National College of Ireland

Helping Non-Technical Business Executives Know if They are a Target of Cybercrime

MSc Research Project
Cyber Security

Jordan Robert Enwright
Student ID: X21238103

School of Computing
National College of Ireland

Supervisor: Dr. Imran Khan

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name: Jordan Robert Enwright

Student ID: X21238103

Programme: MSCCYB1 **Year:** 2023

Module: MSc Research Project

Supervisor: Dr. Imran Khan

Submission Due Date: August 14th, 2023

Project Title: Helping Non-Technical Business Executives Know if They are a Target of Cybercrime

Page Count: 29 (including Project submission sheet, references, and appendix)

Word Count: 9544

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: Jordan R. Enwright

Date: September 18th 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
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.	□

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):	

Helping non-technical business executives know if they are a target of cybercrime

Jordan Enwright
21238103

Abstract

The raise of cyber-attacks has posed significant challenges for Small and Medium Enterprises (SMEs). There is often a disconnect between cyber security employees and business executives which hinders effective risk management if the business even has a cyber security team. This research aims to address this gap by proposing the development of a Cyber Crime Attractiveness Score (CCAS). A way to score a business's cyber risk that utilizes basic business data to assess the likelihood of SMEs becoming targets for cyber criminals. Why use basic business data? Basic business data is used because unlikely firewall configurations, network segmentation, and other security policies, all employees should be able to answer basic questions about their business. These basic business specifications should be able to be tied to cyber risk factors. While other cyber security assessments exist most focus on being as detailed as possible which serves a great purpose but alienates those, they may need it the most, the non-technical staff. By focusing on simple business data and its connection to cyber risk, I believe that we can inform non-technical staff of their risk level without intimidating them. By providing executives with a clear and concise report, the CCAS aims to enhance their understanding of cyber risks, ultimately leading to improved cyber resilience within SMEs. To achieve this objective, the research follows a multifaceted approach. First, various cyber security reports are analysed to identify key elements and common vulnerabilities that make businesses susceptible to cyber-attacks. This analysis serves as a foundation for understanding the motivations and tactics employed by cyber criminals, allowing the research to gain insights into the dynamics of cybercrime across different business sectors. The research leverages this knowledge to develop the Cyber Crime Attractiveness Score (CCAS). The CCAS is designed to combine information from the cyber security reports with the basic business data provided by employees, enabling a comprehensive assessment of a business's risk of being targeted by cyber criminals. By combining these two perspectives, the CCAS can offer executives an accessible and easy-to-understand report to help motivate informed decisions about cyber risk management strategies.
Keywords: **cybersecurity, cybercrime, risk assessment, cyber risk**

1 Introduction

The field of cybercrime is experiencing a rapid increase, with supply chain breaches and ransomware attacks reaching alarming levels, as reported in the Verizon Data Breach

Investigation Report for 2022 (Verizon, 2022). Notably, ransomware alone accounted for nearly 13% of the investigated breaches, surpassing the cumulative increase of the past five years. Over the last few years, there has been a significant rise of approximately 30% in stolen credentials, highlighting the prevalent use of credential theft as a means of unauthorized access to organizations. While IT leaders and cybersecurity professionals possess a shared vocabulary to effectively address business concerns, there exists a disconnect when conveying these concerns to decision-makers, particularly in small and medium enterprise (SME) owners. As Benz and Chatterjee (Benz and Chatterjee, 2020) assert, "Few business executives understand the risks and do not see themselves as likely targets."

It is important to address the element that comes before any of these considerations, attractiveness. How attractive is a company to a criminal? On a base level a criminal is a criminal. The person who wants to burglarise a house might be deterred by exterior lighting and a guard dog, while other homes are just as defended by a mere fence and being in a lower crime area. Studies of criminals in the physical world has enlightened the public as to what things will generally deter criminals, and what makes a victim more attractive and therefore more motivating for the criminal. According to one study, having information about a person's financial status, a person's lifestyle, and even how a person walked made them more or less likely to be victims of robbery (Azumah et al., 2020). My research is the first step in the education process, before they are worried with implementing complex technical cyber security frameworks and mitigation techniques that they do not understand. My research aims to point out to the company the way that they "walk" through cyberspace and how that walk might be attractive to criminals.

To address this critical gap, there is a need to provide business executives with a simple yet compelling demonstration of the likelihood of their businesses falling victim to cybercrime. By utilizing data specific to their organizations, decision-makers can make informed decisions and allocate the necessary resources for comprehensive cyber security defences. This research aims to bridge the divide between tech-savvy cyber security personnel and business executives, ensuring the allocation of adequate resources for cyber threat defence. While business managers and executives may not possess intricate knowledge of their organization's network architecture, mail servers, IoT devices, or wireless access points, they are well-versed in their industry, the number of employees, and other essential factors that contribute to their company's attractiveness to cyber criminals. By providing decision-makers with a clear report on how appealing their company appears to potential criminals, they will be better equipped to engage in conversations regarding their business's cyber security needs.

The literature review indicates that greater awareness within a company correlates with better preparedness against cyber-attacks. Therefore, a quick and straightforward questionnaire can serve as an initial step towards strengthening a business's cyber defences. This not only benefits the business itself but also protects its employees, business partners, and the entire economic chain associated with it. SMEs are increasingly targeted, as they historically lacked the resources to allocate to cyber defence. Moreover, as more SMEs become providers to larger companies, they are targeted as vulnerable members of the supply chain.

By providing business executives with a Cyber Crime Attractiveness Score (CCAS), derived from a few key data points, this research aims to enable a robust assessment of a business's appeal to cybercriminals. Any employee within the organization possessing the relevant information should be able to complete the questionnaire to obtain the CCAS. With the CCAS in hand, discussing cyber security needs with budgeting authorities becomes more accessible, effectively bridging the gap between IT professionals and other business executives. By analysing comprehensive cyber security reports covering various industries and carefully considering reports on criminal motives, it is hypothesized that this information, combined with other key business data, can enable the assignment of a risk rating.

This research seeks to contribute to existing knowledge by providing a clear and concise score, devoid of technical jargon, to enhance the understanding of business executives regarding the risks they face. While there are numerous well-written reports from highly respected entities, such as the European Union Agency for Cybersecurity (ENISA) Threat Landscape Report (ETL) and Verizon's Data Breach Investigations Report (DBIR), these reports can be overwhelming for non-technical readers, often spanning over a hundred pages and delving into complex topics beyond the scope of an executive's understanding. The goal here is to create an easily comprehensible report, no longer than a single page, presenting top-level information in a concise and accessible manner.

Research Question: How can non-technical SME business executives be better informed as to how likely they are to be a target of cybercrime?

Figure 1: (NIST, 2019)

2 Related Work

My research required an understanding of risk and risk assessment. It was beneficial to examine previous work related to risk assessment and work that had enabled companies to gain a better understanding of their risk levels and potential vulnerabilities. Additionally, it was advantageous to understand the motives behind cybercriminals and comprehending the targets of cybercrime.

2.1 Calculated Risk

Several parties are deeply invested in comprehending risk. Notably, those financially motivated, such as business executives and insurance providers, are eager to understand and communicate about risk. To develop a cybersecurity evaluation tool (CET), M. Benz and D. Chatterjee utilized a 35-question online survey, administered to IT leaders, to self-assess their company's security posture (Benz and Chatterjee, 2020). Feedback indicated that the survey was "surprisingly accurate" in estimating costs and efforts from the participants' perspective. This survey does not directly compete with the proposed research, as the goal was to identify a subset of questions that could be asked while still providing a realistic representation of cyber risk and to create a scoring system for non-technical employees. Nonetheless, the work of M. Benz and D. Chatterjee was encouraging, and the proposed scoring system could potentially precede their survey. Once the scoring system was implemented, non-technical executives could receive a clear explanation of potential risks, possibly leading them to take M. Benz and D. Chatterjee's survey for further insights.

Insurance providers also showed a profound interest in risk assessment. Many insurance companies have begun offering cybersecurity insurance, which requires a better understanding of their clients' risk factors. Recognizing that cyber risk differed from conventional risk, the insurance sector had traditionally calculated (Böhme, Laube, and Riek, 2021). R. Bohme, S. Laube, and M. Riek highlight how standards and certifications could be indicative of good security practices from an insurance perspective. However, they noted that compliance with such standards didn't reliably predict actual security (Böhme, Laube, and Riek, 2021). Notably, even PCI DSS and NIST CSF couldn't prevent breaches, as demonstrated by the case of the US retailer, Target. This emphasized that security standards should not stand alone, and organizations must gauge their attractiveness to cybercriminals. Also, there is a lack of consistent standards for cyber security across sectors (CISA, 2023). Although the articles offered distinct cybersecurity insights, they were not designed for non-technical staff, potentially leading to inaction. The objective remained to prompt informed actions for enhancing business security, hinging on comprehension by business executives.

