Research Report:

Risk Assessment Tool That Calculates The Type, Cost And Likelihood of Breaches.

Institute of Technology Carlow

Department of Computing & Networking

Student Name: Eimhin Lane
Student Number: C00240680

Student Name: Eimhin Lane
Student Number: C00240680

Abstract:

To evaluate the risks posed to many businesses and users we must analysis the various aspects of evaluating a risk and how to present that to the user. We will need a detailed understanding on the processes and objective of the business or user and a background on what could be at risk in this system. Through the existence of similar technologies, articles, reports and frameworks we can obtain a detailed understanding of risk assessment systems methodologies and how to better them for the user. Ultimately providing an easy-to-follow breakdown on not only the risk type, but also the likelihood of the risk occurring and the cost of a possible breach.

Table of Contents:

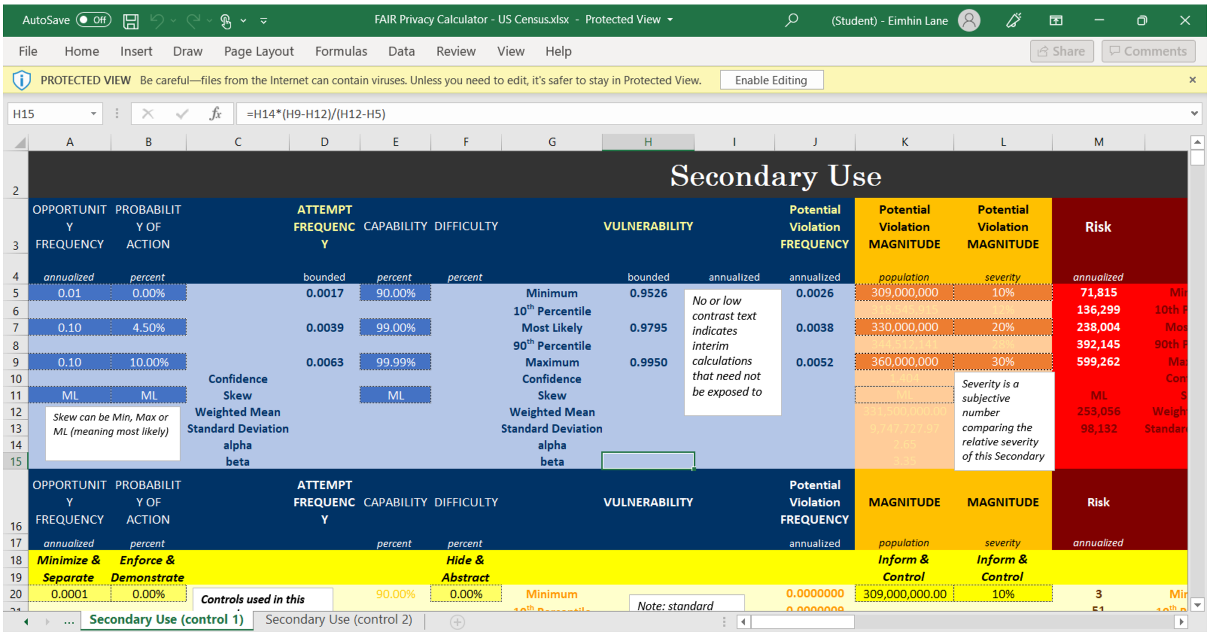
Introduction:

Quantitative Risk Assessment is the process of analysing a threat and quantifying the cost envelope within which they should be implemented [1]. The purpose of these tools is to find vulnerabilities and provide a breakdown on these threats, along with possible solutions to the threat on hand. Risk Assessment Frameworks are used in the quantification of the risk, to determine what is at high risk or low risk. The tool I am creating is to provide this functionality in an intuitive interface for less technically inclined users.

1. Similar Technologies:

1.1 NIST –

NIST’s website has two downloadable tools for risk assessment purposes. The first of which is FAIR privacy, while the second is more internally developed named PRAM [2]. Upon downloading from their github repository it seems to only include risk models and no tool. The two models seem to share many files and seem to simply be based on a US census with no quantitative tool having been installed. This information is still helpful in discerning how assessing a risk is done and how to portray this information such as the breakdown of threat likelihood.



PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

H15 =H14*(H9-H12)/(H12-H5)

	A	B	C	D	E	F	G	H	I	J	K	L	M	
2								Secondary Use						
3	OPPORTUNITY FREQUENCY	PROBABILITY OF ACTION		ATTEMPT FREQUENCY	CAPABILITY	DIFFICULTY		VULNERABILITY		Potential Violation FREQUENCY	Potential Violation MAGNITUDE	Potential Violation MAGNITUDE	Risk	
4	annualized	percent		bounded	percent	percent		bounded	annualized	annualized	population	severity	annualized	
5	0.01	0.00%		0.0017	90.00%		Minimum	0.9526		0.0026	309,000,000	10%	71,815	Mi
6							10th Percentile				318,545,915	12%	136,299	10th P
7	0.10	4.50%		0.0039	99.00%		Most Likely	0.9795		0.0038	330,000,000	20%	238,004	Mos
8							90th Percentile				344,512,141	28%	392,145	90th P
9	0.10	10.00%		0.0063	99.99%		Maximum	0.9950		0.0052	360,000,000	30%	599,262	Ma
10			Confidence				Confidence				1,404			Con
11	ML	ML	Skew		ML		Skew				ML		ML	S
12			Weighted Mean				Weighted Mean				331,500,000.00		253,056	Weigh
13			Standard Deviation				Standard Deviation				9,747,727.97		98,132	Standar
14			alpha				alpha				2.65			
15			beta				beta				3.35			
16	OPPORTUNITY FREQUENCY	PROBABILITY OF ACTION		ATTEMPT FREQUENCY	CAPABILITY	DIFFICULTY		VULNERABILITY		Potential Violation FREQUENCY	MAGNITUDE	MAGNITUDE	Risk	
17	annualized	percent			percent	percent				annualized	population	severity	annualized	
18	Minimize &	Enforce &				Hide &					Inform &	Inform &		
19	Separate	Demonstrate				Abstract					Control	Control		
20	0.0001	0.00%			90.00%	0.00%	Minimum			0.0000000	309,000,000.00	10%	3	Mi

Skew can be Min, Max or ML (meaning most likely)

No or low contrast text indicates interim calculations that need not be exposed to

Severity is a subjective number comparing the relative severity of this Secondary

Controls used in this

Note: standard

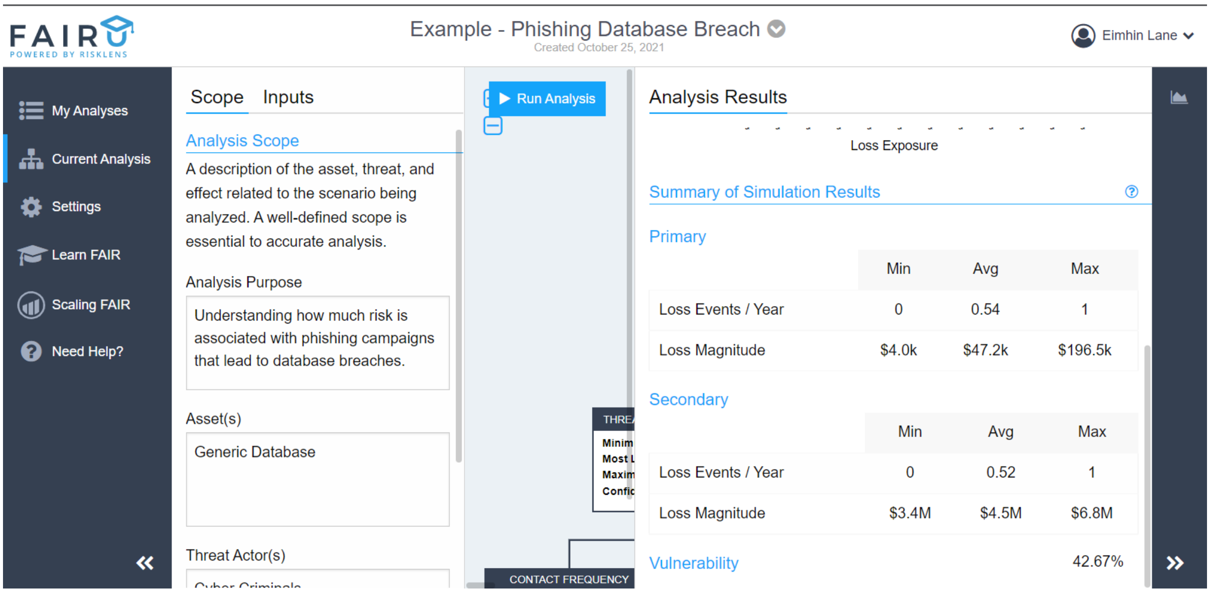
Threat Levels According to NIST		
Threat Level:	**Description:**	**Vulnerability Percentage:**
Min	The least threatening level of vulnerability to a system, not necessarily a priority and while fixes should be they should be done when not costly.	10%
Max	The most threatening level of vulnerability to a system, should be taken as a priority to fix.	90%
ML (Most Likely)	Can be used in place of Max and should be treated with the same level of priority.	90%

