I reduced, A reduced
Vampire - converts	~12hrs every 24hrs	Hope you enjoy eating flies Renfield	C jeopardized, I greatly reduced, A reduced
Vampire - drains	~12hrs every 24hrs	You are murderfaced	Complete loss of C,I & A
Twilight	100% annoying	Ugh. Just STAHP	C complete loss, Complete loss of I, A…probably get some dates

Mileage GREATLY varies. Feeling Lucky?

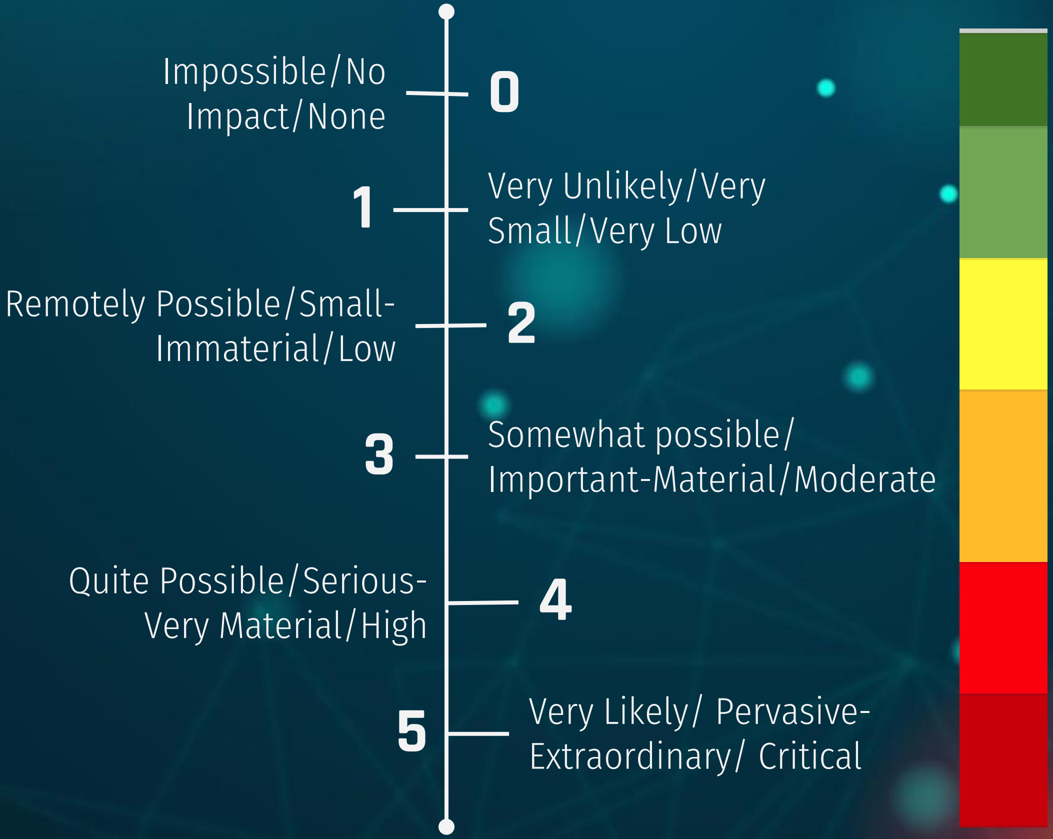
Strengths – Strength, agility, telepathy to control anyone he's bitten across the world, weather manipulation, control of nocturnal animals, transforming into a bat, a wolf, and mist, among others.

Weaknesses - Wooden stake in the heart and his head has to be chopped off at the same time, sunlight, crucifixes, garlic, sacramental bread, not being invited into your home, crossing running water and not having home soil.

Likelihood & Impact summary

Threat	Likelihood	Impact	Overall Risk
Werewolf	Once every 29.5 days	You are murderfaced	Complete loss of C, I & A
Vampire	~12hrs every 24hrs	Varies	Varies
Vampire - feeds	~12hrs every 24hrs	Bad Hickey, tired	C jeopardized, I reduced, A reduced
Vampire - converts	~12hrs every 24hrs	Hope you enjoy eating flies, Renfield	C jeopardized, I greatly reduced, A reduced
Vampire - drains	~12hrs every 24hrs	You are murderfaced	Complete loss of C,I & A
Twilight	100% annoying	Ugh. Just STAHP	C complete loss, Complete loss of I, A…probably get some dates
Cthulhu	~ Once every millennium	Complete end of reality as you know it	Complete loss of C,I, A