2.2 Target Acquired

After gaining a better understanding of the risks at hand, it became essential to identify the targets of cybercriminals. While considering as many factors as possible would have been ideal for my research, a paper based on Gmail accounts served as a baseline dataset to understand targets of phishing and malware attacks. As over 90% of successful cyber-attack are initiated through phishing emails (CISA, 2022). This dataset comprised 17.0 million weekly anonymized Gmail accounts targeted by phishing or malware (Simoiu, 2020). Though this research was limited to personal accounts and anonymization was necessary, similar targeting distributions could be anticipated in the business environment. The Verizon Data Breach Investigation Report (DBIR) revealed web applications, email, and carelessness as the top three action vectors for cyberattacks (Verizon, 2022). Combining insights from both documents underlined the critical role of email in security. Nevertheless, the exact significance remained uncertain, as both reports had limitations.

Regarding the origins of these attacks, it was important to categorize potential sources. Initially, one might have expected numerous threat actor categories. However, both M. Rai

and H.L. Mandoria's work, as well as the ENISA Threat Landscape 2022 report (ETL), identified only four categories. Although the labels differed slightly, both reports converged on four categories: state-sponsored, cybercrime, hacker-for-hire, and hacktivists (European Union Agency for Cybersecurity, 2022; Rai, 2019). Notably, state-sponsored actors resembled cyber warfare, and hacker-for-hire and cyber espionage could be subsumed into cybercrime. The alignment indicated that, for future research, three main threat actor groups could be considered based on motivations: state-sponsored, cybercrime, and hacktivism.

Ever since the COVID-19 pandemic “organizations must pay closer attention to securing mobile and BYOD ...which has expanded the risk surface” (Garcia Perez, Lopez Martinez and Gil Perez, 2023) as more and more employees work remotely. Remote work has drastically increased lately and with that so has the risk. Employees should be told not to proceed with sensitive work while using public networks and that their mobile hot spot is more secure than using public networks (Tripwire, 2023a).

2.3 Industry Reports and Governmental Reports

Industry level reports from Deloitte, IBM, Verizon, and Accenture, along with governmental reports like the UK's "Cyber Security Breaches Survey" (CSBS) and the European Union's ENISA Threat Landscape report (ETL 2022), provided insights into cybersecurity states and threat trends. Comparing industry reports to governmental reports revealed interesting differences in aesthetics, where industry reports were more visually appealing, while governmental reports prioritized content over design. This contrast was significant because reports that are difficult to read are less likely to be consumed, especially by non-technical individuals. Despite the alignment in presented information, the practical value of industry and government reports for average business executives is likely diminished due to the challenges of navigating the duller content presentation style. My research aims to streamline information for executives, while adhering to industry standards but enhancing readability.

IBM Security's "Cost of a Data Breach Report 2022" offered crucial data about industries affected by cybercrime and associated costs. However, while this data was essential, it didn't directly explain why certain industries were targeted. The expense of a data breach often far exceeded the criminal gains (IBM, 2022), emphasizing the need to delve deeper. The data from this report was used in my research to assess the CCAS provided to business executives. Comparing IBM Security's report with the UK's CSBS revealed that the CSBS focused exclusively on UK businesses and charities, whereas IBM's report aimed to encompass a wider range. The localized focus of the governmental report provides a narrower dataset for future research. CSBS also highlighted insights into business executives' involvement in cybersecurity and their perceived importance of it. Notably, only a small percentage carried out cybersecurity vulnerability audits or invested in threat intelligence (Department for Digital, Culture, Media, & Sport, 2021). Consequently, a secondary goal of the proposed research is to increase these numbers by offering information tailored to specific businesses, increasing their understanding of their likelihood of being targeted.

2.4 Culture of Cyber Defence

To quote (Sweeney, 2016) “All companies connected to the internet are vulnerable to cyber-attacks. And the potential losses are significant.” It is true, the only companies that are immune to cyber-attacks are ones that only exist in the physical world and never touch the internet, and those types of business are disappearing quickly, as even small companies run by elderly executives are brought online by well-intentioned younger family members or employees. If any part of the company uses the internet, cyber security needs to be a concern. A surprisingly effective defensive measure is “promoting a culture of defence” (Sweeney, 2016). Getting a cyber security employee is great, but a team is only as good as its weakest link. Cyber security employees need to be supported by CEOs and enabled to truly enact positive change in the organization if the company is to stand a chance against cyber-crime. Human error is a major contributing factor to data breaches according to many current reports, in fact more than 340 million people may already have been affected by a data breach only four months into 2023 (Tripwire, 2023b), "Humans are almost always a part of cybercrime, and investing in the people that form a company is essential to harness better security measures" (Tripwire, 2023b).

The more cyber security is discussed it becomes more important to temper the conversation to avoid fear mongering as well as complacency. While it is true that every internet connected organisation is at risk of being targeted by cyber criminals, that still true of physical criminals. It is not the intention of this paper to make people fearful to go about their digital lives, it is to inform them so that they may do so with better defences. However, "many mid-market organizations seem to have a sense of security bravado that leaves them particularly vulnerable to compromise... They do have valuable data but are generally unprepared for the assault" (Tripwire, 2017). In fact, 70% of ransomware attacks are lodged at organizations with less than five thousand employees, and 60% of them will go out of business within six months of the attack (Tripwire, 2017).

2.5 Current Cyber Security Frameworks

Most articles and papers discuss assessing cyber risk at a deep level, technical mitigation, prevention techniques, or reports of cyber-crime incidents. Most of the articles that are related to this work discuss cyber security for SMEs in terms the layperson would not understand. One article addresses a similar topic to my research, which is a paper by Benz and Chatterjee, (Benz and Chatterjee, 2020). Their paper addresses the cyber security concerns of small and medium sized enterprises (SMEs) with a cyber security evaluation tool. This cyber security evaluation tool is a 35-question online survey, which is intended to be completed by a company’s IT leader. The work done for this paper is detailed and well organized. When, considering most of the current IT leaders in SMEs, the IT leaders are not likely the ones that need an evaluation tool. “A team is only as good as its weakest link” (Tripwire, 2023b), and it is not the IT leaders that are the likely weakest link in any SME team but rather the non-technical employees. These non-technical employees are the employees who are most likely to be unaware of current phishing schemes, ransomware attacks, or malware trends. Even 40% of C-suite executives surveyed stated they lacked a clear understanding of their company’s cybersecurity protocols (Sweeney, 2016). While many similarities can be drawn between my research and that of Benz

and Chatterjee, the key difference is that my research is targeted at strengthening the “weakest link” on the SME’s team.

Another similar tool that exists is in the European Union Agency for Cybersecurity’s (ENISA) “Cybersecurity Maturity Assessment for Small and Medium Enterprises” This assessment is more than twice as long as Benz and Chatterjee’s evaluation tool with 70 questions in the first 2 of the 3-phase maturity assessment. The wording of the ENISA SME cybersecurity is clearly more targeted at less technically savvy employees, with a large percentage of the questions offering answer options of “I do not know” and “I do not understand the question” (ENISA, 2023a).

As a part of the research, I took the assessment for an Irish SME that I am intimately involved with and found the line of questions tedious and the website to not be user friendly. Between each question there is an awkward delay that makes the user think they need to click something else or that they missed clicking the “next question” button only for the page to load in time for the user to click the next button on the new question and that causes the user to have to click "previous" and thus the cycle continued for 70 plus questions. In addition to the poor user experience, many of the questions were not written in a way that was easy to understand. Some questions had grammatical errors that left the question open to a level of ambiguity, while other questions were written in a way that even a technical employee might need to research. Furthermore, this is a maturity assessment. It does not educate the user as to what is likely to make them a target of cyber-crime. Overall, it is great that this assessment exists, but my research project will develop a shorter questionnaire that will be easily understood without the need for any user to feel the need to answer, “I do not understand the question”.

Researchers at Mahidol University in Thailand also identified the absence of an efficient approach to measure and compare cybersecurity endeavours, resulting in a scarcity of vital data for the enhancement of cybersecurity. To address this, S. Malaivongs et el. proposed a Cyber Trust Index (CTI), a simplified framework for evaluating and enhancing organizations' cybersecurity performance. They developed baseline security controls from research papers and standards, alongside Control Enablers and Capability Tiers for measurement. The CTI was tested with 35 organizations, revealing that about 28.57% were beginners with high-risk exposure, 31.43% were leaders with low-risk exposure, and 40% fell in between. Control Enablers and cyber regulating bodies were identified as key factors differentiating these groups. The study emphasizes the importance of internal factors for cybersecurity and the positive impact of cyber regulating bodies, as mentioned earlier. The CTI framework offers a more efficient data-capturing process than previously seen in Thailand, using binary questions and question path techniques to reduce time and effort. It requires 50% fewer questions than their compared measurement methods, making it a more streamlined and resource-efficient approach. Their framework is one that should be emulated even though it’s “results may depend on a respondent’s motivation and cognitive skills to provide accurate responses” (Malaivongs, Kiattisin and Chatjuthamard, 2022), which is a limitation the CCAS plans to avoid by ensuring questions are simplified so that results are consistent across respondents of the same organization, regardless of their skills or knowledge.