1.2 FAIR Institute –

The FAIR website has a dedicated risk management tab on their website where it explains what risk assessment is. It explains that for a risk assessment system to be effective it must be explicit instead of implicit. An implicit system an organisation might have aligned its cybersecurity policies with a framework like NIST CSF, and it might have a NIST CSF-based enterprise risk assessment performed annually. The cybersecurity staff probably prioritise and works hard to address the findings from that assessment. Where an organisation ends up risk-wise however, is a by-product of these efforts [3]. To be an explicit tool we need a quantified risk target and provide long term or active management solutions.

FAIR also have a risk assessment tool known as "FAIR-U" or "FAIR UNIVERSITY". This tool runs in browser rather than being a downloadable application and provides users the ability to answer a variety of security questions to provide a run down on potential flaws. The tool requires an account, either one created for it specifically or a LinkedIn account. The interface is somewhat cluttered but offers many functionalities you would want from the type of tool that it is, such as inputting money earned and estimated breaches per-year.

Analysis results provided will provide a breakdown on all the losses you could be exposed to, the likelihood of a breach occurring and the percentage of which you are vulnerable. Losses are broken down into a minimum, average and maximum amount which can help offer a broader picture of what's at stake if you do not remedy the potential problem.



Example - Phishing Database Breach
Created October 25, 2021

Analysis Scope

A description of the asset, threat, and effect related to the scenario being analyzed. A well-defined scope is essential to accurate analysis.

Analysis Purpose

Understanding how much risk is associated with phishing campaigns that lead to database breaches.

Asset(s)

Generic Database

Threat Actor(s)

Cyber Criminals

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.54	1
Loss Magnitude	$4.0k	$47.2k	$196.5k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0.52	1
Loss Magnitude	$3.4M	$4.5M	$6.8M

Vulnerability 42.67%

1.3 Engineering Safety Consultants –

While not written from the perspective of cyber security the base topics of risk assessment can be used to help further our understanding of the process. With this deeper understanding we can cross reference how this risk assessment system works and overlaps in how a cybersecurity risk assessment system can work. It describes a breakdown of the various objectives in risk assessment along with when risk assessment is used during a products life cycle. Stating that the job of "managing risks throughout a project life is a role that a risk assessment tool fall into" [4].

2. Frameworks:

2.1 ISO Framework –

The ISO Framework is an industry standard used to help keep information assets safe. The exact type used in many businesses is ISO/IEC 27000 which provides requirements for an information security management system (ISMS). ISO was developed by the ISO/IEC joint technical committee JTC 1 and can be certified by third party external certification bodies. These bodies do use "several standards developed by ISO's personal conformity assessment committee called the CASCO Standards" [5].

2.2 NIST Framework –

The NIST framework is used similarly to the ISO framework with the intent to help organizations better understand and improve their cybersecurity risk management systems. They provide various files on the process which can be broken down to some basic headings. These are "Identify, Protect, Detect, Respond and Recover" [6].

3. Helpful Articles:

3.1 Risk Assessment in 5 Steps –

This articles primary purpose is to provide a basic breakdown on the process of risk assessment from a cybersecurity perspective. It gives various tips and insights into the how to perform cybersecurity risk assessment. Breaking down the process to a user by using keywords for instance can provide a concise method of relaying analysis results.