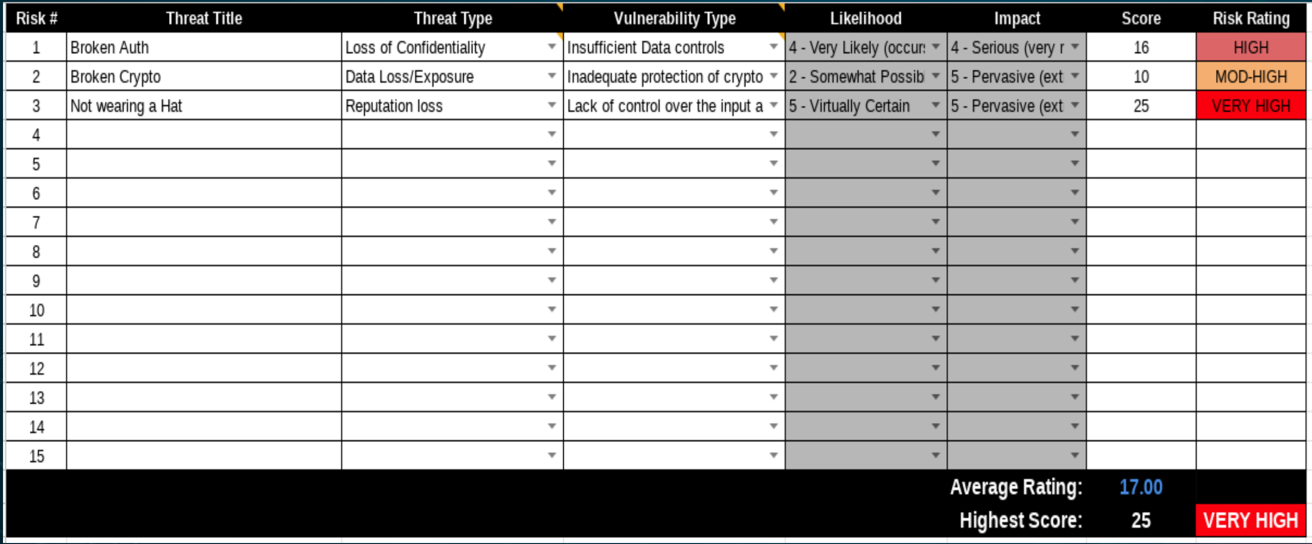
HOW ARE WE QUANTIFYING RISKS?



- 0 Impossible/No Impact/None
- 1 Very Unlikely/Very Small/Very Low
- 2 Remotely Possible/Small-Immaterial/Low
- 3 Somewhat possible/ Important-Material/Moderate
- 4 Quite Possible/Serious-Very Material/High
- 5 Very Likely/ Pervasive-Extraordinary/ Critical

