

An Investigation into the Benefits of Risk Management & Monitoring to aid Cybersecurity in an SME

MSc Research Project
Masters in Cybersecurity

Megan Haybyrne
Student ID: X21189439

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

**National College of Ireland
MSc Project Submission Sheet**

Student Name: Megan Haybyrne

Student ID: X21189439

Programme: Master Research Project

Year: Masters
Addon, 2023

Module: Masters in Cybersecurity

Supervisor: Mark Monaghan

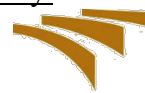
Submission Due

Date: 14th August 2023

Project Title:

An Investigation into the Benefits of Risk Management to aid
Cybersecurity in an SME, with a focus on email security.

School of Computing



**National
College of
Ireland**

Word Count: 6119

Page Count: 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Megan Haybyrne

Date: **18th September 2023** (Originally 12th August 2023)

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Contents

1	Introduction.....	2
2	Related Work.....	3
2.1	The Importance of IT Security Reporting within a Company.....	3
2.2	Reporting Styles/Sources.....	3
2.3	Email Security	4
3	Research Methodology	4
3.1	Research Process (steps).....	4
3.2	The Data Required to Answer Question.....	5
3.3	How I obtained the data.....	5
3.4	How I analysed this Data.....	6
4	Design Specification	6
4.1	Design and Solution Development.....	6
4.1.1	Desired Output.....	6
4.1.2	Technologies.....	8
4.1.3	Reporting Techniques	13
4.1.4	Model Description.....	13
5	Implementation	15
6	Evaluation	16
6.1	Case Study 1: Healthcare Company 1	16
6.1.1	About the Company.....	16
6.1.2	External Risk Scanning	16
6.1.3	Internal Scanning.....	17
6.1.4	Internal Risk Management	17
6.2	Case Study 2: IT Company 1.....	18
6.2.1	External Risk Scanning	18
6.2.2	Internal Scanning.....	19
6.2.3	Internal Risk Management	19
7	Conclusion and Discussion.....	20
	References	20
	Appendix	21

An Investigation into the Benefits of Risk Management to aid Cybersecurity in an SME, with a focus on email security.

Megan Haybyrne
X21189439

Abstract

The main goal of this project was to generate a cybersecurity report that could be communicated to any part of a company and would be understood by all. The main motivator for this product came from my own experience in IT and the confusion and misunderstandings I have witness between management and IT personnel when discussing reports and outcomes. IT is a separate world to most other areas of a business in terms of processes and terminology, and as IT professionals, I feel it is easy to forget that not everyone speaks and understands the same terminology that those in this area live and breathe. I set out to generate a report that would help cybersecurity personnel explain their overall work and scoring in the various areas it stretches across. I wanted to ensure that this report was meaningful to all, with or without IT experience, as I feel IT Security is becoming more and more prominent in businesses around the world, but not many understand what's involved.

The report I have generated will hopefully bridge this gap and provide a straightforward measurable reporting tool that can adequately monitor and represent improvements, or downgrades, in cybersecurity in companies of all sizes in all industries around the world.

1 Introduction

Throughout this project, the discussion will revolve around risk management and how it can improve the overall cybersecurity stance of a company in today's environment. This discussion will involve both internal and external risk management techniques, with a specific look at the tools most crucial to this area. The goal of this project is to combine these areas to adequately demonstrate, and measure, how risk management can be used to improve the overall cybersecurity of a company. I plan to demonstrate a reporting tool that can pull data from the relevant areas, to summarise the risk improvements for a selection of companies I began investigating at the start of this process, in February 2023.

The question that I highlighted earlier in my college course focuses on "*how adequate risk management can improve the overall cybersecurity of an SME in today's climate. When considering risks in an organisation*". The question will also delve into the use of a risk matrix, as a risk management tool and how this can help the overall implementation and management of risks. This metric will also be used to measure the effectiveness of the risk management within the organisation, with a specific look into email security.

The product that will be explored is a reporting tool that will pull together the various risk elements and present a dashboard that can be used to portray the improvement over time and summarise into a central location and generate a central overall score. The benefits of such a product include providing a central tool that allows information security professionals to demonstrate the current state and the improvement over time. This can be used as a monitoring tool for within the information security team and as a reporting tool to show board members/management the improvements over time. This is useful as it can show management and company leaders that the information security within the company is either adequate and worth the budget, or that improvements are needed and therefore can be used to push information security within an organisation.

2 Related Work

2.1 The Importance of IT Security Reporting within a Company

Before I began this project, I first went searching for similar work. I felt that researching what type of opinions are out there on IT security reporting was a good first step. One article I came across claimed that “A cyber security incident report is a document that captures the details of a cyber security incident, such as a data breach.” And while I definitely agree with the statement, it opened my eyes to the lack of awareness around regular IT security reporting and about how critical it can be in a business [1]. This article also claims that reporting such incidents is important to do “as soon as possible gives security teams the best chance of mitigating the threat and preventing the company from suffering damage and financial losses”, and again, I do not disagree. However, I think that my approach is building on this idea. My motivation is to generate a tool that helps to highlight the importance of cybersecurity without an incident or breach having to occur. My tool will help IT personnel to back up their requests and explain their workings without having to be using an incident as a benchmark. My tool will present all of the facts and risks facing the company and allowing for proactive management of these risks, without leaving gaps for cybercriminals to identify.

2.2 Reporting Styles/Sources

My investigations into the various reporting styles in IT also led me to an article that stated that “The advantage of using data gathered by OSINT is that security threats arising in cyberspace can be addressed. However, if a user uses data collected by OSINT for malicious purposes, information regarding the target of an attack can be gathered, which may lead to various cybercrimes, such as hacking, malware, and a denial-of-service attack. Therefore, from a cybersecurity point of view, it is important to positively use the data gathered by OSINT in a positive manner.” [2] This further solidified my belief that this is a crucial area for a company to be proactively managing. This article also highlighted a downside to OSINT reporting, claiming that “*The amount of information is too large*”. I found this to be the case also, and this further propelled my desire to present a tool that could summarise the important bits and communicate only what is required, which I feel my tool does.

The next area I investigated was regarding how important risk management is to an organisation, which I immediately found was considered important according to existing

works, for example “*A successful risk management program helps an organization consider the full range of risks it faces*” accurately sums up my opinion in this regard. [3].

2.3 Email Security

As email security was a big focus of mine when working with the two companies, I also investigated the importance of email security. I found multiple articles that agreed that this is a key area for a business to monitor and protect. [5] Another element that I felt important was phishing. A lot of the improvements in email security that was made were related to training end users, so I investigated this online to check that I wasn't working on something that others felt was unimportant. The general opinion was that this is a huge risk area to companies around the world, regardless of their size or industry. [6], [7], [8]. I didn't go into too much detail on my literary review as I have previously done a deep dive into this before starting my own project for a previous semester's assignment. So I also consulted my previous sources and read through, but for the sake of the word count, I will not delve into each source.

3 Research Methodology

3.1 Research Process (steps)

Step 1: My first port of call in generating my report was to get my companies setup on the five required platforms, Cynomi, Blackkite, Tenable IO, SimpleRisk and DecisionTime. These are discussed further throughout this report and the separate configuration steps are included in the configuration manual.