ENISA's European Cybersecurity Month (ECSM) 2022 Campaign report discusses employee behaviour change for the better (ENISA, 2023b), which is also a shared goal of my research. My research hopes to present under-informed employees with a simple evaluation tool that explains to them their level of attractiveness to cyber criminals. The ECSM 2022 was an initiative for the European Union that was implemented by member states in their own way following the ECSM guidelines. The ECSM 2022 campaign report is the reported results of the campaign. However, the results in regard to user behaviour seem positive yet there is not enough information to get a deep understanding of how the behaviour was changed and what influences had more impact than another. This report is too far removed from the user level, it has reported information from the member state level which is far beyond the enterprise level my research is concerned with addressing. The report even states that "critical investigation needs to be undertaken, at an organisational and national level, to understand barriers to motivation, e.g., organisational or technological issues, as well as the level of security culture and risk of insider threat." (ENISA, 2023b).

The article titled "Adaptive vulnerability-based risk identification software with virtualization functions for dynamic management" written by Perez et al., focuses on implementing a software solution that SMEs can be used to perform automated risk management (Garcia Perez, Lopez Martinez and Gil Perez, 2023). Their solution is based on a virtual machine (VM) or docker container that can be operated on hardware the company already owns. The software takes some configuration and scans the business network daily. It indicates issues and keeps track of how long the issue has been present. While the work put into this article is impressive, it does not meet the needs of the layperson who does not know what a VM is or what to do about the issues once the system has identified a concern. Furthermore, the first question a company may be asking is why they need this security solution. The answer could come from getting their Cyber Crime Attractiveness Score (CCAS) from my research project.

Source	Summary
Benz Chatterjee, 2020	Their work targeted SMEs but IT professionals at SMEs
ENISA 2023a	A framework for SMEs but still showed that it was not for non-technical employees with questions offering answers of "I do not understand the question"
ENISA 2023b	Reported the results of the European Cybersecurity Month Campaign from 2022.
Böhme, Laube, and Riek, 2021	Indicated good security practices and highlighted that standards do not predict security.
Simoiu, 2020	Highlights the importance of email security.
CISA, 2023	Notes a lack of security standards across sectors.
CISA, 2022	Mentions cybercrime trends and other useful statistics
Verison, 2022	Contained vital information about cyber-attacks and attack vectors.
IBM 2022	Mentions the cost of cyber-attacks.

ETL, 2022	Covers many topics and is used at a European Union member state level.
Tripwire 2023a	Notes that employees need to be cautioned against using public networks
Tripwire 2023b	Mentions the fact that human error is a major factor in cybercrime.
Garcia Perez, Lopez Martinez and Gil Perez, 2023	Discussed the expanded risk surface of an organization using BYOD
Rai 2019	Discussed the motivations for cybercrime.
MKC 2022	Proposed a cyber trust index, focused on companies in Thailand, but allowed for variance in responses depending on who completed the framework.
Department for Digital, Culture, Media, & Sport, 2021	Covers cyber security issues related to the United Kingdom.
Tripwire, 2017	Mentions the fact that most cyber-attacks are targeting SMEs
Sweeney, 2016	While being the oldest reference, it still had many relevant points when it came to the executive's perspective of cyber security.

3 Research Methodology

This research builds on the security frameworks that have come before it, mainly, the National Institute of Standards and Technology's (NIST) cybersecurity framework (CSF), Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals (CPG), and European Union Agency for Cybersecurity's (ENISA) Cybersecurity Maturity Assessment for Small and Medium Enterprises (CSMA for SMEs). Each framework was evaluated and compared to the goals for this research. Then each question asked in the frameworks was reviewed and categorised as to whether or not it should be used in this research.

3.1 NIST CSF

This cybersecurity framework is highly regarded and widely adopted as a standard methodology in the United States of American. Its primary objective extends beyond safeguarding individual organizations, aiming to guide the development of the nation's cyber resiliency infrastructure and foster a safe and secure environment.

The NIST CSF serves as a universal language to articulate cybersecurity activities, risk profiles, business objectives, and improvement goals. It is designed to accommodate the unique needs, risk tolerance, and resources of both public and private entities. Comprising 96 standards organized into categories and subcategories (refer to Appendix 1), the framework establishes a comprehensive approach to cybersecurity (NIST, 2019).

However, the NIST CSF does have certain limitations. While it empowers organizations of all sizes and cybersecurity expertise to implement risk management principles and best practices, it demands a considerable effort to adopt. Learning an entirely new vocabulary, as outlined in

the 55-page guidebook, proves to be a challenging task. The complexity of comprehension and implementation adds to the difficulties faced by organizations.

Another drawback is that the NIST CSF lacks explicit guidelines for acceptable ratings on the stated standards. Consequently, organizations are unable to assess the effectiveness of their security policies and procedures in comparison to others. Furthermore, the framework does not offer predefined best practices or specific recommendations for improvement. Instead, each organization must independently set its targets for enhancement based on its unique environment. The NIST CSF is a good tool for the IT professionals of larger companies where they do not need to perform several roles and can focus on a single task such as implementing the NIST CSF over the course of several months or even a year. Where in smaller businesses the IT professionals are more likely to be handling a wider range of responsibilities without being able to dedicate the large amount of time needed to properly implement the security framework. The IT professionals may not even be afforded the resources, time or financially to implement the NIST CSF, especially when the non-technical executives do not understand the risks.

3.2 CISA CPG

The CISA CPG, is based on the NIST CSF and maintains the same core functions of addressing identify, protect, detect, respond, recover (CISA, 2023). The main improvement regarding the focus of this research is that "the CPGs are written and designed to be easy to understand and relatively easy to communicate with non-technical audiences, including senior business leadership" (CISA, 2023). These performance goals are on track with what this research aims to do but could still be seen as a second step in the cyber security defensive discovery phase of a SME. This is because the shear breadth of content the CPG covers as well as some of the terminology is still not immediately understood by non-technical employees. However, the CPG does include a glossary which should help bridge some of the knowledge gaps users may have. There are 38 questions in the CISA CPG checklist (CISA, 2023) which are well labelled and include rankings for cost, impact, and complexity. This will serve as the reference for the recommendations used after users receive their CCAS.

3.3 ENISA CSMA for SMEs

This assessment had 3 sections, and it took answering 70 questions to get through only the first 2 sections of the assessment. Users were not able to complete the last section unless they had answered enough questions to qualify the user to be able to access the highest tier of cybersecurity maturity or updated the answers from the first two sections to represent improved cybersecurity stance. This assessment was tedious, and the user-interface was not smooth. The wording of several of the questions left the question ambiguous and hard to answer even for a person who is aware of cyber security terminology. This assessment is offered by ENISA, along with several articles about securing SMEs and the challenges and recommendations for SME cyber security. These other articles were found to be very informative and written in a way that would be easier for more people to understand. Wording and phrases cues were taken

from these associated articles to help word the CCAS and ensure the CCAS users were able to understand the questions.

3.4 Cyber Crime Attractiveness Score Development

After evaluating each of the aforementioned cybersecurity frameworks, one thing was clear, they are not written in a way that communicates the risk of cyberspace to laypeople. Each question asked by the previously mentioned assessments was reviewed and any question that used a technical term, industry jargon, or was ambiguous was left out, while still noting the category of the question. From the remaining questions ten questions were selected that would cover the most foundational elements of cybersecurity that any non-technical employee should be able to answer. These questions were then further supported by more research to ensure that they covered the key foundational areas of cybersecurity for SMEs, while being void of jargon and technical terms. Also, the finalized questions are meant as a true starting point. Where many of the other evaluation tools currently out require that the user has some understand of technology or cybersecurity or that the SME already have some security features implemented, as is the case with the ENISA CSMA for SMEs. The questions are meant to be able to be answered by any employee with basic information about the company so that if any employee were to get the CCAS they could share it with an executive and the wording would be in a way that they all could understand.

