Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool.

ZUHAYR AAMIR MIRZA, University of Twente, The Netherlands
SUPERVISOR: DR. ING. MOHAMMAD ELHAJJ, University of Twente, The Netherlands

Abstract: As the number of small and medium enterprises (SMEs) rises in the world, the amount of sensitive data used also increases, making them targets for cyberattacks. SMEs face a host of issues such as lack of resources, and poor cybersecurity talent, resulting in multiple vulnerabilities which increases overall risk. Cybersecurity risk assessment frameworks have been developed by multiple organisations such as the National Institute of Science and Technology (NIST) and the International Organization for Standardization (ISO), but they are complicated to understand, and challenging to implement. This research aimed to create an effective cybersecurity risk assessment framework specifically for SMEs, while considering their limitations. This was achieved by first identifying common threats and vulnerabilities and categorizing them according to their importance, and risk. Secondly, popular frameworks like the NIST CSF and ISO 27001/2 were analyzed for their proficiencies and deficiencies while identifying relevant areas for SMEs. Finally, novel techniques catered to SMEs were explored and incorporated to create an effective framework for SMEs. This framework was also developed in the form of a tool, providing an interactive and dynamic environment. The tool was effective and the framework is a promising start but requires more quantitative analysis.

Additional Key Words and Phrases: SMEs, cybersecurity risk assessment framework, NIST, ISO

1 Introduction

Over the past few years, the number of cyberattacks has skyrocketed, with around 62% of Australian small and medium enterprises (SMEs) being victims of cybercrimes [6]. SMEs are incredibly vulnerable due to several constraints. Many SMEs do not possess the financial capability to invest in cybersecurity, with their main focus being revenue. This limitation is complimented by the lack of cybersecurity talent available [13].

However, there are a number of cybersecurity frameworks that aim to provide a structure for firms to protect themselves from cyberthreats. Examples of such frameworks include the NIST Cybersecurity Framework, ISO27001/2, Essential Eight, and PCI-DSS. Each of these frameworks has advantages and disadvantages, but do not completely cater to SMEs, since they can be notoriously difficult to implement and understand. [1].

Due to this complexity, a large number of SMEs tend to ignore parts of the framework, and employ a 'fail-safe' approach, where they attempt to cover most bases to avoid critical errors [4]. Moreover, there are numerous threats to SMEs which can be categorized as physical, psychological, and technical [26]. It has been reported that 1 in 3 startups that are affected by a cyberattack, end up shutting down due to financial loss and the inability to recover [26]. This grim statistic reflects the need for a framework that can better protect SMEs while being easy to implement.

The research paper discusses some challenges with SMEs in the problem statement section by identifying research questions to guide the development of the framework and tool. A literature review was conducted to gather information about current vulnerabilities with SMEs, issues with established frameworks, and promising solutions. Further, the framework and corresponding tool are discussed with a clear focus on potential limitations and future work. An extension to the research has also been discussed with a proposed pilot assessment.

2 Problem Statement

This section provides a short description of the problems that SMEs are facing, along with an introduction to the research questions.

2.1 Problem Introduction

SMEs are incredibly important since they can represent 90% of companies in some regions, creating economic opportunities for many individuals [11]. A survey conducted by Heikkilä et al. (2016) discovered that only 40% of companies have an employee directly responsible for security issues, meaning that the majority of businesses are largely underequipped, increasing vulnerability. Mainstream cybersecurity frameworks have international recognition and are used by various large enterprises, but lack scalability for SMEs. Despite their large attack surfaces, large enterprises have the resources to better equip themselves with the necessary defenses [6]. Therefore, it is clear that the frameworks mostly cater to these larger enterprises.

The disparity in resources between small and large firms leads to a poorer comprehension of these frameworks, resulting in a lower motivation to properly implement good cybersecurity posture [32]. Cybersecurity posture can be defined as the strength of cybersecurity protocols for preventing, predicting, and handling attacks while they are happening, and their aftermath [7]. The frameworks largely provide ideas of good practices and structures that could be set in place to counter certain threats. Based on these threats, it is prudent to combine elements of established frameworks with promising ideas for adaptability.

2.2 Research Questions

Based on the problem statement defined in section 2.1, the main goal of this research paper is to answer the four research questions below.

(1) RQ1: How are SMEs susceptible to common cybersecurity threats such as malware, web-based attacks, and phishing?
(2) RQ2: How do existing cybersecurity frameworks such as NIST CSF, and ISO 27001/2 address the specific challenges and limitations encountered by SMES?

TScIT 41, July 5, 2024, Enschede, The Netherlands

(3) RQ3: What techniques or approaches can be implemented to tailor cybersecurity risk assessment methodologies, specifically for SMEs, considering their resource constraints and unique operating environments?
(4) RQ4: How can the effectiveness of the developed framework and tool be evaluated and validated in real-world SME environments?

3 Background

This section aims to provide an overview of the literature review exploring RQ1 and RQ2. This will provide knowledge to develop the framework, by considering specific vulnerabilities faced by SMEs, and examining the advantages and disadvantages of popular frameworks.