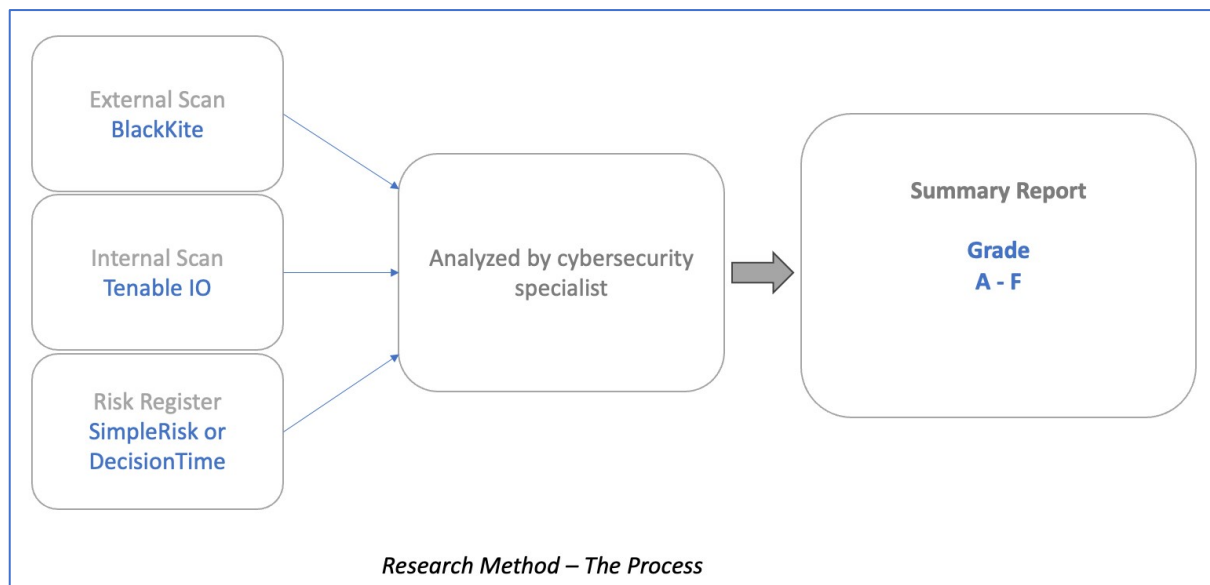
Step 2: the next phase consisted of populating and gathering the required data in these platforms. This included giving the external and internal reporting tools time to run and gather information on the companies in question.

Step 3: While this happening, I began the tasks of populating the risk registers. To discover the gaps in each organisation, I held meetings with the relevant members of the companies and went through multiple questionnaires in a gap analyse tool called Cynomi. This stage of the project was very time consuming as it required a lot of back and forth, and calls, to get all the required questions answered.

Step 4: This tool then takes all answers and spits out a breakdown of the areas a company needs to address and the areas that they do well in. My next step was to investigate these results and transfer the relevant points to the chosen risk management tool.

Step 5: Now that all tools were configured, I began the task of managing identified risks and vulnerabilities by advising the companies of the issues that we were uncovering. I used reporting as a way to flag these areas with the companies.

Step 6: The final stage of this was taking the gathered information and reports and calculating a cyber security grade for the company I was working on. The below diagram gives a high-level overview of how these tools and results were used to generate the desired output that I created for this project.



3.2 The Data Required to Answer Question

I felt that to adequately answer the present in this project, I would need to gather information on a range of companies to properly demonstrate the improvements in a selection of areas that show a good summary of the overall security improvements/stances of the companies in question.

I chose two types of companies to gather data on. These were healthcare companies and Information Security companies. I felt that two of each would be sufficient to demonstrate my points.

3.3 How I obtained the data

I am currently employed in a cybersecurity firm and therefore work with companies daily that are looking to improve their cybersecurity stance. This project presented a good opportunity to use the improvements obtained using risk management in a way that can be used to showcase how efficient this approach is in the overall cybersecurity of a company. I decided to incorporate risk management reporting into my workload for the sole purpose of acting as a metric in answering my research question.

As mentioned above, I decided to choose companies in two different areas.

- **Healthcare:** I picked two healthcare companies that were at the beginning of their cybersecurity/risk management journey, these are called Healthcare Company 1 and Healthcare company 2 throughout this report.
- **Information Security:** I also chose two information security companies that I felt would benefit from risk management procedures. These are named IS Company 1 and IS Company 2 throughout this report.

To begin my investigations, I had to setup my chosen companies in the platforms I decided to go with for my project. The platforms I loaded the companies into, and monitored them in, for the purpose of this project will be discussed in detail later in this report, but to summarise, I decided to use an external scanning tool, and internal vulnerability management

tool and an overall risk management/logging tool. I began my investigations in 2022 around the time that I came up with my research question.

Once I had the companies successfully setup and running in each platform, I began prioritising actions to be complete and logging the scores in each platform for each company at least monthly. By doing this, I was able to not only chose what areas to recommend they focus on in each company, but I was also able to see the changes and improvements that occurred as a direct result of the close monitoring on each system. I felt that the three types of platforms in use together presented a good overview of each company cybersecurity and would be ideal for answering the question at hand.

3.4 How I analysed this Data

This section is discussed in more detail in the configuration manual, with steps for how each bit of data setup and then pulled from the platforms. To summarised, I used the abovementioned tools to generate reports for the various elements and worked this into my report template.

4 Design Specification

4.1 Design and Solution Development

4.1.1 Desired Output

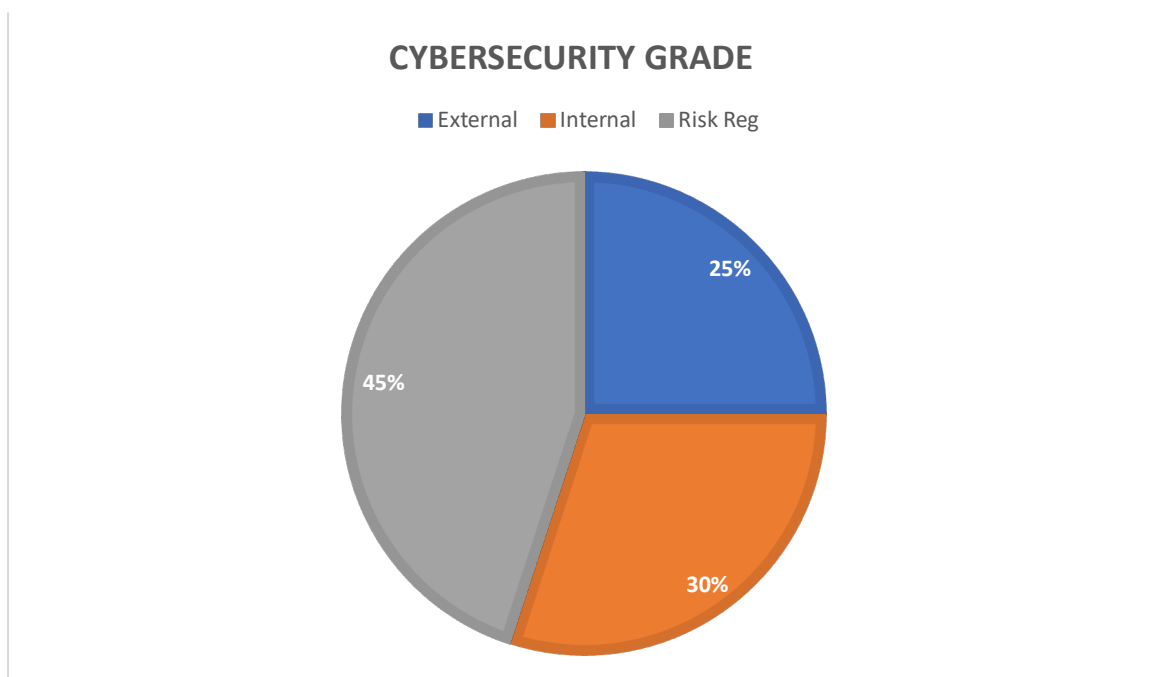
To fully understand the design aspect being described in the below sections, it is crucial to comprehend what exactly it is I was attempting to design. As mentioned, the question I hope to answer in this project revolves around how adequate risk management techniques can help to improve the overall cybersecurity stance of a company in today's climate. I felt that to successfully answer this "question", I would require a tool that considered the various elements of cybersecurity in a company and would pull information on these elements and summarise it into one dashboard. The goal of this dashboard is to not only show the overall cybersecurity status of a company at the chosen point in time, but to also provide comparisons that would allow a user to compare their company's stance before a certain project/framework was implemented. In relation to my research question, this product or tool, would allow me to successfully measure a company's cybersecurity "score" before a risk management strategy was implemented and then again after required changes were complete. As this tool consider all aspects of vulnerabilities, such as external, internal and risks, this would give an accurate answer to the question I intend to answer.