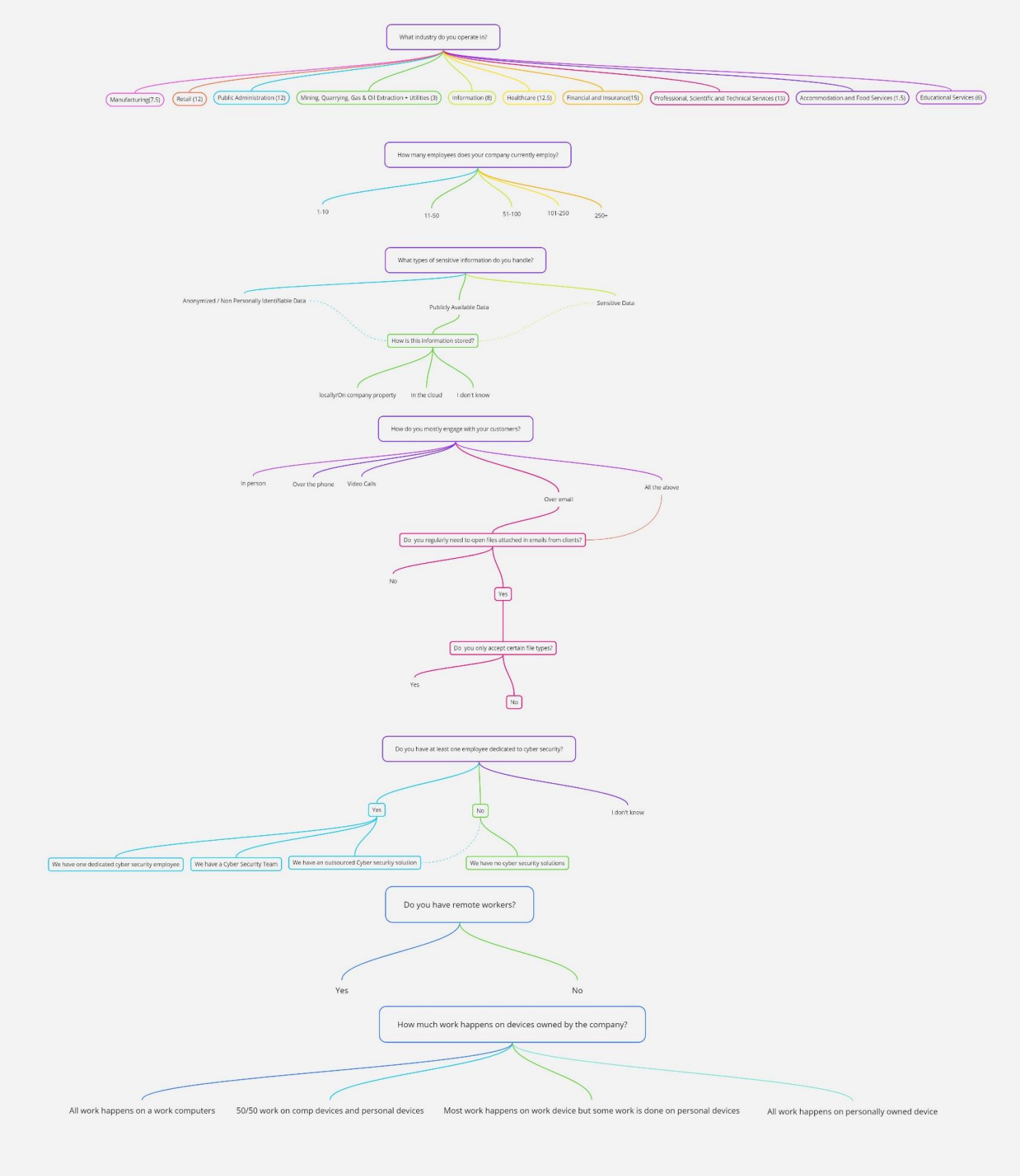


Figure 2: CCAS Question Flow Chart

	Questions									
Reference/Source	1	2	3	4	5	6	7	8	9	10
(Garcia Perez, et el., 2023)	X									X
(Malaivongs, et el., 2022)			X							X
(Sweeney, 2016)								X		
(Tripwire, 2023b)		X								
(Tripwire, 2017)		X	X							
(Tripwire, 2023a)									X	
(CISA, 2022)	X				X	X	X			
(Verizon, 2022)				X						
(Ojoawo, 2023)					X	X	X			
(ENISA, 2023b)		X		X				X	X	
(NIST, 2019)	X	X	X	X	X	X	X	X	X	X
(CISA, 2023)	X	X	X	X	X	X	X	X	X	X
(ENISA, 2023a)	X	X	X	X	X	X	X	X	X	X
CIS CSC	X	X	X	X	X	X	X	X	X	X
COBIT 5	X	X	X	X	X	X	X	X	X	X
ISA 62443-2-1:2009	X	X	X	X	X	X	X	X	X	X
ISO/IEC 27001	X	X	X	X	X	X	X	X	X	X
NIST SP 800-53	X	X	X	X	X	X	X	X	X	X

Table 1 Supporting Documents

4 Design Specification

Each of these questions are supported by the preceding cybersecurity frameworks but narrowed down to focus on what is likely to be the ten easiest questions for a non-technical employee to answer. By asking these questions, a Cyber Crime Attractiveness Score can be established based on giving each answer a weighted score and adding all the scores from each question answered into the overall score. This score would represent less targeted organisations with a smaller number and more targeted organisations with a larger number. The CCAS aims to identify cyber risks and convey them to non-technical employees. This enables the CCAS to be understood by the users and should aid them in being able to implement security measures and enhance the user's overall cybersecurity posture.

Question one is "To which industry does your company belong?" Looking at the 2022 Verizon Data Breach Investigations Report (Verizon, 2022), the ENISA Incident Reporting (ENISA, 2022), and other sources point out that different industries are attacked by cyber criminals with varying amounts of success. The question of what industry a SME operates in adds to the SME's CCAS by taking into consideration the industry's reported incident frequency. The user's CCAS is increased by an amount that represents the frequency with which the industry has experienced cyber incidents. The industry titles are maintained from the Verizon report as they closely resemble the titles used by ENISA and other cybersecurity reports.

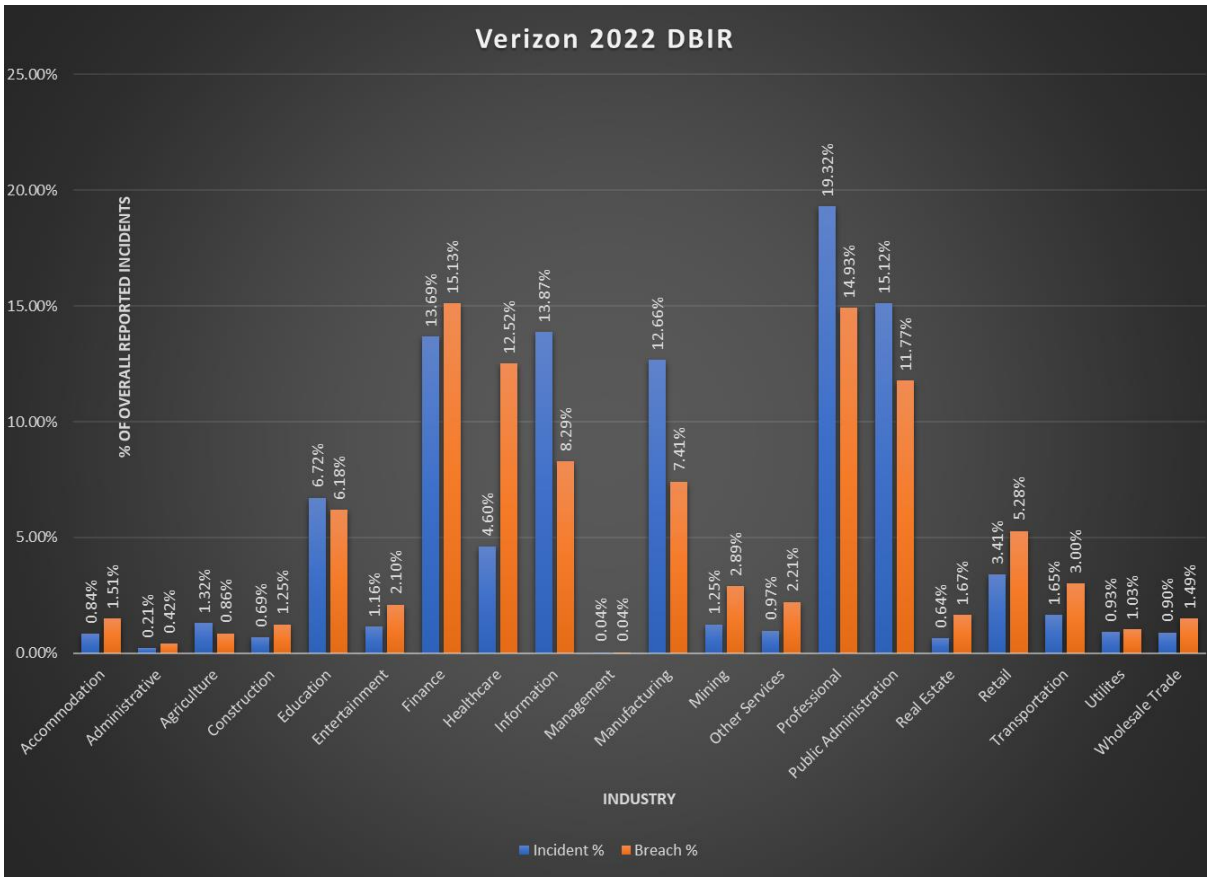


Figure 3. Data from Verizon DBIR 2022 visualized in a chart.