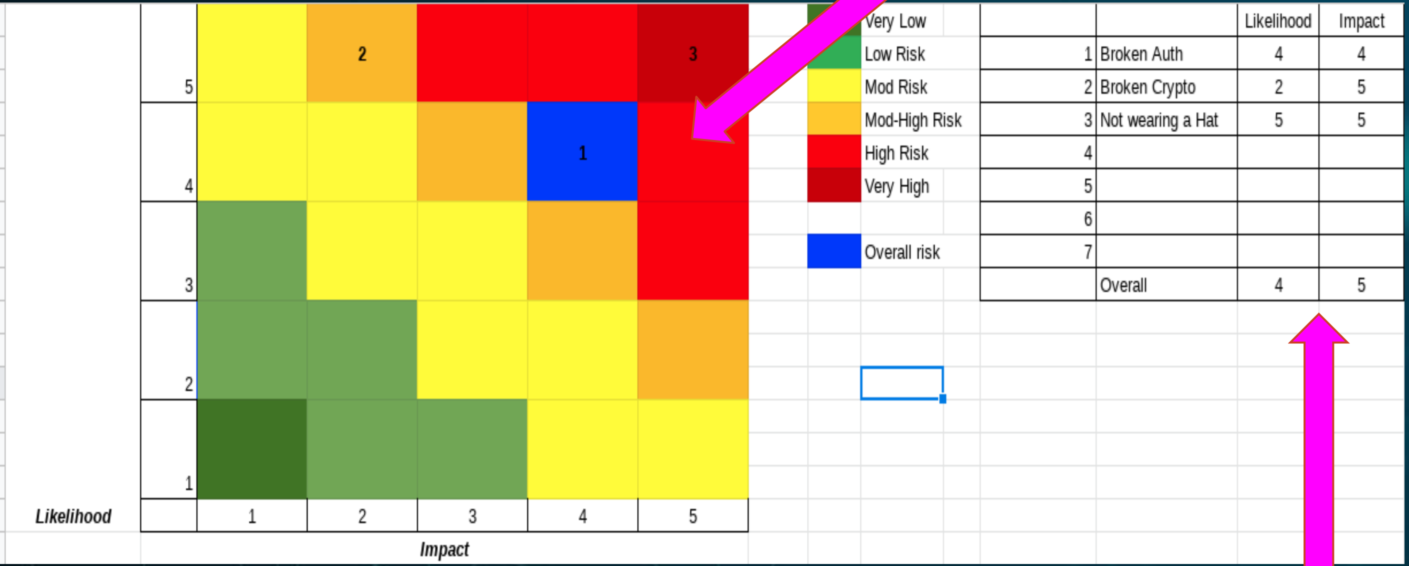
WORK IT OUT

Taking a look at each issue independently first, the Likelihood and Impact are assessed based off of what COULD happen if that risk was realized. The total aggregate risk can be expressed numerically and with standardized words/levels



Risk #	Threat Title	Threat Type	Vulnerability Type	Likelihood	Impact	Score	Risk Rating
1	Broken Auth	Loss of Confidentiality	Insufficient Data controls	4 - Very Likely (occur:	4 - Serious (very r	16	HIGH
2	Broken Crypto	Data Loss/Exposure	Inadequate protection of crypto	2 - Somewhat Possib	5 - Pervasive (ext	10	MOD-HIGH
3	Not wearing a Hat	Reputation loss	Lack of control over the input a	5 - Virtually Certain	5 - Pervasive (ext	25	VERY HIGH
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
					Average Rating:	17.00	
					Highest Score:	25	VERY HIGH

Anyone Catch CRob's screenshot mess-up?



5	🟨	🟧 2	🟥	🟥	🟥 3
4	🟨	🟨	🟧	🟦 1	🟥
3	🟩	🟨	🟨	🟧	🟥
2	🟩	🟩	🟨	🟨	🟧
1	🟩	🟩	🟩	🟨	🟨
Likelihood	1	2	3	4	5

Impact

🟩	Very Low
🟩	Low Risk
🟨	Mod Risk
🟧	Mod-High Risk
🟥	High Risk
🟥	Very High
🟦	Overall risk

		Likelihood	Impact
1	Broken Auth	4	4
2	Broken Crypto	2	5
3	Not wearing a Hat	5	5
4			
5			
6			
7			
	Overall	4	5