The second element of my report I implemented is an overall cyber "grade" that would give one a complete cybersecurity ranking. The way I calculated this score was by assigning a percentage of the score to each element I was reporting on. The breakdown and rationale is discussed below.

- **External Score** – In my opinion, this section of the report deserved 25% towards the complete grade. I felt this was appropriate as this section of reporting as it represents a big chunk of a company's potentially vulnerable assets. I also felt that this was the area that is worth the least against the other two sections as although it gives a good insight to potential external gaps, it is not always one hundred

percent accurate. The reason I say this is because, in my experience, this type of reporting can sometimes bring in false-positives when it comes to domains or retired systems. So while I think this is an important element to include, I think it should have the lowest impact on the score.

- **Internal Scanning** – This area is worth more of the overall grade in my opinion. I chose to assign 30% of the result to this section as it provides a real insight to the actual devices on the network and provides up to date, daily, reports on the actual vulnerabilities present on a company’s network at the time of the report.
- **Risk Management** – This is the area that I felt should hold the most weight against the end result. The reason for this is because this area encompasses all risks areas within IT and potentially effecting the IT infrastructure and data of a company. This doesn’t just deal with one section and it doesn’t pull from one tool, this can include alerts from all monitoring tools, from management and from security incidents and their opportunities for improvements (OFI). There are endless sources that a risk could come from which leads me to believe that this particular section is invaluable in demonstrating how well a company’s IT security is functioning. This does come with its own downfalls however. For example, if a company does not have a sophisticated information security management system, or IT security team, in place, their risk register may be inadequate or lacking in accurate details. This presents a potential gap. However, in this project, I felt that I had sufficient experience with risk management as this is my primary role so I feel that the risks I logged were mostly accurate and included the relevant risks to correctly show the company’s stance. I gave this area 45% of the grade.



4.1.1.1 End Result

By using the above approach, I also hope to generate an overall risk score by applying a certain weight, or percentage, to each area and using their scores to generate one score to summarise a company’s overall cyber score. The above pie chart shows the breakdown of

how each section contributes to this score. I understand that this may be viewed as a subjective score but I plan to include my rationale for the weight given to each section and will still include the breakdown of each area to give a well-rounded view to the recipients of such reports. This will be highlighted more as we go through the report.

The reason I felt that this was an area of cybersecurity that would be beneficial is because I see how difficult it is in my daily job to give an accurate presentation of a company's cybersecurity status to individuals that are not experienced in this area. By this I mean management, board members and stakeholders that are not very familiar with IT and its ever-evolving elements. These roles in a business are often responsible for big decision making and funding approvals for areas such as IT security, and I felt that a tool like the one I designed as part of my project provides an easy way to capture all of the required information and present it in a way that is easy to digest and monitor for readers of all levels of experience.

A	B	C	D	E	F
86 – 100	70 - 85	55 – 70	41 - 55	21 – 40	0 - 20

Image: Grading Breakdown.

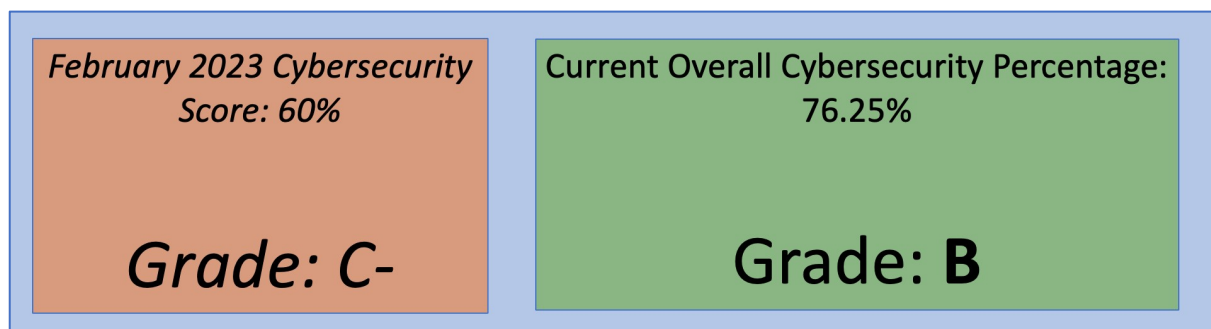


Image: Sample Result, from IT Company 1 Report

4.1.2 Technologies

Before I delved into answering my research question, I knew that I would require a range of tools and technologies that would allow me to measure the required elements to provide an adequate answer. As mentioned, the tool that is being discussed that will answer the research question, includes information for company risks, external vulnerabilities facing the company and its externally facing assets and then internal vulnerabilities that may affect the company's assets.

I have chosen four key technologies/platforms to use for my project which I will discuss in the following sections.

- For external vulnerability scanning Blackkite was chosen.
- For internal vulnerability scanning Tenable IO was used.
- For overall risk management I implemented Simple Risk.
- Risk identification was gathered using a tool called Cynomi.

I will now discuss how each can be used and how they benefit a company.

4.1.2.1 Black Kite

Blackkite is an Open-source Threat Intelligence (OSINT) tool that acts as a “good guys” view of what hackers use to scan networks to find externally vulnerable assets or network components. This tool is used by adding the company’s domain to the site, which begins pulling information that is available on the web related to this domain and any ports/assets and their vulnerabilities. The steps for this are discussed in detail in the uploaded configuration manual.

4.1.2.2 Tenable IO

Tenable IO is an internal vulnerability scanning tool that I configured on devices in the chosen companies, IT Company 1 and Healthcare Company 1, to scan their laptops/desktops on a daily basis and pull together reports on the different vulnerabilities found on each. This system rates vulnerabilities in a similar way to the risk management style I chose to use for this project, with the levels of vulnerabilities being rated by low, medium, high and critical.