3.1 Common Threats and Vulnerabilities Faced By SMEs

The European Union Agency for Cybersecurity (ENISA) releases reports for threat landscapes in cybersecurity. Their most recent report in 2020 detailed the top 15 cybersecurity threats to businesses around the European Union and the globe. The top three threats discussed were malware, web-based attacks, and phishing [17]. These threats can be further placed into categories. Malware and web-based attacks represent a technical threat, through the use of software. Malware can represent any hardware or software that is intentionally placed into a system for a harmful purpose, such as stealing sensitive data [23]. Web-based attacks revolve around finding weaknesses and vulnerabilities in the web-applications that SMEs use like servers [29]. Phishing can be categorized as a psychological threat, where an attacker uses social engineering techniques to steal personal data through different means, commonly e-mail or SMS, while posing as a legitimate entity [22].

These three threats can have serious consequences for SMEs, since ENISA has also reported that the frequency of such attacks will rise over time [17]. Each of the threats also corresponds to common vulnerabilities that SMEs face, such as a lack of expertise in cybersecurity and poor cybersecurity posture. The technical threats are a direct result of having poor security throughout their system by failing to implement a framework. Phishing directly targets employees lacking proper training, and can cause data breaches through links, presenting a serious challenge [22]. Section 3.1.1 highlights one of the most important vulnerabilities for SMEs.

3.1.1 Employee Attitudes Robust security is essential for businesses, but is useless in the event of human error or apathy. Therefore, another threat to SMEs is the attitude of their employees and their work environment. Employee attitudes are important to understanding how cybersecure a business is. A study done by Pugnetti and Casián (2021) found that a majority of employees felt helpless when protecting themselves. They also felt that their company and assets were not important enough to be targeted. This approach automatically increases their vulnerability, since this mindset can lead to lax security measures. This idea indicates that individuals would rather leave security with security specialists, not realising that they also have a large role in protecting the attack surface of the company through their actions [25]. The feeling of helplessness is also a massive concern, since it decreases motivation towards training, and reduces engagement with security policies [25].

Recommendations from this study include raising awareness, empowering employees, and helping them understand how to recover lost information or reset systems [25]. These recommendations are crucial for the framework, since a firm can have a high degree of security, but can be susceptible due human error which is preventable. By improving the work environment and the attitudes of employees, they can collectively become better at maintaining a functional security level. Table 1 provides a general overview of the three threats and the corresponding vulnerabilities at SMEs. It is important to note that there are more threats than those mentioned in Table 1, and that many vulnerabilities overlap.

Attack	Common Types	SME Vulnerabilities
Malware	Ransomware. Adware. Spyware.	Lack of awareness. Lack of security professionals [10]. Cyberslacking [18].
Phishing	Deceptive Phishing [5]. Malware-based Phishing [5].	Lack of training. No warning systems for flagging [25]. No reporting mechanism or verification.
Web-based	Cross-site scripting (XSS). SQL Injection. Distributed Denial of Service (DDoS).	No input sanitization. Lack of firewalls. Poor coding practices.

Table 1. Overview of Threats and Vulnerabilities

3.2 Review of Popular Frameworks

Many cybersecurity frameworks have been credited with developing strong defenses for firms. However, Marican et al. (2023) conducted a study that researched multiple articles, and concluded that there was no framework that assessed the cybersecurity maturity level for startups. Evidently, this is damaging for startups, since they cannot verify their cybersecurity posture, opening themselves up to vulnerabilities [19]. However, it is still important to discuss frameworks and understand their limitations for SMEs.

The NIST CSF is a voluntary framework built upon industry standards and government information, providing five main functions namely, identify, protect, detect, respond, and recover [2]. Each of these functions corresponds to processes that businesses take to protect themselves, such as risk assessment and response planning [6].

Another commonly used framework is the ISO 27001/2, which provides specifications for firms to create an Information Security Management System (ISMS) to protect their information [12]. ISO 27002 extends the previous framework by adding more details for security controls [6]. This makes it a technical and detailed framework, but one which can clearly help establish appropriate defenses. Table 2 shows an overview of the frameworks with their advantages and disadvantages for SMEs.

3.3 Key Findings

The literature review has provided a foundation by answering the first two research questions. The vulnerabilities that SMEs possess

Framework	Advantages	Disadvantages
NIST CSF	Flexible. Common terminology. Reduces confusion [6].	55 page manual. Relatively new terminology for SMEs. Forces businesses to rate themselves (no clear standards) [3].
ISO 27001/2	Robust. Creation of an ISMS. Effective security measures for structure [6].	Extremely technical. Large knowledge gap between technicality and implementation. Complicated process for adoption [9].

Table 2. Overview of Frameworks

for specific attacks have been explored and identified. It is evident that a lack of structure, training, and focus lead to vulnerabilities. Phishing is commonly used as a precursor for these attacks. In terms of frameworks, the strengths and weaknesses of both the NIST CSF and IS027001/2 have also been explored, mentioning that despite their detailed structure, their complexity can pose challenges for SMEs.

4 Related Work

This section specifically covers academic research that concerns the design of a new cybersecurity risk assessment framework for SMEs. These solutions take into account the resource constraints faced by SMEs. It is crucial to explore solutions that have been developed, to combine their advantages and build upon their limitations.

4.1 Promising Solutions for SMEs

Firstly, a solution that extends the NIST CSF was proposed by Benz and Chatterjee (2020), where a cybersecurity evaluation tool (CET) was created, which draws upon 35 standards in the NIST CSF. The CET uses current academic literature and industry experience from experts to provide a platform for organizations to rate themselves, after which they receive receive a recommendation for a certain standard with costs and benefits. [3].