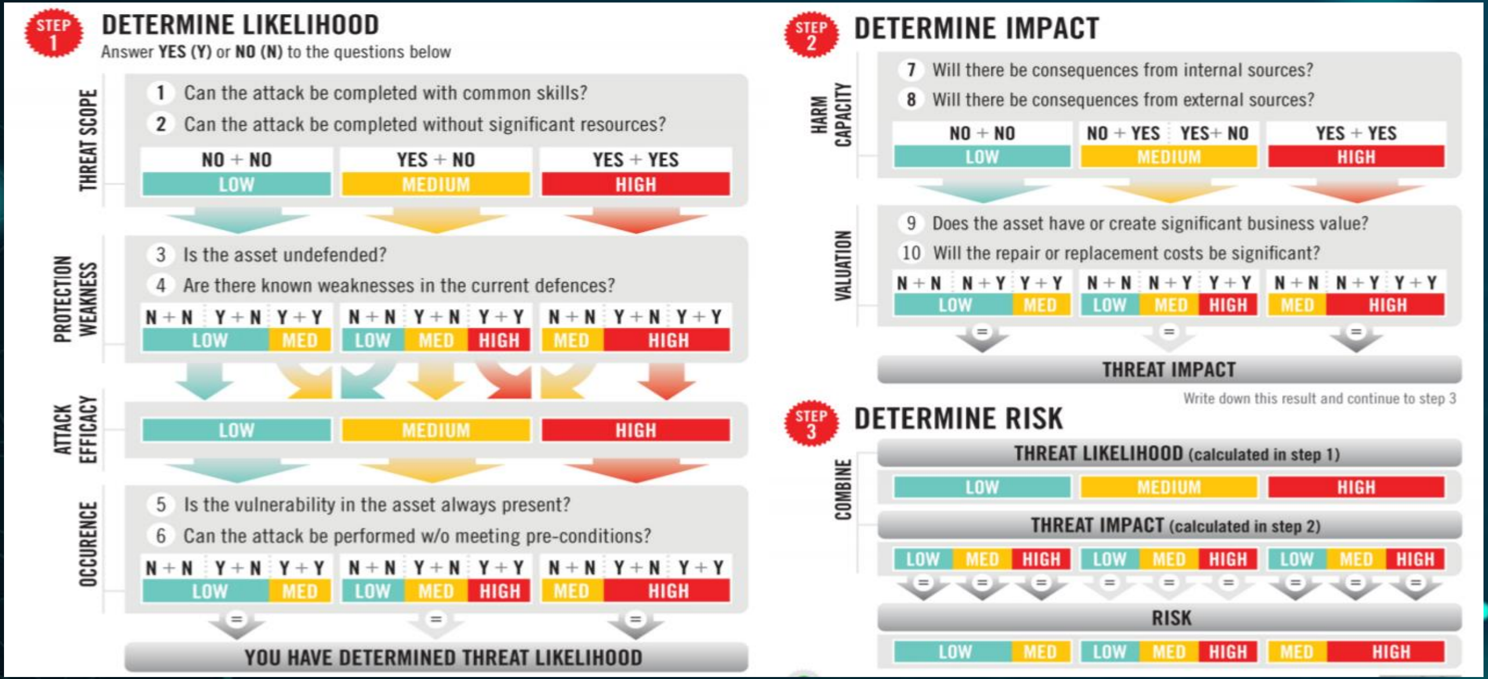
WHAT IS THE MATRIX?

Since we rated our Risk with both Likelihood and Impact, we can plot it on ....THE RISK MATRIX

CyberFace was wondering if anyone was still awake

Binary Risk Analysis

Busy? Risk analysis take “too long” to fit into your schedule? Can you say “Yes” or “No”? Do you have time to answer 10 questions about your problem?



STEP 1

DETERMINE LIKELIHOOD

Answer **YES (Y)** or **NO (N)** to the questions below

THREAT SCOPE

1 Can the attack be completed with common skills?

2 Can the attack be completed without significant resources?

NO + NO	YES + NO	YES + YES
LOW	MEDIUM	HIGH

PROTECTION WEAKNESS

3 Is the asset undefended?

4 Are there known weaknesses in the current defences?

N + N	Y + N	Y + Y	N + N	Y + N	Y + Y	N + N	Y + N	Y + Y
LOW		MED	LOW	MED	HIGH	MED	HIGH	

ATTACK EFFICACY

LOW	MEDIUM	HIGH

OCCURENCE

5 Is the vulnerability in the asset always present?

6 Can the attack be performed w/o meeting pre-conditions?

N + N	Y + N	Y + Y	N + N	Y + N	Y + Y	N + N	Y + N	Y + Y
LOW		MED	LOW	MED	HIGH	MED	HIGH	

= = =

YOU HAVE DETERMINED THREAT LIKELIHOOD

STEP 2

DETERMINE IMPACT

HARM CAPACITY

7 Will there be consequences from internal sources?

8 Will there be consequences from external sources?

NO + NO	NO + YES YES+ NO	YES + YES
LOW	MEDIUM	HIGH

VALUATION

9 Does the asset have or create significant business value?

10 Will the repair or replacement costs be significant?

N + N	N + Y	Y + Y	N + N	N + Y	Y + Y	N + N	N + Y	Y + Y
LOW		MED	LOW	MED	HIGH	MED	HIGH	

= = =

THREAT IMPACT

Write down this result and continue to step 3

STEP 3

DETERMINE RISK

COMBINE

THREAT LIKELIHOOD (calculated in step 1)

LOW	MEDIUM	HIGH

THREAT IMPACT (calculated in step 2)