This tool was used to present the internal section of my report. This is used usually in conjunction with an antivirus software, but for the sake of reporting, I did not include this in my analyse. The devices in question did already have antivirus (Microsoft Defender) installed but the alerts were not captured as part of my investigations.

4.1.2.3 Risk Management Tool

A risk management tool is the third tool that I took information from when pulling together the reports. This tool gives organisations a platform to log, update and report on anything that they consider a risk to the business. This was where I logged any related risks to the companies I was investigating.

In the two companies I chose to report on for this project, I used two different platforms to log their risks.

- **IT Company 1** – for this company, I used a tool named DecisionTime. This presented a more complex risk management tool that gives colourful, visual dashboard that are helpful in reporting.
- **Healthcare Company 1** – for this company, I chose to use a tool called SimpleRisk. This tool provides a more straight-forward approach to risk logging.

4.1.2.3.1 Risk Identification – Cynomi

Cynomi is a tool used to identify risks and gaps in certain areas of a company. When I began this approach, this was phase one of the project. This technology is a web-based platform that I used to go through multiple question sets for the companies I chose to investigate and input data regarding their setups and configurations. This platform then took the answers given and generate a report of all findings. The findings included a summary of what was complete, partially complete and not complete. I used this process as a gap analysis and identified what I felt were cyber security gaps and formed my list of risks from these gaps.

4.1.2.3.2 Risk Scoring & Risk Matrix

Once I had successfully identified the risk list for the company I was working on, I then had to identify the risk scoring formula I wanted to implement and use across my risk management section of this project. This is an area that I have dealt with previously in work so I had a few options to choose from. I decided to implement the below risk matrix, which uses a 5x5 structure and takes likelihood and impact into account when calculating the risk. There are five options in both of these categories that I will expand on below.

Likelihood:

- 1) **Rare** – this is used when the likelihood of occurrence is conceivable but extremely unlikely to ever occur in the company in question.
- 2) **Unlikely** – this applies to incidents that are uncommon but may occur in the future.
- 3) **Possible** – this is used regarding incidents occurring that are distinctly possible at some point.
- 4) **Probable** – this is used for incidents that are likely to occur before long.
- 5) **(Almost) Certain** – this applies to an incident that is bound to happen and is likely happening right now.

Impact:

- 1) **Insignificant** – this applies to incidents that would have minimal impact to operations if they were to occur, with negligible costs.
- 2) **Minor** – this should be used for incidents that would have noticeable but limited operational impacts if it were to occur in a company and would lead to a small cost.
- 3) **Moderate** – An incident in this section would lead to substantial operational impact and would be very costly for the company.
- 4) **Major** – an incident of this impact would result in severe loss of operational capability and would be highly damaging and costly for the company and its reputation.
- 5) **Extreme** – An incident of extreme impact would result in losses that the company could not survive and complete operational failure.

Total Risks Identified		Risk Matrix				
		Extreme	Major	Moderate	Minor	Insignificant
		Complete operational failure, "bet the farm" impact, unsurvivable	Severe loss of operational capability, highly damaging and	Substantial operational impact, very costly	Noticeable but limited operational impact, some costs	Minimal if any operational impact, negligible costs
		5	4	3	2	1
(Almost) certain	We are bound to experience further incidents of this nature - in fact they are probably occurring right now!	Red	Red	Red	Amber	Green
Probable	We are likely to experience incidents of this nature before long	Red	Amber	Amber	Amber	Green
Possible	It is distinctly possible that we will experience incidents of this nature	Amber	Amber	Amber	Green	Green
Unlikely	Incidents of this nature are uncommon but there is a genuine chance that we may experience them at some future point	Amber	Amber	Green	Green	Green
Rare	Although they are conceivable, we will probably never experience incidents of this nature	Green	Green	Green	Green	Green

Image: Risk Matrix (5x5 approach)

I used the above approach in to calculate the overall risk score. I applied two separate formulas for the two of the companies I chose to report on for this project, IT Company 1 and Healthcare Company 1. I will now discuss the formulas for each.

IT Company 1

For this company, I chose to use a formula that rated risks between 0 and 25 and used a green, amber and red colouring to identify the risk criticality.

- **Green:** this is made of risks with a score of 0-6 and would be accepted by the company in question as they pose a low risk to the company. This is the lowest level of risks and the lowest priority. This is referred to as a low risk.
- **Amber:** This represents the mid-level risks to a company and includes risks scored from 6 to 15. This is referred to as a medium risk.
- **Red:** red risks are the highest risks to the company and the highest priority that a company should address first. These risks have scores between 16 and 25 and highlight the areas that pose the biggest threat to the organisation. IT personnel would address this first when carrying out improvements or risk management tasks. This is referred to as a high risk. Red risks scoring 25 are considered critical in this setup.

The formula to calculate the score from this is to multiple the number assigned the impact by the probability (i.e., impact X probability).

Business impact

		Business impact					
		Extreme	Major	Moderate	Minor	Insignificant	
		Complete operational failure, "bet the farm" impact, unsurvivable	Severe loss of operational capability, highly damaging and extremely costly but	Substantial operational impact, very costly	Noticeable but limited operational impact, some costs	Minimal if any operational impact, negligible costs	
		5	4	3	2	1	
Probability	(Almost) certain	We are <i>bound</i> to experience further incidents of this nature - in fact they are probably occurring right now!	25	20	15	10	5
	Probable	We are likely to experience incidents of this nature before long	20	16	12	8	4
	Possible	It is distinctly possible that we will experience incidents of this nature	15	12	9	6	3
	Unlikely	Incidents of this nature are uncommon but there is a genuine chance that we may experience them at some future point	10	8	6	4	2
	Rare	Although they are conceivable, we will probably never experience incidents of this nature	5	4	3	2	1

Note: the colors are generated automatically using Excel's conditional formatting.

The values assigned to each category are *arbitrary* so don't obsess about them: concentrate the need to mitigate those unacceptable red/amber risks!.

Healthcare Company 1

This company has a similar approach and uses the same risk matrix, but when the formula is being calculated, the probability and impact are multiplied and then divided by 4.25 to give a score between 1 and 10. This approach also has 4 colours, green, amber, red and dark red.

- **Green:** this holds the same meaning as green in the first approach, but encompasses risks scored from 0-2.5. These risks are also accepted by the company.
- **Amber:** This is like the amber in the first company's approach, however, the risk scores included are 2.6 to 5.
- **Red:** Unlike the above approach, red does not represent the highest risk group. In this setup, red is a high risk and has a score of 5.1 to 7.4. They should be addressed as soon as possible.
- **Dark red:** these risks are known as critical risks and have a score of 7.5 to 10. These risks pose a critical risk to a business and should be addressed immediately. An example of such risks includes zero-day risks that have been released through threat intel.

Both approaches are slightly different, but both prioritise risks based on score and arrange them into criticality groups.

From here, I had to decide how to present my risks. I had two options for this area.

- **Excel based risk register** – I could manage my risk list through excel and manually update as I work on each section. The below screenshot shows the different headings that I would track against each risk. I decided against this approach as it requires a lot of administrative tasks to setup and update as risk

ID	Risk	Risk Description	Current Probability	Current Impact	Current risk rating	Treatment / Mitigating Controls already in place	Risk Reductions	Current Probability	Current Impact	Inherent risk rating
----	------	------------------	---------------------	----------------	---------------------	--	-----------------	---------------------	----------------	----------------------

status and scores change.