Question two is “How many employees does your company employ?” The number of employees directly impacts cybersecurity efforts. Larger organizations may have a larger attack surface and more sensitive data to protect. Understanding the size of the workforce helps tailor cybersecurity strategies, allocate resources appropriately, and prioritize cybersecurity investments based on risk exposure. In general, the definition of a SME is a company that has less than 250 employees, so that number is set as the upper limit to this question. This question looks at the overall attack surface as it relates to the human component. If a company only has 5 employees, it is easier to communicate to everyone the need to be vigilant about not clicking on malicious email attachments and there is a smaller chance that an employee's email for example is targeted because there are so many other options out there for cyber criminals. However, in a company of 200 plus employees it takes more effort to reach every employee on the same level of urgency about, to use the same example, clicking on a malicious email attachment.

Question three is “What types of sensitive information do you handle?” This is given with the following options for answers: Anonymized Data/ Not Personally Identifiable Information, Publicly Available Data, Sensitive Data. Each option here can add to the attractiveness of the data to cyber criminals as some information people are more eager to protect than others. A SME might not be as worried if their client call list of first names and phone numbers gets stolen as this information could be publicly available versus if a SME loses client medical or financial data. This question went through a few revisions as the research progressed.

Originally, it was thought that different types of data might be more attractive to criminals than another, but the real separation of data types is anonymized data, where all personally identifiable information has been stripped away, publicly available data, and sensitive data. Sensitive data is any data that can be tied to a person or business and used to gather more information than would be publicly available. According to the Center for Internet Security (CIS) Control 13, Data Protection, "all data is classified and protected in accordance with established data classifications (Center for Internet Security, 2023). To establish these data classifications, organizations should develop a list of the key data types and define the overall importance to the organization. This can be used to create a data classification scheme for the organization. Labels, such as "Sensitive," "Business Confidential", and "Public," should be used. The information owners need to be aware of the classification policy and the tools, procedures, and controls on said data" (Tenable, 2023).

ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	· CIS CSC 13, 14 · COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· CIS CSC 19 · COBIT 5 BAI02.01, MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · NIST SP 800-53 Rev. 4 -1 controls from all security control families

(NIST 2019)

Question four is "How is this information stored?" This is one of the only times where the option to answer, "I do not know" is given. This is because it is hard to ask about storage of the data without getting into technical terminology and it is important that users feel they can answer the questions honestly. This also offers a chance to assess the user to some extent. Because if the user is willing to admit they do not know where the data is when it is at rest, then the survey has truly reached the intended audience. As it is built for those who might not know where their data is at all times and the first step in the more advanced frameworks is "Identify" where your data is as well as the assets on the network. The devices will be discussed in later questions. This question focuses on the storage of sensitive information, which is a critical aspect of cybersecurity. Non-technical employees may use various storage methods like local machines, USB flash drives, cloud services, or shared drives. Each method has its security implications. Understanding how information is stored helps identify vulnerabilities and ensures that proper security measures (e.g., encryption, access controls) are in place to safeguard the data. This question provides an opportunity to educate users about cloud security in the results section of their CCAS report.

PR.PT-2: Removable media is protected, and its use restricted according to policy	· CIS CSC 8, 13 · COBIT 5 APO13.01, DSS05.02, DSS05.06 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8

(NIST 2019)

Question five is “How do you mostly engage with your customers?” With the options of in person, over voice calls, video calls, email, all the above. Customer engagement practices involve various communication channels (e.g., email, messaging apps, video conferencing) that can be vulnerable to cyber-attacks. Understanding how employees engage with customers helps identify potential attack vectors like phishing or social engineering attempts. By knowing the preferred communication channels, the organization can educate employees about associated risks and implement additional security measures to mitigate potential threats. Having a defined way or ways that employees are allowed to interact with customers can offer a layer of security, because the approved communication platforms should be protected and be covered in cyber security trainings. This question addresses several foundational cyber security concerns for example the flow of data through an organisation, communication channels, email security, phishing/vishing/smishing attacks and basic cybersecurity training.

ID.AM-3: Organizational communication and data flows are mapped	· CIS CSC 12 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
PR.DS-2: Data-in-transit is protected	· CIS CSC 13, 14 · COBIT 5 APO01.06, DSS05.02, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

(NIST 2019)

Question six is "Do you regularly need to open files attached in emails from clients?” Opening attached files from clients can expose employees to malware and other cyber threats. This question helps gauge the frequency of such activities and assess the level of awareness among employees regarding the risks associated with opening attachments. It enables the organization to reinforce safe attachment handling practices and implement technical solutions like email filtering to reduce the likelihood of malicious attachments reaching employees' inboxes.

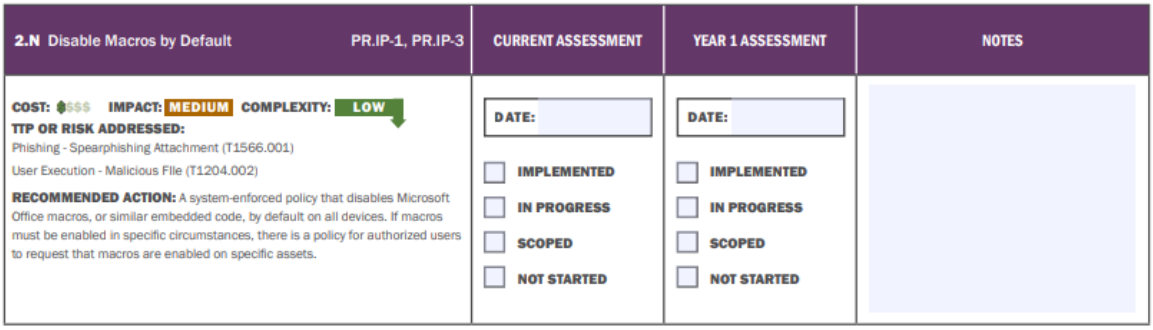
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	· CIS CSC 9, 14, 15, 18 · COBIT 5 DSS01.05, DSS05.02 · ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7

(NIST 2019)

Question seven is “Do you only accept certain file types?” Accepting only certain file types is an effective security measure to prevent the introduction of malware or malicious content. By understanding the organization's policies or restrictions on file types, the CCAS can identify areas where security measures are in place and make necessary adjustments to enhance security. CISA CPG recommends disabling Microsoft Office macros by default on all devices. If the macros must be used in certain scenarios, there should be a policy in place for authorized users to be able to request that the macros be enabled.

PR.DS-5: Protections against data leaks are implemented.	·CIS CSC 13 ·COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ·ISA 62443-3-3:2013 SR 5.2 ·ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 ·NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

(NIST 2019)



(CISA, 2023)

Question eight is "Do you have at least one employee dedicated to cyber security?" Having a dedicated cybersecurity professional is crucial for maintaining a proactive and effective cybersecurity posture. This question assesses the organization's commitment to cybersecurity and risk management. A designated cybersecurity employee can actively identify and address security gaps, implement best practices, and respond promptly to potential incidents. This question also provides insight into the SME's cybersecurity maturity. A SME with even one single dedicated cybersecurity employee is more likely to have a higher cybersecurity maturity score than SMEs that do not have anyone employed to deal with cybersecurity issues.

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· CIS CSC 17, 19 · COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.GV-1: Organizational cybersecurity policy is established and communicated,,	·CIS CSC 19 ·COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ·ISA 62443-2-1:2009 4.3.2.6 ·ISO/IEC 27001:2013 A.5.1.1 ·NIST SP 800-53 Rev. 4 -1 controls from all security control families
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	· CIS CSC 19 · COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 · NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2

(NIST 2019)

Question nine is "Do you have remote workers?" Ever since the Covid-19 pandemic there have been more remote workers than ever before in the history of the internet. The rise of remote

work introduces unique cybersecurity challenges. Remote workers may use personal devices and connect to unsecured networks, increasing the organization's exposure to cyber risks. Knowing the number of remote workers helps the organization tailor security measures to address remote work-related cybersecurity concerns.

PR.AC-2: Physical access to assets is managed and protected	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
PR.AC-3: Remote access is managed	· CIS CSC 12 · COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15

(NIST 2019)

Question ten is “How much work happens on devices owned by the company?” With the answer options being all work happens on a work computer, 50/50 work on company device and personal device, most work happens on a work device, but some work is done on a personal device, all work is done on a personally owned device. Understanding the extent of work happening on company-owned devices is vital for assessing the organization's control over its information and security practices. Company-owned devices can be managed and secured more effectively compared to personal devices used for work. This question helps identify areas where stronger security measures or training on secure device usage may be required.

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	·CIS CSC 3, 9, 11 ·COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ·ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ·ISA 62443-3-3:2013 SR 7.6 ·ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 ·NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
ID.RA-1: Asset vulnerabilities are identified and documented	·CIS CSC 4 ·COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ·ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ·ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 ·NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

(NIST 2019)

The web application was developed using the MERN stack, which stands for MongoDB, Express, React, and Node.js. The MERN stack was chosen because the researcher is familiar with the technology, and it provides built-in security features. The first step in development was to allow users to securely create accounts and sign in, achieved by following a MERN tutorial (Traversy, 2023).