LOW	MED	HIGH	LOW	MED	HIGH	LOW	MED	HIGH

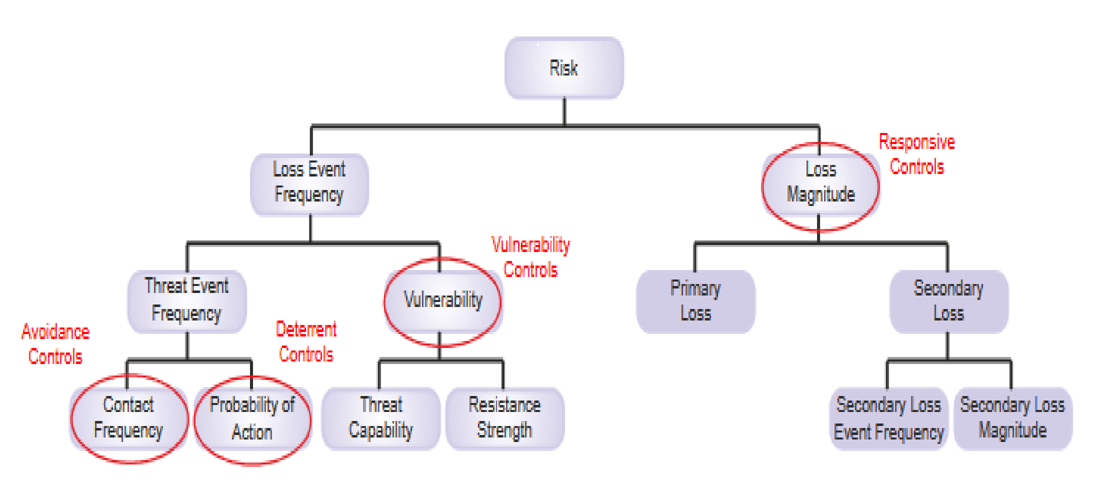
= = = = = = = = =

RISK

LOW		MED	LOW	MED	HIGH	MED	HIGH	

Website
Workcard
Web-based Tool

FAIR/OpenFAIR

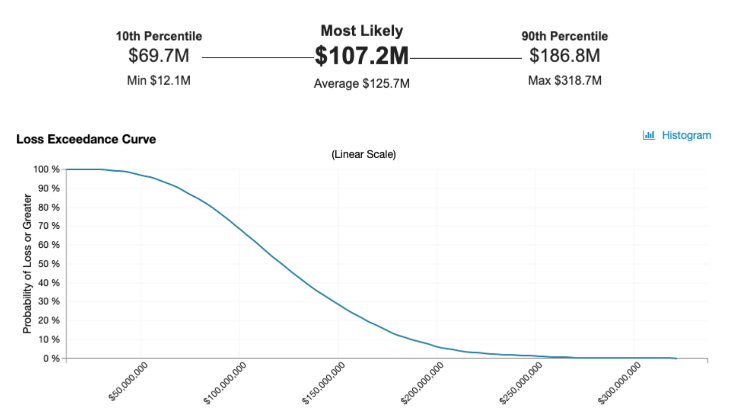


- FAIR is an advanced Qualitative technique.
- Requires more effort & data collection, but once organizational data has been collected future assessments are far-easier
- Provides accurate FINANCIAL-based impacts, ranges, and probabilities

https://www.opengroup.org/certifications/openfair

THE® Open GROUP

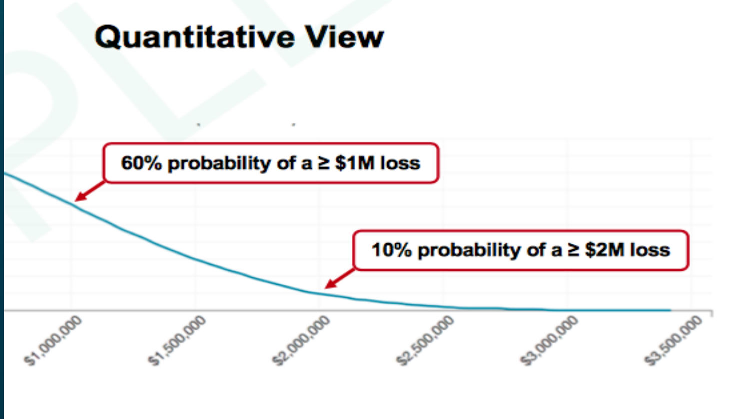
Tools can be Cool!