- **Risk Management Platform** – My alternative option was to use a risk management platform. As mentioned, SimpleRisk and Decision Time were the two risk platforms I chose to investigate. Both provided a way to update risks, log changes and presented dashboards of overall risk data that was helpful in the reporting model I generated for this project.

4.1.3 Reporting Techniques

Once I had my risk scoring and approach planned, I then had to figure out how I wanted to portrait the results to my target audience. As previously discussed, I had board members and management would be the key target audience for these reports as they are, ultimately, the people that sign off on budgets and approvals for IT projects, and therefore, IT security projects.

In my time working with different companies in my IT security role, I have found that summarised reporting is a good way to communicate updates to management within the company. I felt this would be a good approach. PowerPoint seemed like the obvious answer as it can be both sent and presented, depending on the preference of the company in question. I decided to go with a format that presented a summary of each section on one slide and then expanded on the overall score in the next slide. I also chose to include an appendices section that will expand on each individual risk area that is being summarised, the reason I decided to at it is to ensure all required information is available in the report in case the recipient has any questions that the summary does not answer. This brings the report to six slides in total, which is short enough to ensure that the reader does not lose interest, but long enough to cover all required points, to adequately represent the current cyber security stance of the company in question.

4.1.4 Model Description




As discussed in the previous section, the report I chose to go with is PowerPoint based but could be done as a PDF too if required. The product I created for this project is a report that uses Key Performance Indicators (KPIs) from a company's risk management and cybersecurity areas and summarised it into a page with key statistics and trending marked using red, orange and green colour markings. This summary is then used to generate a score between A and F to show the overall cybersecurity status of said company. The below pages are included in the presentation.

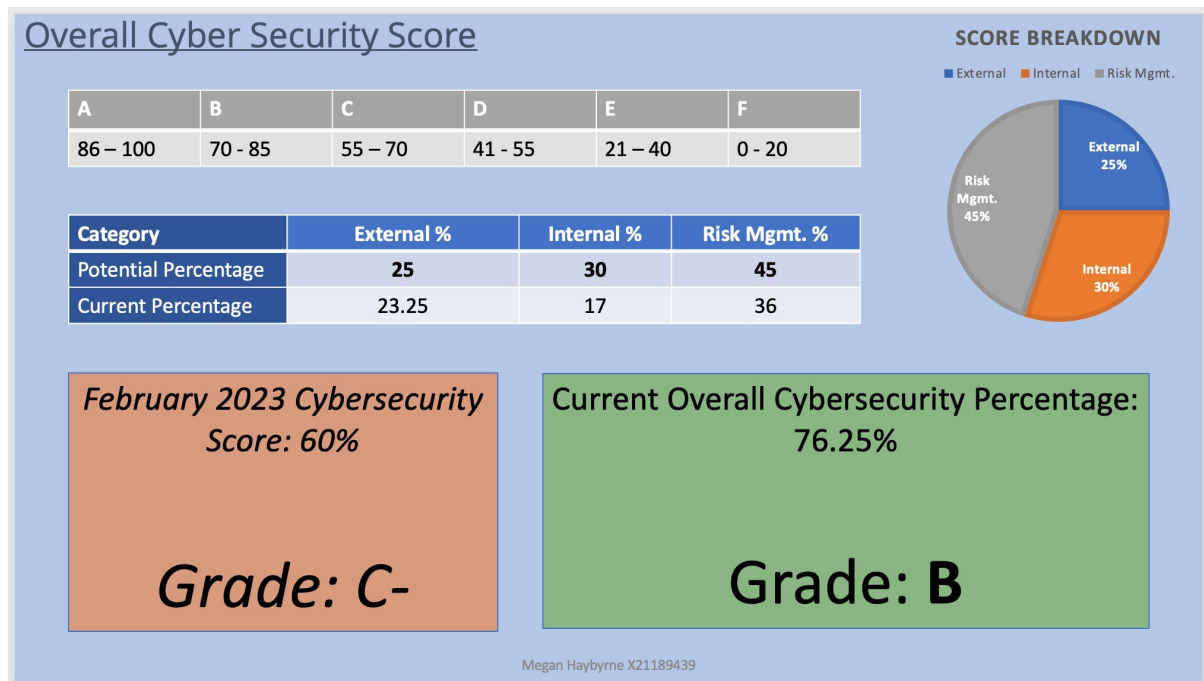
- Title page: this tells the reader the report title, the company title and the date it refers to.

- Summary page: this provides an overview of the cybersecurity areas. It shows the inherent score (starting point), the residual scores (current), the key points, target score and includes a trending section to show which sections are at the target score (green), improving but not there yet (amber) and not improving/below target (red).
- The next slide provides a summary of how each area is broken down in the overall grading system and provides each sections score. This also gives the inherent grade a company had and the current grade. The ideal result here would be the grade increasing. This is the case with IT company 1, in the below slide it shows that the score increased from a C- to a B.
- The remaining slides make up the appendices. These were provided as I have witnessed certain levels of management often require more information on certain topics but don't always want to be bombarded with information on every slide. I felt this was a good approach, going with the saying "better to have an not need, than need and not have" by giving readers the option to dig deeper into the various elements that contributed to both summary and overall cyber result pages. These include;
 - An external risk findings page.
 - An internal risk, or vulnerability management, page.
 - A Risk management page.

The following screenshots show how I broke down each of these section in my reporting model.

Summary Page:

Information Security Overview:							
Key Performance Indicators	Inherent Score - 6 months ago		Residual Score		Target	Trend	Key Points
Open Risks This shows the quantity of open information security risks grouped by their current (residual) score compared to their initial February 2023 score.	4		0		0 Red		<ul style="list-style-type: none"> • In the 6 months that we've been monitoring this company, the Red (high risks) have been mitigated and are not down from 4 to 0. • This is really good progress & the next steps are to mitigate the higher amber risks. • The goal is only having green (acceptable risks) – and although this is unlikely to occur, we continue to aim for this. <p>Percentage: 36% [80% x 45%] As all red reduced but further work for mitigation plans etc. required on amber risks.</p>
	45	7	38	19			
External Scan Score This score shows the current external risk score. This is captured by Black Kite. BK takes publicly available information and gathers information on any internet facing assets, devices or sites related to IT Company 1.	B+		A		A		<ul style="list-style-type: none"> • IT Company 1 currently have a score of 93% with an "A" rating in this area and we have no critical or high vulnerabilities. • This has been consistent for the last 4 months – since improvements increased the score from a B+ to an A grade - the reason for this is the fact that an A score is considered good so this hasn't been a priority action for this company. <p>Percentage: 23.25 [93% x 25%]</p>
Vulnerability (Internal) This is taking from our Tenable.IO platform that is scanning all VISO assets daily to check for any vulnerabilities or exploitable software.	9	41	7	26	0 Critical		<ul style="list-style-type: none"> • While this area is improving – it still is above the 0 critical target that we aim to achieve. • The plan to reduce this is to begin weekly reporting of vulnerabilities & chasing end users/IT support to get these vulnerabilities remediated and updated sooner. <p>Percentage: 15% [10% as all enrolled and 7% as going in correct direction but still not sufficient].</p>
	100% of devices enrolled.		100% of devices enrolled.		100% devices		



5 Implementation

As mentioned above, the above presentation is the desired output. To implement this, it involved a number of steps.