Another solution proposed by van Haastrecht et al. (2021) uses employee motivation through self-determination theory (SDT) to create a threat-based risk assessment framework, in an app. A threat-based risk assessment framework identifies potential threats for systems, while making a plan to counter them. It focuses on identifying areas with the highest risk in terms of potential impact, and consequently developing a solution. SDT is used to motivate individuals through an interface displaying potential threats, to implement defensive strategies [32]. With this approach, employees can be more proactive with security, trying to be more secure. A data model was used to correctly evaluate threats and provide recommendations with the GEIGER app that was developed by a European Union funded Horizon group [32]. However, the application is a prototype and requires further testing to be used by SMEs.

Pawar and Palivela (2022) explore the use of Least Cybersecurity Controls Implementation (LCCI), a framework using the Confidentiality, Authentication, and Integrity (CIA) triad to help businesses in identifying their mission critical assets (MCAs), while simultaneously providing recommendations. The framework creates different security levels based on which principles of the CIA triad have been implemented. For example, Level 1 has been reached if only confidentiality has been integrated, and reaching Level 3 means that all three principles of the CIA triad have been implemented. By condensing the idea of security into three easily definable terms, security can be simplified for SMEs. A useful part of the framework is that it is specifically built for SMEs, therefore, there are different levels of basic security that SMEs can implement, according to their resource constraints [24]. However, it is a relatively new framework and needs quantitative feedback to determine whether it can be used by SMEs.

Finally, Carías et al. (2020) propose using a more holistic approach to securing SMEs, through the lens of a cyber-resilience framework. Cyber-resilience moves away from the traditional cybersecurity aspect of 'fail-safe' methodologies where all errors are avoided to protect the system, and instead moves towards 'safe-fail' methodologies to maintain business systems, regardless of attacks [4]. Most SMEs use the 'fail-safe' methodology since cyber-resilience requires more investment, therefore making them more reactive which can lead to issues when facing an unknown attack. However, this is a relatively new concept, and the framework has only been evaluated in a qualitative manner, thus suggesting a need for quantitative analysis.

4.2 Techniques for the Framework

Building upon these promising solutions can aid the development of a cybersecurity risk methodology that is tailored to SME resource constraints. For example, the solution proposed by van Haastrecht et al. (2021) directly considers these contraints, suggesting that using threat-based risk assessment in conjunction with self-determination will motivate employees to research threats on their own, and work harder to protect their systems. The LCCI framework developed by Pawar and Palivela (2022) creates a system of three levels of security that SMEs can implement based on their resources. The levels also have descriptors verify whether the security requirement for a certain level has been met.

Therefore, after considering these solutions for RQ3, the framework described in this research utilises a combination of SDT, threat-based risk assessment, and LCCI. This results in a detailed and specific framework for SMEs, which can be used to target specific threats, and create a reasonable cybersecurity posture. This can mitigate certain threats, preventing unnecessary consequences.

5 Framework

This section of the research covers all aspects of the framework that was constructed on the basis of the literature review about SME vulnerabilities, established frameworks, and promising solutions. It provides a brief overview of the framework, later diving into each section and explaining their rationale. Figure 1 shows the start of the framework.

1 Framework Overview.

This is a cybersecurity risk assessment framework developed and designed for SMEs. It combines various promising techniques such as threat-based risk assessment and LCCI to create solutions that are both convenient and understandable for SMEs. It covers three common threats: malware, web-based attacks, and phishing, while providing different solutions based on the structure of the SME. It also provides a path for creating a basic cybersecurity structure so that a business can either modify their current plan or create a strategy.

2 How to Use This Framework?

The framework is divided into different sections to properly understand and apply the principles mentioned.

1. **Basic Cybersecurity Tips**: All businesses should implement basic cybersecurity tips regardless of their policy. These tips should also extend beyond the workplace and be continually provided to employees to make them daily rituals.
2. **Mapping Business Systems**: Companies should explore their business and map out their systems to fully understand their scope and potential vulnerabilities.
3. **Identifying Risks and Solutions**: For each system, identify potential risks and areas of concern. Once identified, explore solutions to detect and prevent potential threats. The framework provides solutions with different levels of security, which businesses can implement based on their resources and convenience.

3 Basic Cybersecurity Posture

3.1 Basic Cybersecurity Tips and Employee Training

This section covers basic cybersecurity principles that should be daily rituals in the business and part of current and future employee training.

Fig. 1. Start of Developed Framework.

5.1 Overview

This custom framework for SMEs combines aspects from the promising solutions such as threat-based risk assessment, LCCI, and SDT to create a framework for SMEs. The framework is organized in such a way to first provide general advice to establish a decent cybersecurity posture, based on advice from established frameworks and current research. These are basic security principles that all firms should generally follow.

Secondly, the framework aims to aid SMEs to understand their business on multiple levels, such as identifying their assets, potential vulnerabilities, administrative processes, and examining the employee work environment. Moreover, the framework offers tier-based solutions for phishing, malware, and web-based attacks. The legal section offers advice to firms about the General Data Protection Regulation (GDPR) and cyber-insurance. Finally, the support section discusses the opportunity for firms to collaborate with each other for common solutions. For the three threats, levels of security will be established, which can be applied by SMEs, depending on their resource limitations. This is a combination of both threat-based risk assessment and LCCI, incorporating two promising solutions.

Threat-based risk assessment allows companies to create specific plans for the potential threats in their business. By first identifying the relevant threats/risks, they can take steps to mitigate and prevent them from occurring. LCCI is also important by having different levels of security that can be implemented by SMEs. Firms first identify their MCAs after which a solution that properly fits within their parameters and implementation is chosen. These levels also make it possible for SMEs to scale up their security structure as they grow. Figure 2 showcases interactions between the components of the framework.