10th Percentile $69.7M Min $12.1M

Most Likely $107.2M Average $125.7M

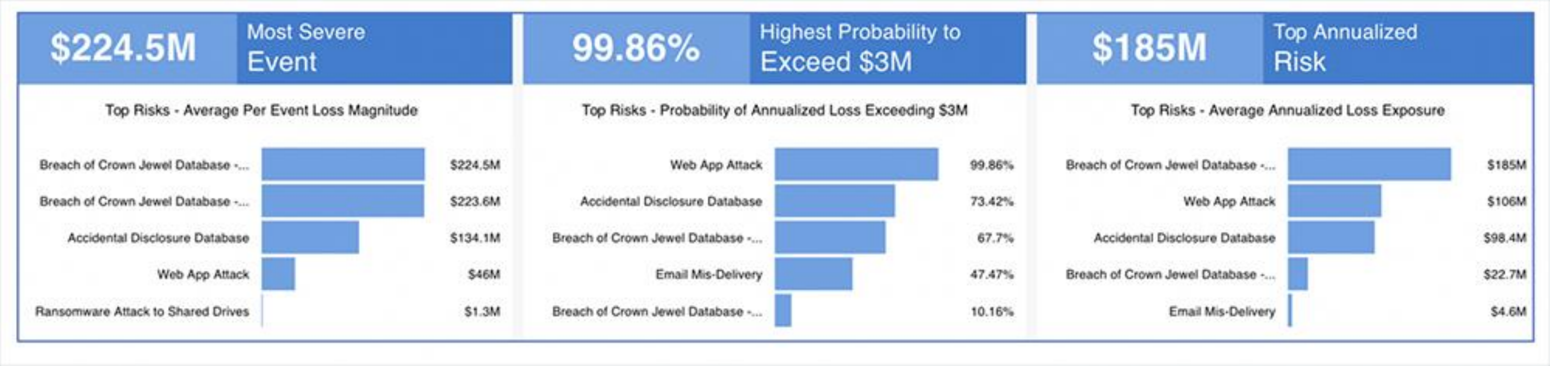
90th Percentile $186.8M Max $318.7M



Quantitative View

60% probability of a ≥ $1M loss

10% probability of a ≥ $2M loss



$224.5M Most Severe Event

Top Risks - Average Per Event Loss Magnitude

Breach of Crown Jewel Database -...	$224.5M
Breach of Crown Jewel Database -...	$223.6M
Accidental Disclosure Database	$134.1M
Web App Attack	$46M
Ransomware Attack to Shared Drives	$1.3M

99.86% Highest Probability to Exceed $3M

Top Risks - Probability of Annualized Loss Exceeding $3M

Web App Attack	99.86%
Accidental Disclosure Database	73.42%
Breach of Crown Jewel Database -...	67.7%
Email Mis-Delivery	47.47%
Breach of Crown Jewel Database -...	10.16%

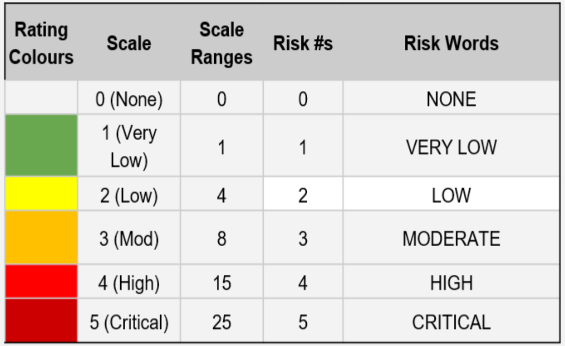
$185M Top Annualized Risk

Top Risks - Average Annualized Loss Exposure

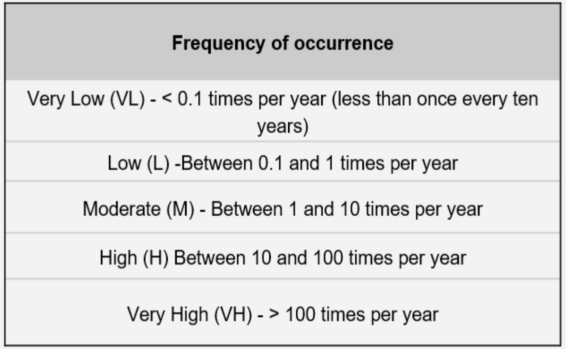
Breach of Crown Jewel Database -...	$185M
Web App Attack	$106M
Accidental Disclosure Database	$98.4M
Breach of Crown Jewel Database -...	$22.7M
Email Mis-Delivery	$4.6M

Cyberface says “I, for one, welcome our new robot...oops I mean tool overlords! Tools can help shape and present your message.”