- The configuration of the various tools was crucial in this project, more details can be found in the configuration manual on this.
- The next important step for this was the actual managing of the various elements in the companies discussed. My presentation and discussions mainly revolve around the output I achieved, but majority of my time and efforts over the last six months went into working to ensure that the overall score for these two companies did improve. This included a lot of work that isn't necessarily mentioned in this report.
 - Overall management, for both of these companies, I provided a monthly report (like above) to communicate where each was at each month.
 - External risk management: This was reported monthly, but I also had weekly meetings with management and IT personnel in both companies (separately) to highlight the findings of the external scan. The approach here was to tackle findings based on criticality and work down through the list as we went. In some instances, new critical or high findings would flag via email and would require communications sent to the involved company to mitigate.
 - Vulnerability Management: A similar approach was taken for this area, this was also discussed in weekly calls and reported monthly. However, I also generated support tickets with the companies' IT Providers or IT team to get vulnerabilities mitigated or updated as required. The reason I did this is because new internal vulnerabilities popup more regularly then external

ones and can be easily updated (in a lot of cases) through group policy or a pushed out patch.

- Risk Management: Again, this was included in the monthly reports and discussed weekly. The weekly calls would include discussing and reviewing the risks based on criticality and whether or not the risk was due a review. On top of this, I would also work to update the risks daily (where there were updates to provide) based on ongoing projects or feedback from the company.
- The above checks and calls would all feed into the end report and help to generate improvements for my report to reflect.
- The other element included the overall grading system. I've discussed the percentage that I felt was fair for each of the three areas and the rationale for each percentage is included in the summary of the presentation.

6 Evaluation

6.1 Case Study 1: Healthcare Company 1

6.1.1 About the Company

This company is a small organisation that is responsible for managing a healthcare body based in the Republic of Ireland. It has roughly fifty users that primarily use laptops and desktops. They have no mobile devices in use.

6.1.2 External Risk Scanning

The Excel for this company presents more information on the overall status of the external scanning of the Healthcare Company. However, the below screenshot demonstrates the various changes of this company over the last few months.

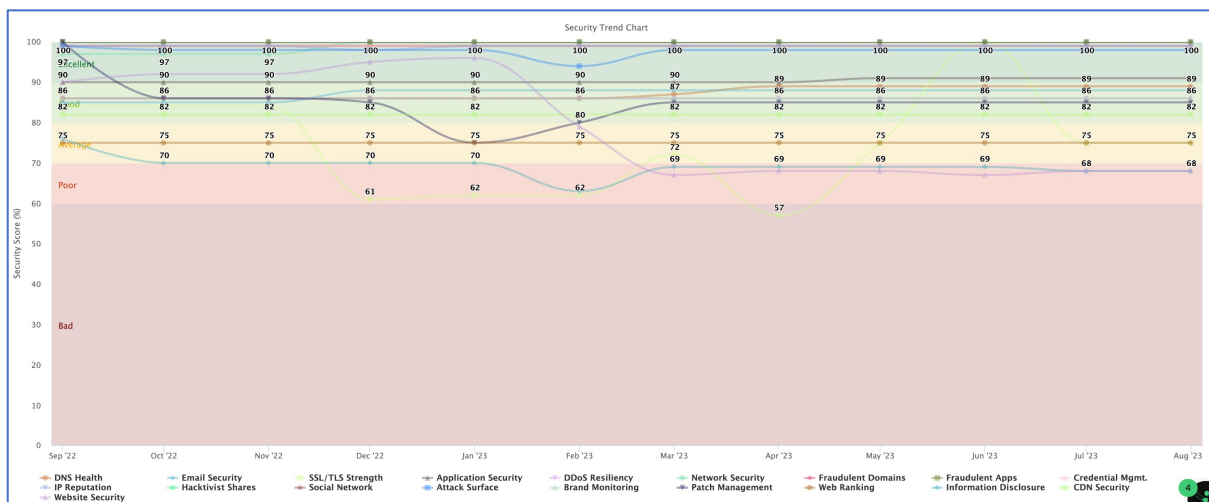


Image: Security Trends within Healthcare Company

6.1.2.1 Email Security Changes

The below screenshot shows how email security has increased from 85 to 88 in the few months it has been monitored. This particular screenshot demonstrates how this approach can be used to focus solely on one area of the business and its improvements.