5.2 Fundamentals of Information Security

This section of the framework offers the most basic tips for companies to adhere to. SMEs should implement these tips first, ensuring a basic structure, before implementing advanced layers. These should

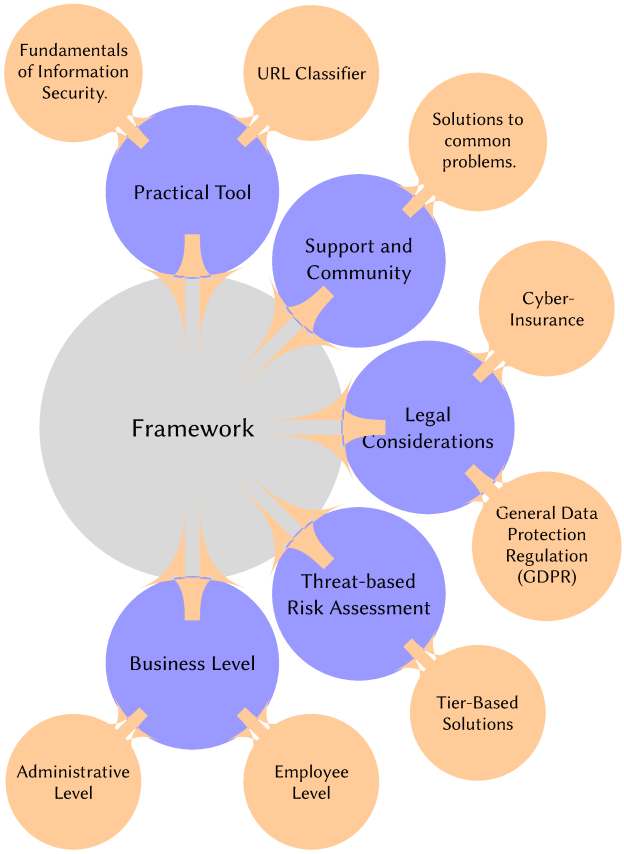

Fig. 2. Key components of the framework.

also be provided to employees for a secure lifestyle. Examples of these tips include maintaining strong passwords, regularly backing up data, and the use of virtual private networks (VPNs).

With these tips, SMEs can protect their assets, and reduce preventable incidents. It was found that 43% of individuals are using the same or slightly modified password across different accounts, representing a security lapse [31]. A random password generator which creates robust passwords can mitigate this lapse [16]. For example, when combining strong passwords with multi-factor authentication (MFA), 99% of attacks regarding compromised accounts can be prevented [30]. This highlights how a simple security technique can greatly elevate the cybersecurity safety level of employees at a firm.

The inclusion of the CIA triad in the framework is important so that SMEs can understand its fundamental principles. Confidentiality will ensure that information is only accessible to those who are authorized access [21]. Integrity will ensure that information and data remain consistent over their lifetime, meaning that unauthorized changes will not be made [21]. Finally, availability will ensure that information must remain accessible to users with proper authorization [21]. If this triad of principles is incorporated into a cybersecurity policy, it will improve the security of the systems in the business. By deeply understanding these three principles,

companies can evaluate their systems by verifying whether each one is upheld.

5.3 Cybersecurity Levels

The framework has been divided into different levels which have been described below.

5.3.1 Business Level This level focuses on key business activities and MCAs. It provides steps on identifying the business as a whole while recognising which systems are being used. Mapping out the entire business and identifying key goals is a key part of understanding which systems may be more vulnerable to certain threats. This will allow for a focused cybersecurity posture.

5.3.2 Administrative Level This level focuses on understanding the management process. This involves creating an incident response planning and implementing Role-Based Access Controls, which refers to the idea of assigning permissions to employees based on their roles in the company [27]. Finally, AAA principles such as authentication, authorization, and accounting should be used while maintaining logs for auditing [20].

5.3.3 Employee Level This level focuses on evaluating the work environment and cybersecurity training for employees. It also seeks to provide information about employee best practices and how to support them through SDT and intrinsic motivation. By continually preparing employees, the probability of human error leading to an attack can be reduced.

5.4 Threat Classification

This level firstly provides information about phishing, malware, and web-based attacks. Symptoms of these attacks and their consequences for firms are also discussed, so that firms do not underestimate their impact. For each attack, the common systems they target, and the common ways that they enter these systems have also been discussed. Finally, tier-based solutions are offered based on different resource requirements, with each solution building upon the previous one.

6 Tool

This section provides an overview of the tool that was developed with the framework, while also diving into design choices, limitations, and future extensions.

6.1 Overview

The tool represents the framework digitally in the form of a web-based application, to improve interactivity and accessibility for users. The tool contains a machine-learning (ML) model which can be used to classify URLs. Users can input links, and the application will classify them using the model Implementing a threat detection model is important since phishing has become increasingly complicated to detect for employees. Since phishing can be a precursor to malware and web-based attacks, protection is vital. Employees can use a practical tool to check any links that they have received, thus providing another layer of security.

6.2 Methodology to Develop Model.

6.2.1 Identifying the goal: Before choosing a model and extraction features, the first step is to set a goal. The threat detection of URLs is based upon their classification into different labels. For this model, the four classifications are benign, malware, phishing, and defacement. Benign URLs are neutral and the most common. Malware URLs usually contain malicious code that will be executed upon interaction. Phishing URLs are deceptive and will redirect users to fake websites. Finally, defacement URLs are links to websites that have been altered, with the content posing as a legitimate entity.