The CCAS web application is built around a scoring system, where each question has a set of answer options with specific values associated with them. The scoring system is designed to assess the attractiveness of an organization to cyber-crime. The questions were narrowed down

to the ten easiest ones for non-technical employees to answer, making it accessible to users with different levels of knowledge.
Each answer option is weighted either with a real-world data as in question one where data about industries cyber-crime incidents was used or by using CGP's impact rating of low, medium and high. Where answering in a way that was out of alignment with a CPG labelled high impact, the answer option would be valued higher for example 250 points, while answering out of alignment with a goal labelled low impact would be valued lower for example 100 points. Answering in line with performance goals would be valued lower still for example 50 points. This is to ensure that risk is never underestimated. It would be irresponsible to provide a false sense of confidence by valuing answers that were in line with cyber security performance goals as zero, because that would be interpreted as being a zero risk which is unfortunately never the case in cyber security.

The scoring system is based on assigning weighted scores to each answer option and then adding all the scores from each question to calculate an overall score. This score represents the organization's attractiveness to cyber-crime, with larger numbers indicating more targeted organizations and smaller numbers indicating less targeted ones.

The CCAS utilizes data from the Verizon Data Breach Report as well as many other cyber security reports to assign logical values to the answer options in relation to real-world cybersecurity incidents. The data from these reports help to ensure that the values assigned to the options align with actual cybersecurity risks. The other cyber security reports that were used to inform the selection of questions and values associated with the answer options include NIST CSF, CIS CSC, COBIT, ISO/IEC 27001, and NIST SP 800-53 Rev. 4. As stated above each question can be mapped to the more complex preexisting frameworks.

The goal of the CCAS is to be understandable to non-technical employees and executives. Therefore, the web application's user interface was designed to be simple, short, and easy to comprehend. The questions are to be clear and concise, and the answer options are straightforward.

Since the web application deals with sensitive information, it is crucial to implement security measures to protect user data and prevent unauthorized access. The MERN stack was chosen, in part, due to its built-in security features, Json Web Tokens are used in the authorisation process to ensure data privacy and integrity. Passwords are immediately hashed and salted to ensure confidentiality and integrity.

The scoring system and logic used to calculate the Cyber Crime Attractiveness Score must be accurate and reliable. The questions and their associated values are based on sound research and data, ensuring that the resulting score provides a realistic representation of an organization's cybersecurity posture.

5 Implementation

The web application is the product of the research performed. The research led to the types of questions to ask users and how best to word these questions. Now, to allow people to benefit from this research a web application was developed to be able to tell users how attractive they might be to cyber-crime. To develop this web application, the MERN stack, which stands for MongoDB-Express-React and Node.js, was used due to the researcher's familiarity with the technology stack as well as its built-in security features. The first step of development was to build a way for users to securely create an account and sign in. This was accomplished by following a MERN tutorial (Traversy, 2023). Next, a scoring system had to be developed for each of the questions. Some questions have many answer options, and each answer option needed its own value. As in question one where the user is asked to state in which industry do they operate, there needs to be a value associated with each industry option. The values of each option also need to make logical sense in relation to the reports about cybersecurity incidents in the real world. Other questions were simple. Yes or no were the only options, so the value for those questions had to make sense with the context of the question and the cybersecurity reports. For example, the question about does the company have at least one employee dedicated to cybersecurity, there are three answer options: yes, no, and I do not know. For the sake of this question, the “no” and “I do not know” options are both given the same value, which is more than the value associated with if the user answers “yes”.

When evaluating this research, it is important to consider the cyber security frameworks that are currently published. Most of them are written in a way that does not meet the average users at their level of understanding. The current frameworks are mostly written to assist IT professionals in their pursuit of ever enhancing the cyber defences of their work environment. These frameworks are not written at an introductory level so that more people can understand them. The CCAS that has been established through this research allows anyone no matter their knowledge level to be able to get an understanding of their current cyber security posture. The CCAS is not a better cyber security framework than those already published, but it is a better starting point than any of the current frameworks. The CCAS’s line of questions are short, simple, and important. This meets the goal of the research by being able to communicate cyber security needs to non-technical employees and executives. The hope is that any employee all the way up to the CEO of a SME can take the CCAS and know that there is some level of concern and will help counter act some of the over confidence in SME’s cyber security or the lack of concern over cyber security (Tripwire, 2017).

The implementation of the proposed solution focuses on the final stage of the project, which involved the development of a web-based application called the Cyber Crime Attractiveness Score (CCAS) that assesses an organization's vulnerability to cyber-crime. The main outputs produced during this implementation phase include the web application, the scoring system, and easy to read results accompanied by CPG’s recommendations. The CCAS web application was developed to allow users to assess their organization's cyber security posture. The application provides a user-friendly interface for non-technical employees and executives to answer a set of ten carefully selected questions. These questions were designed to be easily understandable and concise.

The final output of the CCAS web application is the Cyber Crime Attractiveness Score, represented by a numerical value. This score indicates the organization's vulnerability to cyber-crime, with larger scores implying a higher likelihood of being targeted and smaller scores suggesting a lower attractiveness to cyber-criminals.

Lastly, the CCAS questionnaire was tested by several business executives and the web application receive positive feedback as to its utility and simplicity. Tester's feedback included comments such as “Oh, yes this was very easy to understand, I was afraid when you asked me to look at something with cyber security, I wouldn’t be able to know what how to answer the questions, but I was able to answer each question honestly and found the recommendations very useful.” and “Wow, we are on the higher side of the risk spectrum, I really didn’t think we were that bad off. This is good to know.” and “Very user friendly. Easy to do in under 5 minutes.”

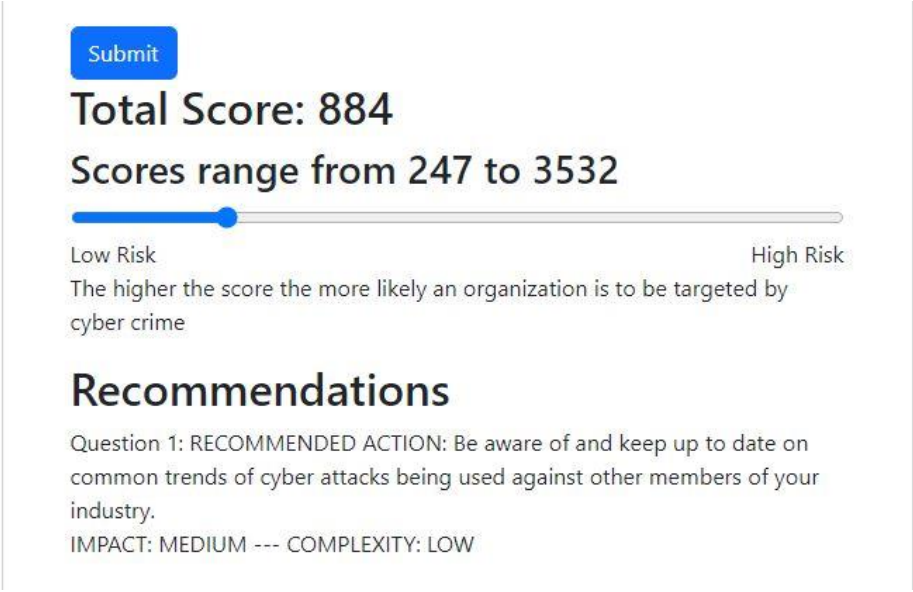


Figure 3. Screen shot of the results section and a CCAS more screen shots: appendix 2,3,4,5

Tools and Languages Used:

1. MERN Stack:
The web application was developed using the MERN stack. MongoDB was employed for data storage, Express facilitated backend development, React was used for building the user interface, and Node.js supported server-side functionality.

2. Data Sources:
Data from the Verizon Data Breach and Incident Report, NIST CSF, CISA CPG, ENISA’s incident and other sources were used as a key reference for assigning logical values to answer options. This helped in ensuring the accuracy and relevance of the scoring system.

3. Web Development Tools:

Various web development tools, such as VS Code, Node Package Manger (NPM) as the package manager, and git and GitHub for version control, were utilized to streamline the development process.

The implementation phase of the project focused on creating the Cyber Crime Attractiveness Score web application using the MERN stack and incorporating the scoring system. The outputs produced include the fully functional CCAS web application capable of calculating and presenting a numerical score representing an organization's vulnerability to cyber-crime.

6 Evaluation

To assess the research, involves verifying that the research effectively addressed the research question. Upon scrutinizing the data gathered during the data analysis phase, patterns emerged, aiding in resolving the research question. To corroborate this further, the questionnaire CCAS, in conjunction with feedback from end users, will offer insights into how these observed dataset patterns manifest in real-world scenarios. Subsequent validation transpired during the research's testing phase, wherein beta testers validated the utility of the Cyber Crime Attractiveness Score and Recommendations. The main findings of this study are that there is a way to inform non-technical employees of cyber risk without using technical jargon. By reviewing the most popular cyber security frameworks available today, as well as cyber security incident reports, cybersecurity articles, and research papers, key areas of concern can be identified and communicated without all the complexity currently found in cyber security frameworks. Because the CCAS operates as an entry point into understanding cyber risk, it does not cover the components that would be associated with an organization that has a higher level of cyber security maturity such as detect, respond, and recover as in NIST CSF and CISA CPG. Most of the CCAS questions are focused on the identify and protect segments of the NIST CSF. Three questions are dedicated to digital communications as “more than 90% of successful cyber-attacks start with a phishing email” (CISA, 2022). This statistic clearly shows the importance of protecting SME’s email and other forms of communication. By reading many cyber security resources and comparing what each had to offer the end users, it was determined that it is possible to communicate cyber risk to non-technical executives while still providing a realistic indication of risks.