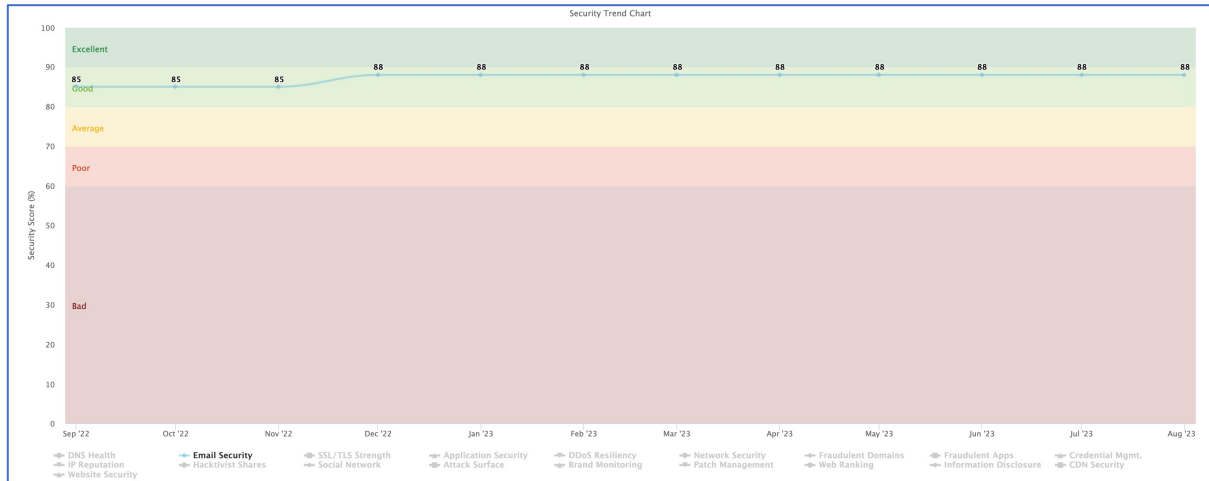


Image: Email Security Trend within Healthcare Company

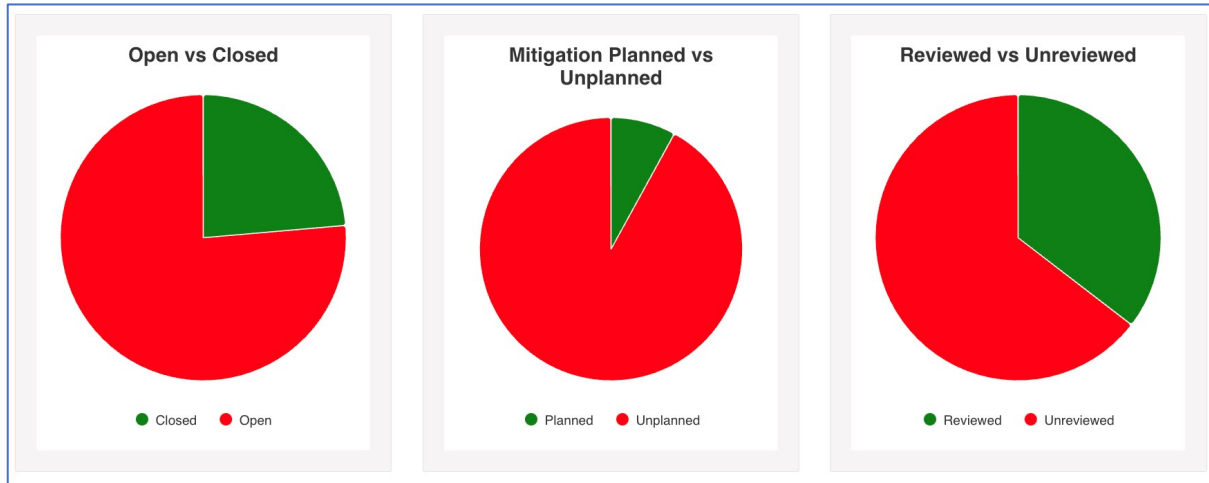
6.1.3 Internal Scanning

The internal scanning of this company is also summarised in the excel and is within the presentation. See the below snippet for an example of this.



6.1.4 Internal Risk Management

As above, this is expanded on in the attached excel and presentation but the below demonstrates this current status.



6.2 Case Study 2: IT Company 1

6.2.1 External Risk Scanning

The Excel for this company and the attached PowerPoint presents more information on the overall status of the external scanning of the IT Company. However, the below screenshot demonstrates the various changes of this company over the last few months.

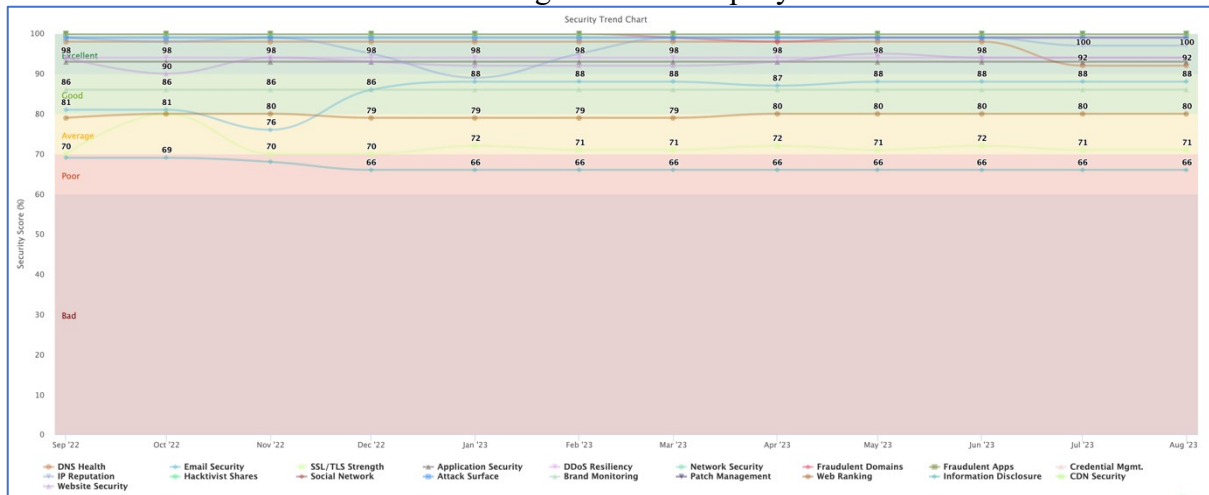


Image: Security Trends within IT Company

6.2.1.1 Email Security Changes

The below screenshot shows how email security has increased from 76 to 88 in the few months it has been monitored. This low score helped me to identify that this company did not make use of DKIM and DMARC records and this was one of our first recommendations once we completed this scan. This is reflected in the increase in scoring in this area.

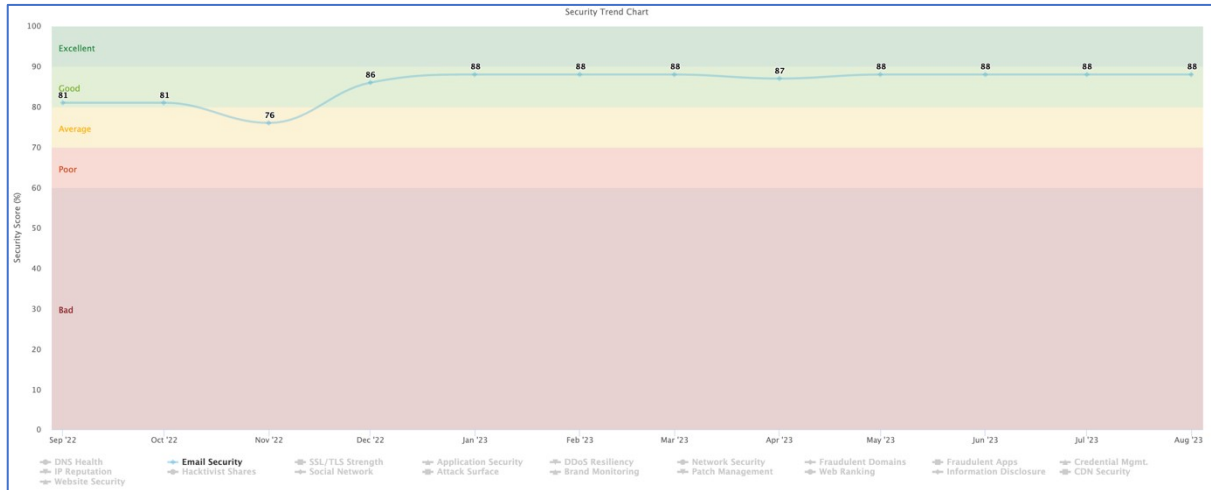


Image: Email Security Trend within IT Company

6.2.2 Internal Scanning

The internal scanning of this company is also summarised within the presentation. See the below snippet for an example of this.

Vulnerability (Internal) This is taken from our Tenable.IO platform that is scanning all VISO assets daily to check for any vulnerabilities or exploitable software.	9	41	7	26	0 Critical	<ul style="list-style-type: none"> While this area is improving – it still is above the 0 critical target that we aim to achieve. The plan to reduce this is to begin weekly reporting of vulnerabilities & chasing end users/IT support to get these vulnerabilities remediated and updated sooner. <p>Percentage: 15% [10% as all enrolled and 7% as going in correct direction but still not sufficient].</p>
	100% of devices enrolled.	100% of devices enrolled.	100% devices	Megan Haybyrne X21189439		

6.2.3 Internal Risk Management

As above, this is expanded on in the attached excel and presentation but the below demonstrates this current status.

Open Risks This shows the quantity of open information security risks grouped by their current (residual) score compared to their initial February 2023 score.	4		0		0 Red	<ul style="list-style-type: none"> In the 6 months that we've been monitoring this company, the Red (high risks) have been mitigated and are not down from 4 to 0. This is really good progress & the next steps are to mitigate the higher amber risks. The goal is only having green (acceptable risks) – and although this is unlikely to occur, we continue to aim for this. <p>Percentage: 36% [80% x 45%] As all red reduced but further work for mitigation plans etc. required on amber risks.</p>
	45	7	38	19		

7 Conclusion and Discussion

To conclude, I feel that the reporting tool I have generated allows for an easy to use reporting system that is accessible by people of all levels of technicality. I also think it summarises cybersecurity in a way that greatly benefits a company in managing the important elements to improve their overall safety.