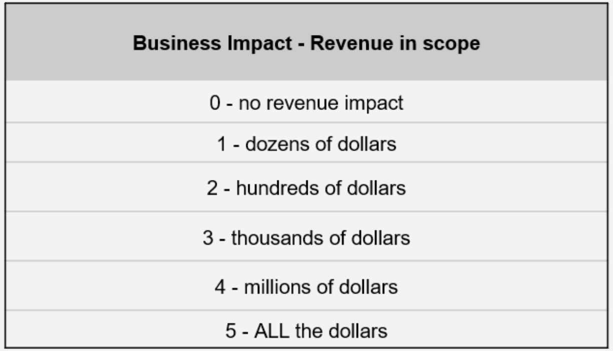
OpenFAIR scales



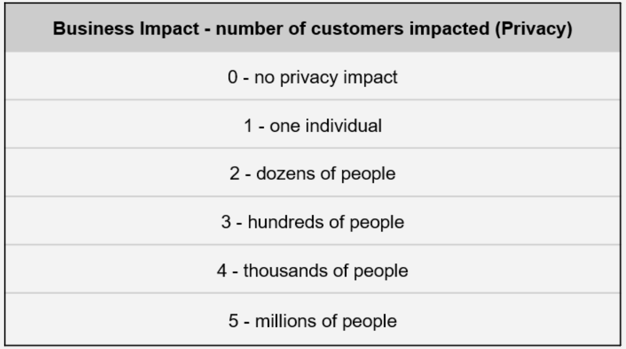
Rating Colours	Scale	Scale Ranges	Risk #s	Risk Words
	0 (None)	0	0	NONE
🟩	1 (Very Low)	1	1	VERY LOW
🟨	2 (Low)	4	2	LOW
🟧	3 (Mod)	8	3	MODERATE
🟥	4 (High)	15	4	HIGH
🟥	5 (Critical)	25	5	CRITICAL



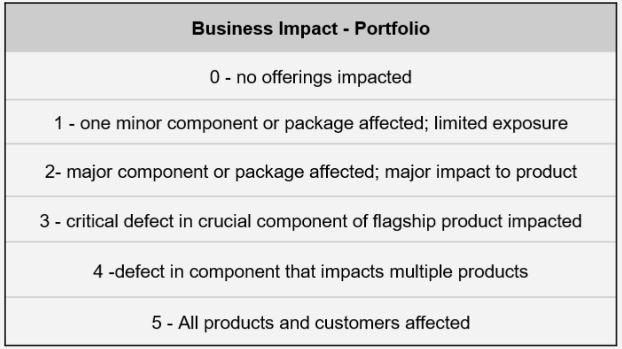
Frequency of occurrence
Very Low (VL) - < 0.1 times per year (less than once every ten years)
Low (L) -Between 0.1 and 1 times per year
Moderate (M) - Between 1 and 10 times per year
High (H) Between 10 and 100 times per year
Very High (VH) - > 100 times per year



Business Impact - Revenue in scope
0 - no revenue impact
1 - dozens of dollars
2 - hundreds of dollars
3 - thousands of dollars
4 - millions of dollars
5 - ALL the dollars



Business Impact - number of customers impacted (Privacy)
0 - no privacy impact
1 - one individual
2 - dozens of people
3 - hundreds of people
4 - thousands of people
5 - millions of people



Business Impact - Portfolio
0 - no offerings impacted
1 - one minor component or package affected; limited exposure
2- major component or package affected; major impact to product
3 - critical defect in crucial component of flagship product impacted
4 -defect in component that impacts multiple products
5 - All products and customers affected

CyberFace says “Pick the right Impact data for the scenario you’re analyzing.”

SHOW ME THE MONEY

Evidence-based reports, like the annual Verizon Data Breach Report can provide invaluable anecdotal data if you don’t have numbers from your own incidents

CyberFace says “This is all great, but how can I tie all this together to present it to my decision-makers?”

OPTIONS & IMPACTS

Option A:

What is the first things that could happen?

Describe the thing briefly

ⓘ Explain what is done with Option A simply – who is doing what?

✓ Pros

Explain the good things that come from this path

✗ Cons

Explain the negative things that could come from this path

Option B:

What is the other thing that could happen?

Describe the other thing briefly

Pros

ⓘ Explain what is done with Option B simply – who is doing what?

✓ Pros

Explain the good things that come from this path

✗ Cons

Explain the negative things that could come from this path

Cyberface says “Using O&I helps you lay out the good and bad things that could/will happen for any choice or risk that lays before you so that business leaders can make their decision on which course to pursue.”

SBAR

Situation	What is the problem?
Background	What has been done/How did we get here?
Assessment	What are the risks caused by the problem?
Recommendation	What should be done to fix the problem?