6.1 Case Study

	Number of Questions	Complexity	Use of technical terminology
NIST CSF	96	High	Yes
CISA CPG	38	Medium	Yes
ENISA CSMA for SMEs	70+	Medium	Yes
CCAS	10	Low	No

Table 2 Comparison of Cyber Security Frameworks

6.2 Discussion

The limitations of this kind of research are categorised into two separate limitations. The first of which is that all the cyber security data is reliant on reported incidents. It is likely that SMEs are being targeted and they are not even aware of the incident, so it goes unreported, or the organization is embarrassed and does not want to report the incident as most organizations list reputational damage as the most likely result to a data breach as well as legal liabilities (Sweeney, 2016). The second limitation is that the threat landscape is constantly changing and evolving.

As of writing this section, there is news of artificial intelligence being used to clone a person's voice and the new AI voice is impersonating people over phone calls and scamming people other the phone. "Be cautious of phone calls: Be suspicious of phone calls that ask for personal information or try to trick you into giving away sensitive data" (Ojoawo, 2023). These results are a good snapshot of the current situation but would need regular maintenance to stay up to date with the current cyber security attack trends.

My proposed work focuses on the development of a cybersecurity awareness tool tailored for small and medium-sized enterprises (SMEs), with a primary objective of ensuring accessibility and understanding for non-technical employees. It effectively identifies the limitations of existing cybersecurity frameworks, which often employ technical terminology and industry jargon, making them inaccessible to laypeople. The criteria for selecting the questions for the tool, were mainly the exclusion of technical terms and jargon, is a practical approach that aims to democratize cybersecurity awareness within SMEs.

My research recognizes the unique needs of SMEs in the cybersecurity domain, where limited resources and expertise may limit the implementation of complex security measures. The validation of the CCAS through beta testing further enhances its credibility and utility by both executives and employees. This underscores the importance of fostering cybersecurity awareness at all organizational levels.

However, the proposed work would benefit from a more comprehensive evaluation of existing frameworks, a deeper comparative analysis with other cybersecurity tools, and a clearer exposition of the research methodology employed to validate the selected questions. These enhancements would bolster the tool's effectiveness in promoting cybersecurity awareness and practices among SMEs while accommodating the dynamic nature of the cyber threat landscape.

7 Conclusion and Future Work

Can non-technical SME business executives be better informed as to how likely they are to be a target of cybercrime? Could a series of questions be identified that could convey to non-technical employees a realistic level of cyber risk, in a way that they could understand and not be intimidated by answering these questions? The objective of this research was to discover if there was a subset of key factors that could indicate a realistic level of cyber-crime risk to non-technical executives and their employees. After gathering and analysing many

recently published papers and cyber security articles, it is the researcher's belief that it is possible to do just that. The analysis of the cyber security industries' leading organizations reports from the likes of ENISA, CISA and NIST leads to the key findings that while not a complete picture of an organization's cyber risk can be created from only ten questions, but a realistic estimate of cyber risk can in fact be made from only a few key questions.

As for the proposals for future work, there are several efforts to be pursued. Firstly, it would be beneficial to get the CCAS tool in front of more testers who self-identify as "non-technical" and would be willing to give honest feedback as to what they do and do not understand about their CCAS, and well as how recommendations could be improved to further help understanding. By aggregating feedback from the testers, the researcher can refine the questionnaire and the reporting process, gaining a more comprehensive understanding of the requirements and inclinations of the participating individuals. Ultimately, this feedback will contribute to the enhancement of future work, ensuring the alignment with the needs of the end users. Secondly, it would be beneficial if users were able to get a CCAS from the CCAS web site and then send it to their co-workers and bosses, so that more people in the organization can be aware of their cyber risk. Lastly, one of the minor objectives of the research was to be able to confirm that various employees of the same organization should get similar if not the same CCAS. This was never tested as all the testers worked for different organizations. In the future it would be ideal to be able to present the CCAS to an entire company at once, have all the employees get a CCAS and then compare and see how aligned the scores were this can help the CCAS improve and could show executives how aligned their employees are or are not when it comes to their understanding of the company's cyber risk.

References

Azumah, F.D., Nachinaab, J.O., Krampah, S. and Ayim, P.N. (2020). Determinants of Target Victim Selection: A Case Study of Criminals from Gambaga Prisons. *Journal of Victimology and Victim Justice*, 3(1), pp.93–112. doi:https://doi.org/10.1177/2516606920927258.

Benz, M. and Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, [online] 63(4), pp.531–540. doi:https://doi.org/10.1016/j.bushor.2020.03.010..

Böhme, R., Laube, S. and Riek, M. (2021). *A Fundamental Approach to Cyber Risk Analysis*. [online] Available at: https://www.casact.org/sites/default/files/2021-07/Approach-Cyber-Risk-Bohme-Laube-Riek.pdf [Accessed 15 Apr. 2023].

Center for Internet Security (2023). *CIS Control 3: Data Protection*. [online] CIS. Available at: https://www.cisecurity.org/controls/data-protection.

CISA (2022). *YEAR IN REVIEW CISA 2 0 2 2*. [online] Available at: https://www.cisa.gov/sites/default/files/publications/CISA-YearInReview_v1_508.pdf.

CISA (2023). *PERFORMANCE GOALS*. [online] Available at: https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

Department for Digital, Culture, Media, & Sport (2021). Cyber Security Breaches Survey 2021. (Cited by 20)

ENISA (2022). *Incident reporting*. [online] CIRAS. Available at: https://ciras.enisa.europa.eu/ [Accessed 10 Aug. 2023].

ENISA (2023a). *Cybersecurity Maturity Assessment for Small and Medium Enterprises*. [online] ENISA. Available at: https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises/ [Accessed 10 Aug. 2023].

ENISA (2023b). *ECSM 2022 Campaign Report*. [online] *https://www.enisa.europa.eu*. Available at: https://www.enisa.europa.eu/publications/european-cybersecurity-month-2022-campaign-report [Accessed 10 Aug. 2023].

European Union Agency for Cybersecurity (2022). ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022: European Union Agency for Cybersecurity.

Garcia Perez, A., Lopez Martinez, A. and Gil Perez, M. (2023). Adaptive vulnerability-based risk identification software with virtualization functions for dynamic management. *SSRN*, [online] pp.1–30. Available at: https://ssrn.com/abstract=4469646 [Accessed 10 Aug. 2023].

IBM (2022). *Cost of a Data Breach Report 2022*. [online] Available at: https://www.ibm.com/downloads/cas/3R8N1DZJ.

Malaivongs, S., Kiattisin, S. and Chatjuthamard, P. (2022). Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance. *Applied Sciences*, 12(21), p.11174. doi:https://doi.org/10.3390/app122111174.

Simoiu, C. (2020). Who Is Targeted by email-based Phishing and malware? Measuring Factors That Differentiate Risk. In: A. Zand and E. Bursztein, eds., ACM Internet Measurement Conference.

NIST (2019). *Cybersecurity Framework*. [online] National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework.

Ojoawo, E. (2023). *Phishing attacks: The phisherman, the phish, the bait and the hook | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-security/phishing-attacks-phisherman-phish-bait-and-hook.

Rai, M. (2019). A STUDY ON CYBER CRIMES, CYBER CRIMINALS AND MAJOR SECURITY BREACHES. International Research Journal of Engineering and Technology, [online] 6(7). Available at: https://www.irjet.net/archives/V6/i7/IRJET-V6I740.pdf.

Sweeney, B. (2016). *Cybersecurity Is Every Executive's Job*. [online] Harvard Business Review. Available at: https://enterprisersproject.com/sites/default/files/cybersecurity_is_every_executives_job.pdf [Accessed 10 Aug. 2023].

Tenable (2023). *CIS Control 13: Data Protection (CIS Controls Assessment Specification)*. [online] docs.tenable.com. Available at: https://docs.tenable.com/security-center/CIS-CAS/Content/PDF/CIS_CAS_Controls.pdf [Accessed 10 Aug. 2023].

Traversy, B. (2023). *MERN Crash Course (Part 1) - Backend API, Middleware, Database, JWT*. [online] www.traversymedia.com. Available at: https://www.traversymedia.com/blog/mern-crash-course-part-1 [Accessed 10 Aug. 2023].