If I had more time and resources to further develop my reporting tool, I would want to turn this into an automated platform that would pull the information from the various tools and gather it into an exportable page that could be shared with the company in question. The goal for this model is to provide central location to monitor and report on a company's cybersecurity stance to allow them to clearly see their problem areas and to also allow them to see the improvements occurring to their systems as they improve their risk management techniques and subsequently improve the security of their IT infrastructure. I envision this tool being used across all sectors of business and eventually being used to report on industry risk statistics that could help companies around the world by providing benchmarks for what to expect from cybersecurity in their chosen field.

Another element I would explore further would be the area of the overall risk score I've included in my report model. If I had more time on this project, I would have sought the opinions of specialists and major firms in cybersecurity on how best to calculate the percentage assigned to each risk area. I would also use these opinions to find out if there are any further risk areas that should be included as a part of the overall cybersecurity score. Currently, an A – F grading system is the best approach, but I would investigate other options to see if there was a more accurate or meaningful way to grade companies' cybersecurity.

References

- [1] *Cyber security incident report importance: RiskXchange* (2023) *riskxchange.co*. Available at: <https://riskxchange.co/1006863/cyber-security-incidentreport/#:~:text=The%20first%20reason%20to%20report,and%20how%20to%20mitigate%20them>. (Accessed: 12 August 2023).
- [2] Hwang, Y.-W. *et al.* (2022) *Current status and security trend of OSINT, Wireless Communications and Mobile Computing*. Available at: <https://www.hindawi.com/journals/wcmc/2022/1290129/> (Accessed: 12 August 2023).
- [3] Tucci, L. (2023) *What is risk management and why is it important?*, *Security*. Available at: <https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important> (Accessed: 12 August 2023).
- [4] Michael Power Envelope, A. *links open overlay et al.* (2009) *The risk management of nothing, Accounting, Organizations and Society*. Pergamon. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0361368209000580> (Accessed: August 1, 2023).

[5] Pandove, K., Jindal, A. and Kumar, R. (2010) “Email security,” *International Journal of Computer Applications*, 5(1), pp. 23–26. Available at: <https://doi.org/10.5120/8821253>.

[6] CybSafe (2023) *The ripple effect: How one phishing attack can cause disaster across your organization*, CybSafe. Available at: <https://www.cybsafe.com/blog/how-can-phishing-affect-a-business/#:~:text=Phishing%20attacks%20aren't%20just,outages%20and%20other%20nasty%20disruptions>. (Accessed: 1 August 2023).

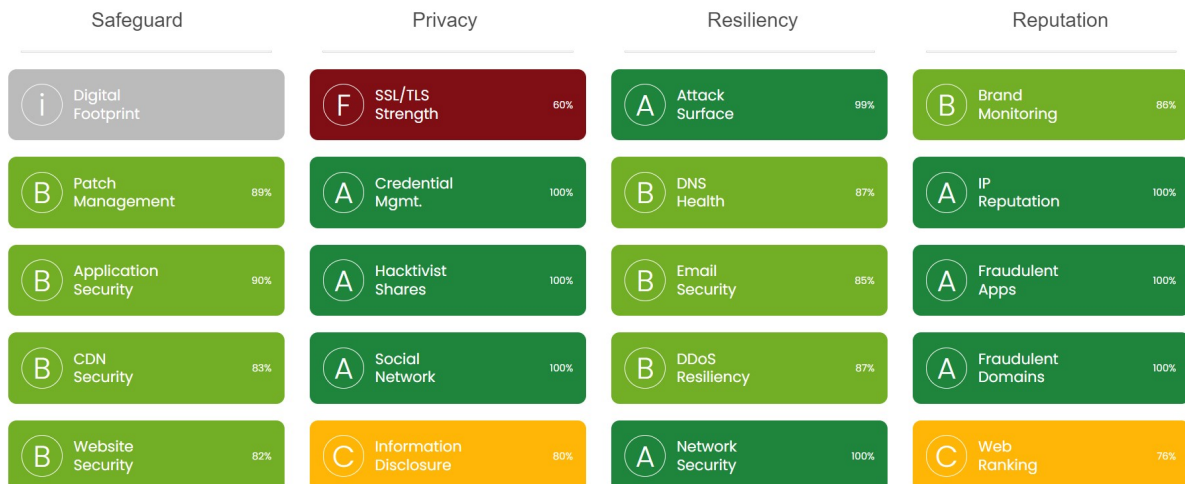
[7] *(Effect of personality traits on trust and risk to ... - IEEE xplore*. Available at: <https://ieeexplore.ieee.org/abstract/document/7497779> (Accessed: 1 August 2023).

[8] *How phishing poses a threat to your business* (2023) Cofense. Available at: <https://cofense.com/knowledge-center/phishing-threats/> (Accessed: 1 August 2023).

Appendix

Healthcare company 1 stats:

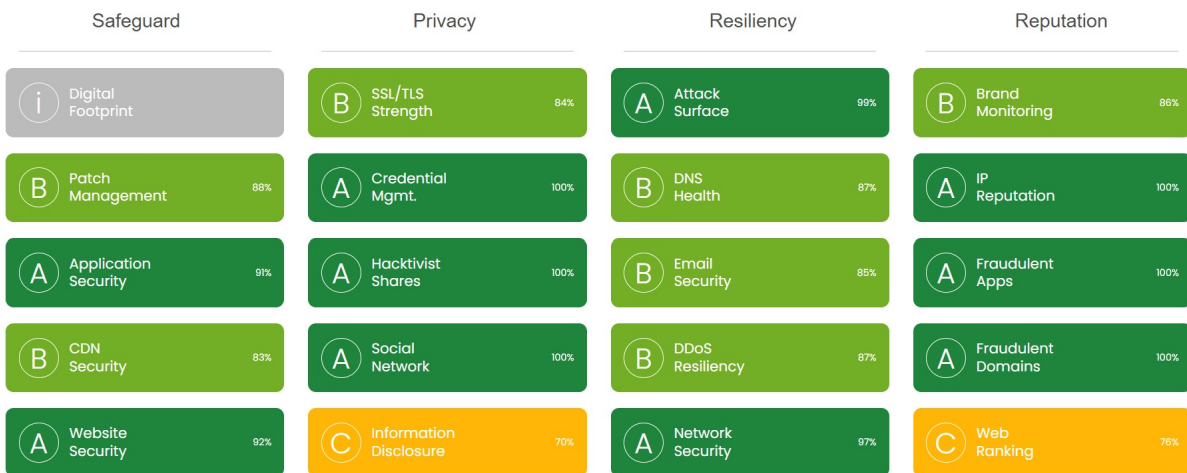
August



September 2022



October 2022



ID	Risk	Risk Description	Current Probability	Current Impact	Current risk rating	Treatment / Mitigating Controls already in place	Risk Reductions	Current Probability	Current Impact	Inherent risk rating
----	------	------------------	---------------------	----------------	---------------------	--	-----------------	---------------------	----------------	----------------------