Cyberface says “SBAR helps to defuse early derailing of your presentation by preempting questions, showing a summary of the problem, your analysis, and a proposed solution right at the beginning.”

FIRM

FIRM is a method to articulate risks. It divides problems into four categories:

Is there an impact to our profitability or expenses?

FINANCIAL

Is there an impact to our core business/ processes / tooling?

INFRASTRUCTURE

Would this impact customer desire / retention?

REPUTATION

Would this affect the level of customer trade / expenditure / our market-share?

MARKET

Cyberface says “You need to frame the conversation with leadership in terms they know and care about!”

CALL TO ACTION 04

Actions Items ALL AROUND!

CyberFace says “I must not fear. Fear is the mindkiller that brings total oblivion…”

CHOOSE YOUR WORDS WISELY

Thinking about the fact that in 2021 and beyond it is likely that your customers will predominantly be BUSINESS/GENERALIST-style users. You need to adjust your language both externally as well as internally

CyberFace says "No business person cares if the muffler bearings on the dynamic flux capacitor are progressively failing in a cascading spiral on non-binary kubernetes software-defined networks." Just say "Availability for our Core Processing System is compromised." The End."

BE FIRM

Using FIRM to focus our language and express things in more business-like language we will be more effective in transmitting our information about the choices that lay ahead for the business.

What are the possible **FINANCIAL** consequences?

This problem could cause us to spend $1million dollars to correct

What are the possible **INFRASTRUCTURE** consequences?

Lack of logs means that the we would not know if build pipeline integrity was compromised which could impact our audit and have $42mil implications for fines

What are the possible **REPUTATIONAL** consequences?

If we are seen as untrustworthy or negligent, this could impact our ability to influence upstream code commits, thus impacting our ability to meet new FINTECH customer PCI Requirements which could negatively impact our stock price.

What are the possible **MARKET** consequences?

If our software can not meet customer security requirements will will not be able to execute on being the "open hybrid cloud thought leader", which could impact $400mil in revenue for Q1

WRAPPING IT ALL UP

FOCUS

On understanding your business and areas/processes that will incur greater risks

EVALUATE

Using standard criteria and language, understand the severity and scope of the risks found

COMMUNICATE

With all involved stakeholders using appropriate language

ESCALATE

Manage risk at your level, escalate larger-scope problems

You ARE your brand

Every customer interaction is an opportunity to either improve or take away from that brand

THANKS!

Do you have any questions?

CRob_at_Intel_dot_com
@SecurityCRob
https://github.com/SecurityCRob
https://www.youtube.com/c/SecurityUnhappyHour

CyberFace says "This isn't the end, this is only the **BEGINNING**! (mwahaha)"

Resources

- Hopkin, Paul. *Fundamentals of Risk Management* (5th ed.). Kogan Page, 2018.
- Freund, Jack and Jack Jones. *Measuring and Managing Information Risk - a FAIR approach*.Elsvier, 2015.
- Hubbard, Douglas W. and Richard Seirsen. *How to Measure Anything in Cybersecurity Risk*. Wiley, 2016.
- Landoll, Douglas J. *The Security Risk Assessment Handbook*. Auerback Publications, 2006.
- Talabis, Mark Ryan M. and Jason L. Martin. *Information Security Risk Assessment Toolkit*. Syngress, 2013.
- Allen, Brian and Rachelle Loyear. *Enterprise Security Risk Management*. Rothstein Associates, 2019.
- DeMarco, Tom and Timothy Lister. *Waltzing with Bears - Managing Risk on Software Projects.* Dorset House Publishing, 2003.
- Binary Risk Assessment – https://binary.protect.io/workcard.pdf
- OpenFAIR - https://www.opengroup.org/certifications/openfair

DICTIONARY

- **Risk** - a possibility of damage or harm.
- **Threat** - a circumstance that could have an adverse affect on an asset.   Threats can come from people, technical, or environmental factors.
- **Asset** - could be many things, including a piece of software, a server, or data.
- **Vulnerability** - is a weakness or absence of a safeguard in an asset that provides a higher potential or frequency of a threat occurring.
- **Likelihood** or Probability - how sure the assessor is that an event occurring
- **Impact** - the measurement of what possible costs would be incurred if that event did happen. The Cost could be financial (and typically is what is focused on), but impacts to personnel, morale, organization effectiveness, or delays in delivery times lines are other examples.