6.2.2 Choosing a model: The task is to classify URLs, thus requiring a model that can support this. A number of different models were considered and tested such as Neural Networks, Support Vector Machines and XGBoost, but the best fit was the Random Forest Classifier. It is a type of supervised learning algorithm that builds various decision trees, later combining them to create a more accurate prediction [8]. Advantages of this model are that it does not overfit with trees and is versatile. However, this increases computation time and does not describe relationships within data well [8].

6.3 Data Selection, Sampling, and Distribution.

The dataset for URLs was chosen from Kaggle [28]. It contained URLs labelled benign, malware, phishing, and defacement. Each of these labels was provided a number so that the model could learn with them, and the extracted features. Since the dataset was quite large, data was sampled randomly using Python. For this model, the data was sampled equally with a total of 120,000 entries, 30,000 for each classification. The limitations of this approach have also been discussed and justified in Section 6.5. Figure 3 shows the distribution of labels in the original dataset.

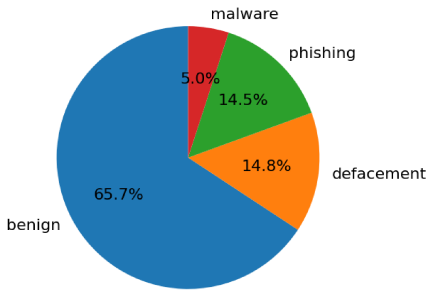

Fig. 3. Distribution of Original Dataset.

6.4 Extracted Features

The ML model extracts features from the dataset to create patterns and relationships between them. The model learns from the features to classify the URLs into their categories. Below, the features and their relevance to the model have been described.

(1) URL Length: Extremely long and short URLs can be a sign of phishing or concealing information.
(2) Number of digits: A URL with a large number of digits can be a sign of redirection or malicious intent.
(3) Number of special characters: A large number of special characters can be an indication of malicious intent.
(4) Has IP address: The presence of an IP address usually means redirection to an unsecure location.
(5) Has HTTPS: If a website contains HTTPs, it has a secure and encrypted connection.
(6) Number of periods: URLs with many dots mean there are multiple subdomains, a common trick to look legitimate.
(7) Domain Length: Very long or short domain lengths can potentially be an indicator of a malicious website.
(8) Port Number: It is unusual for a URL to contain a port number.
(9) Number of Subdomains: A large number of subdomains can be an indicator of a malicious website.
(10) Has Redirection: Redirection to another website, can be an attempt to conceal malicious intent.
(11) Path Length: Varying path lengths can be an indicator of phishing or malware.

6.5 Limitations with Dataset

As seen in Figure 3, the original dataset retrieved from Kaggle has a large imbalance, leaning towards mainly benign URLs [28]. This reflects the real world, where benign URLs are much more common. However, for a ML model, this means that performance for detecting malicious URLs will be poor, since they are a minority class, potentially leading to misclassification. This is a result of the model being biased towards the majority dataset, in this case, benign URLs.

A solution to this problem is to balance the dataset by sampling equal amounts of data from the original dataset. The advantage of this approach is that the model will become better at generally classifying all classes equally, instead of being biased towards the majority class. However, the disadvantage of this approach is the lack of realism. The model could classify benign URLs as malicious, which is not realistic. Nevertheless, it is better to be on the safe side. It is more favourable for SMEs to misclassify a benign URL as a malicious one, rather than the other way around. One approach simply has more tangible consequences for the business.

7 Results

This section of the report covers both qualitative and quantitative results for the framework and the tool. It is important to note that most research done for frameworks is usually qualitative, meaning that their actual effectiveness is unknown. To properly assess a framework, quantitative assessments need to be done to verify its impact on firms. Therefore, a structured pilot assessment proposal is explored at the end of the section.

7.1 URL Classifier

The URL classifier was developed using the ML model, and trained on the features mentioned above. The classification matrix in Figure 4 shows the precision, recall, and F1-score for each of the labels in the dataset. Precision measures how many positive predictions are correct [14]. Recall measures how many positive predictions made are actually correct [14]. The F1 score is essentially a mean of both precision and recall [14]. Based on the extracted features, the accuracy of the model was 98%, meaning that it was very accurate in classifying URLs. Figure 5 shows how this classifier can be used by employees at the firm to check links. Once the employee places the link, and clicks on classify, the pre-trained model makes a prediction and returns information about the link.

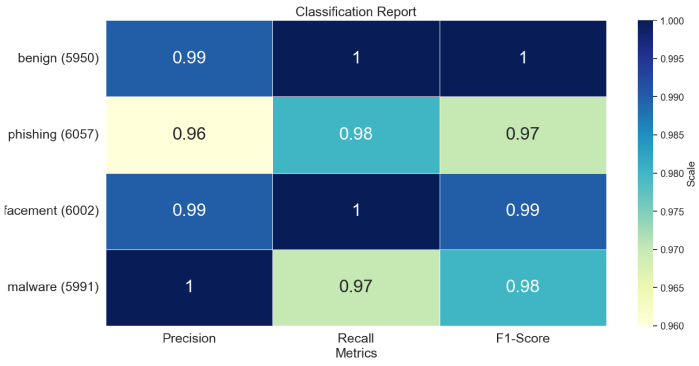

Fig. 4. Classification Report

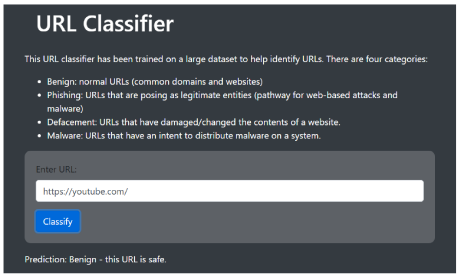

Fig. 5. Developed URL Classifier.