Tripwire (2017). *Small Companies Overconfident about Their Security Posture, Finds Survey | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-

security/small-companies-overconfident-security-posture-finds-survey [Accessed 10 Aug. 2023].

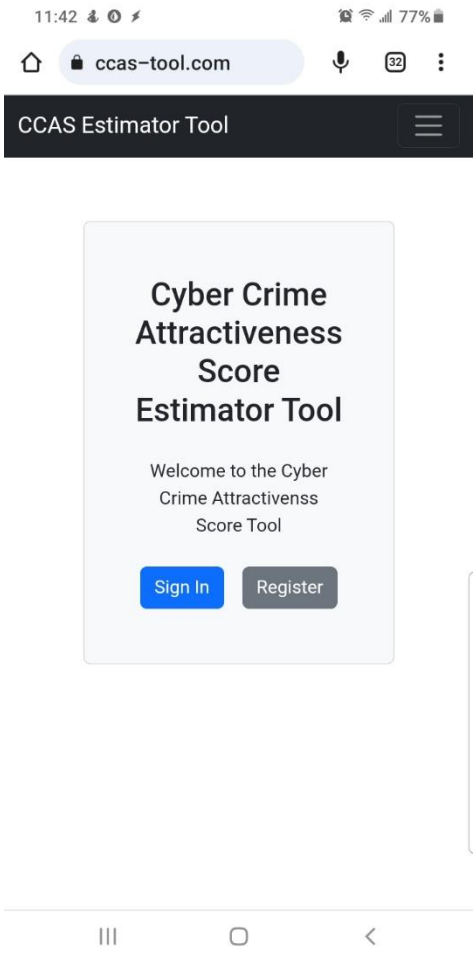
Tripwire (2023a). *Reviewing Remote Work Security: Best Practices | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-security/reviewing-remote-work-security-best-practices [Accessed 10 Aug. 2023].

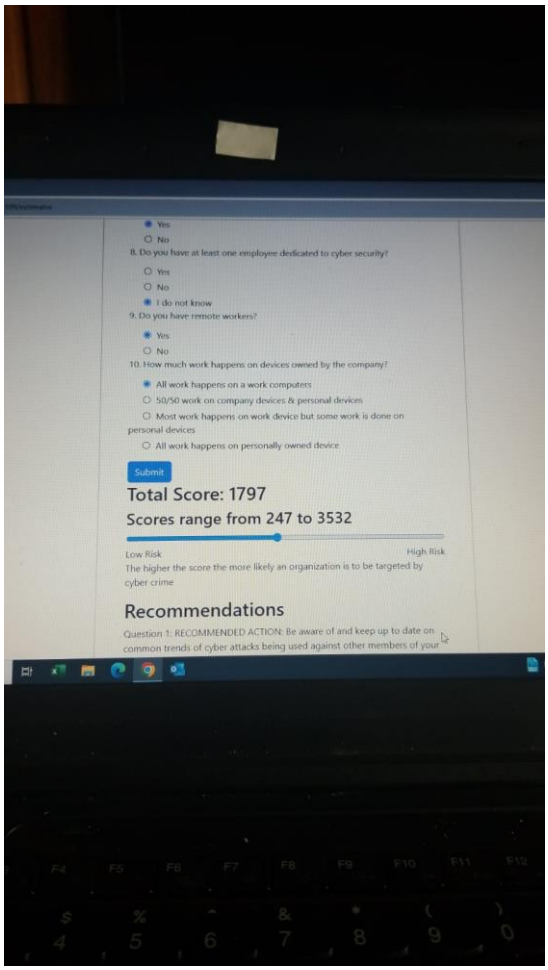
Tripwire (2023b). *Three Reasons Why Business Security Starts with Employee Education | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-security/reasons-why-business-security-starts-employee-education [Accessed 10 Aug. 2023].

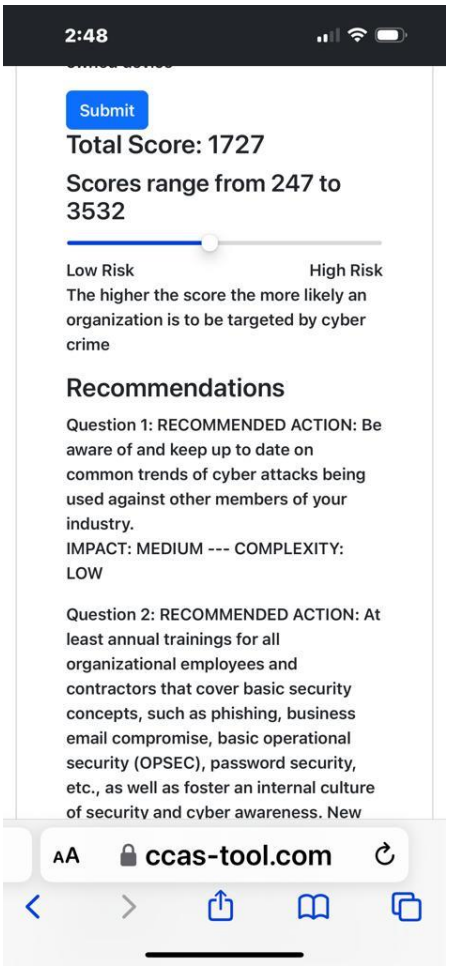
Verizon (2022). *Data Breach Investigation Report*. [online] *www.verizon.com*. Available at: https://www.verizon.com/business/resources/T11a/reports/dbir/2022-data-breach-investigations-reportdbir.pdf [Accessed 10 Aug. 2023].

Appendix

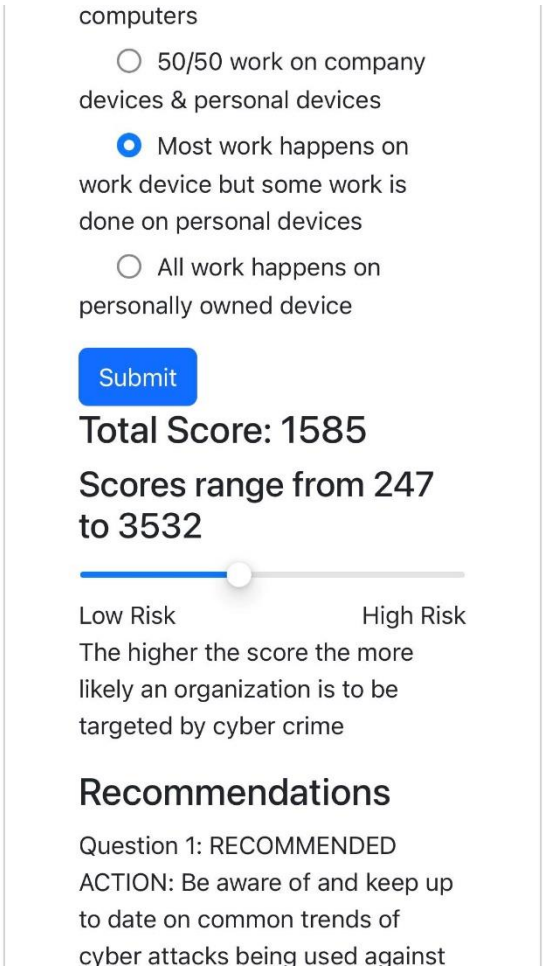
1. https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

2. 
11:42
77%
ccas-tool.com
32
CCAS Estimator Tool
Cyber Crime Attractiveness Score Estimator Tool
Welcome to the Cyber Crime Attractivenss Score Tool
Sign In
Register

3. 
Yes
No
8. Do you have at least one employee dedicated to cyber security?
Yes
No
I do not know
9. Do you have remote workers?
Yes
No
10. How much work happens on devices owned by the company?
All work happens on a work computers
50/50 work on company devices & personal devices
Most work happens on work device but some work is done on personal devices
All work happens on personally owned device
Submit
Total Score: 1797
Scores range from 247 to 3532
Low Risk
High Risk
The higher the score the more likely an organization is to be targeted by cyber crime
Recommendations
Question 1: RECOMMENDED ACTION: Be aware of and keep up to date on common trends of cyber attacks being used against other members of your

4. 
2:48
Submit
Total Score: 1727
Scores range from 247 to 3532
Low Risk
High Risk
The higher the score the more likely an organization is to be targeted by cyber crime
Recommendations
Question 1: RECOMMENDED ACTION: Be aware of and keep up to date on common trends of cyber attacks being used against other members of your industry.
IMPACT: MEDIUM --- COMPLEXITY: LOW
Question 2: RECOMMENDED ACTION: At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security (OPSEC), password security, etc., as well as foster an internal culture of security and cyber awareness. New
AA
ccas-tool.com

5.


computers
50/50 work on company devices & personal devices
Most work happens on work device but some work is done on personal devices
All work happens on personally owned device
Submit
Total Score: 1585
Scores range from 247 to 3532
Low Risk
High Risk
The higher the score the more likely an organization is to be targeted by cyber crime
Recommendations
Question 1: RECOMMENDED ACTION: Be aware of and keep up to date on common trends of cyber attacks being used against