Analysis Results Breakdown Example	
Breakdown Description:	**Example of Breakdown:**
Threat Type -	A Stored XSS Injection
Asset -	Company Server
Vulnerability -	Unpatched
Consequence -	Hijacking of user accounts or sensitive data

4. Interface Design:

4.1 Designing the dashboard UI –

Designing the user interface needs to be an intuitive and easy to follow process, the reason for this is because many users will not necessarily understand the process of what they are doing and need the guidance. Treating it in this manner means most information will need to be provided in the easiest method possible and through dividing the dashboard into various "buttons", for homescreens, creating new sessions, downloading assessment or running the assessment. People recognise and associate logos with certain processes that could otherwise require some explaining if not represented in this manner. Pay attention to "what users take away from their time in other applications" [7] and put those practises into use in yours.

If a user cannot understand how to use a product within a certain amount of time, they will be less willing to return to it. Providing an interface similar to ones they may recognise is paramount to reducing time taken to learn how to use your tool. Design around philosophies used by companies like Microsoft in their office tools or FAIR-U in the portrayal of analysis results while maintaining your own tools "personality". Providing a guide will also help the user learn a tools functionality.

5. Assessment Saving Methods:

5.1 Cloudmersive –

Can be used to transfer information from your program into a excel spreadsheet using keywords signified with a "#" or "$" characters. It requires an account to work but cuts down on transferring information provided by the program after an assessment into an excel spreadsheet with little difficulty.

5.2 Utilising XML –

If information from the assessment is going to downloaded into a word document, we can take advantage of the docx utilising XML to transfer information from our program into the document. It allows all work on the project to remain within itself without the need for help from an external source such as cloudmersive but requires far more work.

References & Bibliography:

1. Meritt, J., n.d. *A Method for Quantitative Risk Analysis*. [online] Csrc.nist.gov. Available at: <https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/p28.pdf> [Accessed 17 November 2021].

2. NIST.gov. 2018. *Risk Assessment Tools*. [online] Available at: <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/risk-assessment/tools> [Accessed 18 October 2021].

3. FAIR Institute, n.d. *The Importance and Effectiveness of Quantifying Cyber Risk*. [online] Fairinstitute.org. Available at: <https://www.fairinstitute.org/fair-risk-management> [Accessed 19 October 2021].

4. ESC. n.d. *Quantitative Risk Assessment (QRA)*. [online] Available at: <https://esc.uk.net/quantitative-risk-assessment/> [Accessed 21 October 2021].

5. ISO. n.d. *Certification*. [online] Available at: <https://www.iso.org/certification.html> [Accessed 22 October 2021].

6. NIST.gov. n.d. *Cybersecurity Framework*. [online] Available at: <https://www.nist.gov/cyberframework> [Accessed 22 October 2021].

7. Justinmind.com. 2020. *Dashboard Design: best practices and examples*. [online] Available at: <https://www.justinmind.com/blog/dashboard-design-best-practices-ux-ui/> [Accessed 11 November 2021].

8. FAIR Institute, n.d. *FAIRU*. [online] Fairinstitute.org. Available at: <https://app.fairu.net/login?redirect=%2Fanalysis%2F24642> [Accessed 19 October 2021].

9. ISO. n.d. *ISO/IEC 27001 Information Security Managment*. [online] Available at: <https://www.iso.org/isoiec-27001-information-security.html> [Accessed 22 October 2021].

10. IT Governance. n.d. *ISO/IEC 27001 Information Security Managment*. [online] Available at: <https://www.itgovernanceusa.com/cyber-security-risk-assessments> [Accessed 24 October 2021].

11. Cobb, M., 2021. *How to Perform a Cybersecurity Risk Assessment Step by Step*. [online] techtarget.com. Available at: <https://searchsecurity.techtarget.com/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step> [Accessed 19 October 2021].

12. Usability.gov. 2020. *User Interface Design Basics*. [online] Available at: <https://www.usability.gov/what-and-why/user-interface-design.html> [Accessed 11 November 2021].