7.2 SWOT Analysis

It is always important to critically analyse frameworks, to properly understand their strengths, weaknesses, and opportunities for improvement. This can be done in the form of a SWOT analysis. A SWOT (strengths, weaknesses, opportunities, and threats) analysis is an assessment framework that can be used to evaluate the key parts of an initiative or project [15]. It is useful to conduct such an analysis for the framework to find areas where it excels and those where it suffers. Table 3 showcases a SWOT analysis of the framework.

7.3 Expert Feedback

Upon consultation with an individual with experience in the cybersecurity field, the following evaluation of the framework was made.

Strengths	Weaknesses
• Modular structure. • Tier-based security solutions based on resources. • Focus on practical employee training. • Focus on common threats. • Encourages creation of support network for SMEs. • Offers legal information.	• Untested with SMEs about utility. • Focused on three common threats. • Dependence on compliant and consistent employees. • Still technical for readers without background knowledge. • Higher tier solutions can be resource intensive.
Opportunities	**Threats**
• Large market of SMEs for potential use. • Can be scalable for businesses. • Tool offers a practical use of the framework. • Integration with other tools opens more pathways.	• Continuous evolution of threat landscape. • Need for periodic review and updates to prevent obsolescence. • Competition with established frameworks. • SMEs may not be comfortable shifting frameworks/policies.

Table 3. SWOT Analysis

The rationale behind the framework was discussed, emphasizing the need for specific techniques for SMEs.

7.3.1 Advantages The detailed inclusion of the fundamentals of information security and focus on employee training were positives. The tier-based system for threats was also highlighted as a positive. The structure of the framework with interconnected sections and the use of a practical tool were also positives, since it could be used by employees throughout a business.

7.3.2 Disadvantages However, as with any novel framework, clear disadvantages were also noted. Limiting the framework to three threats provides a narrow focus, since businesses can face threats outside this domain, leading them to be potentially unprepared. The need for quantitative analysis further emphasized the need for a pilot assessment with SMEs. Finally, the dependence on employee compliance and training can be a pitfall without the proper procedures to facilitate SDT and intrinsic motivation.

7.3.3 Recommendations Properly motivating employees to be cybersecure can be achieved through incentivisation using quizzes or gameifying cybersecurity training. By motivating employees with a reward, they may attain more knowledge and make an extra effort in learning principles from the framework.

7.4 Usability Testing

To gain a better understanding of the framework, usability testing was performed. Participants were asked to read the framework and then review its different traits to measure effectiveness. The framework was reviewed for four different traits, which were clarity, scope, utility, and practicality. Each of these were defined in the scope of SMEs. Clarity is a measure of how easy it was to go through the framework and understand the technical language. Scope is a measure of how the framework covered essential aspects of cybersecurity. Utility is a measure of how useful the framework was in terms of tips and solutions. Finally, practicality was a measure of how achievable the processes and solutions were in the framework; did they consider resource constraints? Figure 6 shows the distribution of responses. The closer a number is to 5, the better the score for each aspect. The closer a number is to 0, the worse the score for the aspect.

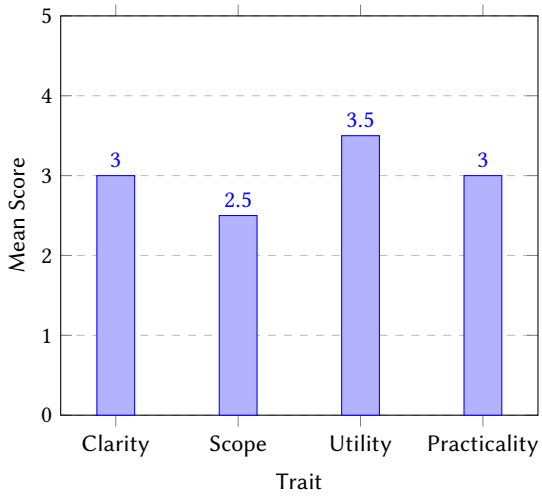

Fig. 6. Mean Scores for Framework Traits.

7.5 Proposed Pilot Assessment

The following section discusses a proposed experiment for a pilot assessment of the framework. The pilot assessment would take place over a duration of between 6-8 months in which a number of SMEs from various industries would be selected. It is vital that they are inherently different, in terms of size, focus, and number of employees, allowing for a diverse dataset.

7.5.1 Setup: During this phase, SMEs selected for the assessment would be provided the framework and documentation to familiarize themselves with it. In this way, they have a foundation upon which they can implement the framework, while simultaneously creating a plan of action for execution. Their initial setup will also be documented.

7.5.2 Implementation and Monitoring: During this phase, the SMEs will implement the framework according to the plan that they made, while monitoring their process and collecting data. During this phase, incidents related to cybersecurity will also be observed and correlated to parts of the framework. Data will also be gathered using a combination of qualitative and quantitative techniques such as surveys, interviews, and reports to gather information about the

effectiveness of the framework.

7.5.3 Evaluation: During this phase, the data gathered will be evaluated on different metrics such as security incidents faced by the SMEs, employee awareness on cybersecurity, and the SMEs feedback on the framework itself. At the end of this phase, the framework's effectiveness in a real-world situation can be evaluated, and can be improved based on the feedback received.

8 Discussion

8.1 Framework

The framework was developed by combining promising solutions from academic literature with basic structures employed by established frameworks. Nevertheless, it was important to verify it's effectiveness objectively to see if it possesses valuable information for SMEs. The SWOT analysis shows that the structure of the framework provides multiple advantages, since it focuses on the fundamentals of cybersecurity, and emphasizing employee training as a big part. However, it does have weaknesses such as a dependence on employee training, a narrow threat focus, and technical language associated with cybersecurity. There is a need for periodic review as the threat landscape is ever evolving, so that the framework is not rendered obsolete.

The usability report also indicated that although the framework has practical and useful information, participants found the technical language and lack of depth challenging. The lack of depth was due to the focus on three threats and the need for more descriptions. However, these results are qualitative, and quantitative analysis could provide a more tangible interpretation of the effectiveness of the framework. Therefore, the proposed pilot assessment can be a good method to quantitatively measure its effectiveness.

8.2 Tool

The tool was developed using Flask with a pre-trained model on the back-end. When a user attempts to classify a URL, a request is made to the back-end to make a prediction on the URL, after which it is displayed on the front-end. The model had an accuracy of 98% in properly classifying URLs into different categories. Figure 4 shows that the model has a reliable performance across different categories, meaning that it can be used by SMEs.

However, SMEs will have to adjust the model and its dataset depending on the URLs they encounter. For example, this model will have difficulty in recognising the top-level domains of some countries because of the sampled dataset. This means that the model will have to be adjusted based the data used by the SME. The tool has also focused on combating phishing, which is not the only threat that is faced by SMEs. The reason to focus on phishing is that it is a precursor to the other two attacks, and reducing the probability of human error leading to an attack can be a good approach to improving security.

9 Limitations and Future Work

9.1 Limitations

Firstly, the framework focused on SMEs and is not completely applicable to larger enterprises, which have a larger attack surface. Solution scalability may be an issue, but the information should not be disregarded. Companies can still verify their existing cybersecurity structure.

Secondly, this framework focuses on the top three threats listed by ENISA, which were malware, web-based attacks, and phishing [17]. However, this list contained 15 threats, meaning that the framework can be expanded to include these threats. However, this can lead to the problem of high complexity. An issue with the NIST CSF and ISO 27001/2 was their high technical complexity, leading to a lack of understanding and motivation. Therefore, it is necessary to ensure the framework maintains the same level of simplicity.

This research also focused on two frameworks, the NIST CSF and ISO 27001/2. However, with the large number of frameworks available which may possess better techniques for certain threats, emphasizing a need for periodic review.

9.2 Future Work

This research is highly valuable for SMEs since it can aid them in creating appropriate defenses against cyber-attacks. However, the limitations mentioned above can be expanded upon.

Future work can be done to develop more quantitative feedback for the framework and the tool. The main issue with developing solutions for SMEs is that they are mainly qualitative without a metric of effectiveness. Most of these solutions have been tested qualitatively through user testing and expert testimonials. Quantitative feedback is yet to be implemented, but needed to identify whether there is a positive or negative effect. This is why a proposed pilot assessment was discussed. The tool could have more checklists to improve its customization and more practicality such as a passport strength checker and IP assistance.

10 Conclusion

This research examined the vulnerabilities associated with SMEs, and how popular frameworks like the NIST CSF and ISO 27001/2 fail to assist them. Vulnerabilities for phishing, malware, and web-based attacks were explored and identified. Based on these weaknesses, a specialized cybersecurity risk assessment framework was created along with a practical tool for SMEs utilization. This framework was created using promising solutions like SDT and LCCI, with an additional focus on employee training. The effectiveness of this framework and tool can further be analyzed through the proposed pilot assessment.

11 Acknowledgements

The author would like to thank Dr. Ing. Mohammad Elhajj for their supervision and guidance throughout the research project.

A AI Statement

During the preparation of this work, the author used Chat GPT in order to debug the code of the machine learning models and

for adjustments to figures and tables in the Overleaf environment. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the work.

References

[1] Khalifa AL-Dosari and Noora Fetais. 2023. Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics* 12, 17 (2023). https://doi.org/10.3390/electronics12173629

[2] Matthew Barrett. 2018. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

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

[4] Juan Francisco Carías, Marcos R. S. Borges, Leire Labaka, Saioa Arrizabalaga, and Josune Hernantes. 2020. Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access* 8 (2020), 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063

[5] Minal Chawla and Siddarth Singh Chouhan. 2014. A survey of phishing attack techniques. *International Journal of Computer Applications* 93, 3 (2014).

[6] Alladean Chidukwani, Sebastian Zander, and Polychronis Koutsakis. 2022. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access* 10 (2022), 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

[7] Stones Chindipha and Barry Irwin. 2023. *Evaluation of the Effectiveness of Small Aperture Network Telescopes as IBR Data Sources*. Ph. D. Dissertation. https://doi.org/10.13140/RG.2.2.29561.03686

[8] Niklas Donges. 2024. Random Forest: A Complete Guide for Machine Learning. https://builtin.com/data-science/random-forest-algorithm.

[9] Daniel Ganji, Christos Kalloniatis, Haralambos Mouratidis, and Saeed Malekshahi Gheytassi. 2019. Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review. *International Journal on Advances in Software* 12, 3,4 (2019), 228–238.

[10] Marjo Heikkilä, Anita Rättyä, Sakari Pieskä, and Joni Jämsä. 2016. Security challenges in small- and medium-sized manufacturing enterprises. In *2016 International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS)*. 25–30. https://doi.org/10.1109/SIMS.2016.7802895

[11] Md. Aminul Islam, Mohammad Aktaruzzaman Khan, Abu Zafar Muhammad Obaidullah, and M.Syed Alam. 2011. Effect of Entrepreneur and Firm Characteristics on the Business Success of Small and Medium Enterprises (SMEs) in Bangladesh. *International Journal of Business and Management* 6, 3 (2011), 289–299. https://doi.org/10.5539/ijbm.v6n3p289

[12] ISO. 2022. ISO/IEC 27001:2022. https://www.iso.org/standard/27001

[13] Hamid Jahankhani, Lakshmi N. K. Meda, and Mehrdad Samadi. 2022. *Cybersecurity Challenges in Small and Medium Enterprise (SMEs)*. Springer International Publishing, Cham, 1–19. https://doi.org/10.1007/978-3-030-98225-6_1

[14] Teemu Kanstrén. 2020. A Look at Precision, Recall, and F1-Score — towardsdatascience.com. https://towardsdatascience.com/a-look-at-precision-recall-and-f1-score-36b5fd0dd3ec.

[15] Will Kenton. 2024. How To Perform a SWOT Analysis — investopedia.com. https://www.investopedia.com/terms/s/swot.asp.

[16] Oleksandr Kubariev, Olena Piatykop, Olha Pronina, and Tetiana Levytska. 2023. The Research on Methods for Generating Random Passwords. In *2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*. 63–66. https://doi.org/10.1109/UkrMiCo61577.2023.10380416

[17] Marco Lourenco and Louis Marinos. 2020. ENISA Threat Landscape 2019/2020 - The year in review. (10 2020), 1–20. https://doi.org/10.2824/552242

[18] Ariel Luna, Yair Levy, Gregory Simco, and Wei Li. 2022. Proposed Empirical Assessment of Remote Workers' Cyberslacking and Computer Security Posture to Assess Organizational Cybersecurity Risks. In *2022 IEEE High Performance Extreme Computing Conference (HPEC)*. 1–2. https://doi.org/10.1109/HPEC55821.2022.9926394

[19] Mohamed Noordin Yusuff Marican, Shukor Abd Razak, Ali Selamat, and Siti Hajar Othman. 2023. Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access* 11 (2023), 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

[20] Samuel Moses and Dale Rowe. 2016. Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques. *International Journal for Information Security Research* 6 (06 2016), 667–676. https://doi.org/10.20533/ijisr.2042.4639.2016.0077

[21] Dietmar P. F. Möller and Hamid Vakilzadian. 2023. Cybersecurity Awareness Training: A Use Case Model. In *2023 IEEE International Conference on Electro Information Technology (eIT)*. 242–247. https://doi.org/10.1109/eIT57321.2023.10187349

[22] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri. 2017. An Introduction to Information Security. , 101 pages. https://doi.org/10.6028/NIST.SP.800-12r1

[23] Committee on National Security. 2022. Committee on National Security Systems (CNSS) Glossary. , 170 pages. https://www.cnss.gov/CNSS/openDoc

[24] Shekhar Pawar and Dr. Hemant Palivela. 2022. LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights* 2, 1 (2022), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

[25] Carlo Pugnetti and Carlos Casián. 2021. Cyber risks and Swiss SMEs: an investigation of employee attitudes and behavioral vulnerabilities. *ZHAW Digital Collection* (2021).

[26] Binita Saha and Zahid Anwar. 2024. A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. *Journal of Information Security* 15 (2024), 24–39. https://doi.org/10.4236/jis.2024.151003

[27] Ravi S. Sandhu. 1998. Role-based Access Control11Portions of this chapter have been published earlier in Sandhu et al. (1996), Sandhu (1996), Sandhu and Bhamidipati (1997), Sandhu et al. (1997) and Sandhu and Feinstein (1994). Advances in Computers, Vol. 46. Elsevier, 237–286. https://doi.org/10.1016/S0065-2458(08)60206-5

[28] Manu Siddhartha. 2021. Malicious URLs dataset — kaggle.com. https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset.

[29] Ankit Singh, Aditi Sharma, Nikhil Sharma, Ila Kaushik, and Bharat Bhushan. 2019. Taxonomy of Attacks on Web Based Applications. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Vol. 1. 1231–1235. https://doi.org/10.1109/ICICICT46008.2019.8993264

[30] Enpass Team. 2023. Why Are Strong Passwords Still Crucial Even with MFA Enabled? - Enpass — enpass.io. https://www.enpass.io/blog/security/strong-passwords-still-crucial-with-mfa-enabled/.

[31] Pieris Tsokkis and Eliana Stavrou. 2018. A password generator tool to increase users' awareness on bad password construction strategies. In *2018 International Symposium on Networks, Computers and Communications (ISNCC)*. 1–5. https://doi.org/10.1109/ISNCC.2018.8531061

[32] Max van Haastrecht, Injy Sarhan, Alireza Shojaifar, Louis Baumgartner, Wissam Mallouli, and Marco Spruit. 2021. A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES '21)*. Association for Computing Machinery, New York, NY, USA, Article 158, 12 pages. https://doi.org/10.1145/3465481.3469199