University of Essex

Online

MSc Computing Project Research Proposal and Ethical Approval Form

Student Details

Student name	Etkin Getir
Proposed title of research	Development of a threat modelling framework and a web-based threat modelling tool for micro businesses
Supervisors	Douglas Millward Stefania Paladini

Section 1 Research Proposal

1.1. Research Summary

1.1.1. Background

1.1.1.1. Definition of “micro business”

Micro businesses are a subset of small and medium-sized enterprises (SMEs). There are several definitions of micro business. While the U.S. Small Business Administration informally defines a micro business as having fewer than 10 employees (Office of Advocacy, 2017), the European Commission's (EC) definition is more precise: The EC defines micro businesses as enterprises employing fewer than 10 persons and having a turnover of less than EUR 2 million (European Commission, 2020). In the UK, on the other hand, businesses with 10 or fewer employees and a turnover not exceeding £632,000 are classified as 'micro' (UK Government, N.D.).

There seems to be a general consensus on the number of employees, but each institution has its own threshold for what constitutes a micro business. As it is less restrictive, and because the sample is selected not exclusively from the UK but from around the world, the EC definition (less than 10 employees with a turnover of less than 2 million euros) is used for this study.

1.1.1.2. Challenges unique to micro businesses

Two challenges are immediately apparent from the above definition:

First and foremost, micro businesses are understaffed, so it is usually not possible to designate an employee to oversee the cybersecurity of a business. In fact, most micro businesses are sole traders. According to the UK Office for National Statistics (Office for National Statistics, 2021), as of 2021, the total number of micro businesses in the country is approximately 2.5 million, with 4.9 million employees. The number of employees per enterprise was therefore 1.96. This suggests that it is not possible to handle cybersecurity professionally in micro businesses.

Secondly, because these businesses are financially constrained, it is not realistic to expect them to invest in cybersecurity. Therefore, it is unlikely that they would hire a cybersecurity professional to model the threats to their business or transfer the risk with the help of third parties, the latter also partly due to the lack of cybersecurity knowledge of small business stakeholders.

1.1.1.3. The impact of micro businesses and the rationale of the study

It should be noted that the impact of micro businesses on the economy is not small at all. In 2022, 95% of all businesses in the UK were micro businesses. These businesses were also responsible for 19% of total turnover and 32% of total employment in the country (Hutton, 2022). Similarly, in the EU, 94.1% of all businesses are micro businesses, generating 16.6% of total turnover and employing 30.1% of the total workforce (Eurostat, 2023). These statistics indicate that the importance of these enterprises should not be underestimated.

However, despite this, there are no specific studies that focus on how cybersecurity, and in particular threat modelling, is handled in micro businesses. This study aims to fill this gap and go further by proposing a non-technical threat modelling framework and an easy-to-use threat modelling tool that can be used by these organisations.

The project falls under the Risk Management & Governance Knowledge Area of CyBOK 1.1 (Burnap, 2021).

1.1.2. Research Question

Can relevant aspects of existing threat modelling frameworks can be incorporated into a non-technical framework so that micro businesses owners can model the cybersecurity threats they face in the absence of cybersecurity expertise and knowledge?

1.1.3. Aim

Design a non-technical threat modelling framework for micro businesses and a web-based threat modelling tool based on this framework.

1.1.4. Objectives

- Conduct a literature review to explore the current state of research.
- Explore current threat modelling frameworks.
- Identify aspects of threat modelling frameworks which would prove useful for micro businesses.
- Conduct a survey to explore how micro businesses approach cybersecurity.
- Design a non-technical threat modelling framework for micro businesses based on the research done.
- Design a web-based threat modelling tool for micro businesses based on the framework.
- Conduct a second survey to gather feedback from the micro business owners in order to validate the framework and the tool.

1.1.5. Artefacts

The project will result in two artefacts being created:

1.1.5.1. Non-technical threat modelling framework for micro businesses

A threat modelling framework specifically designed for small businesses that lack cybersecurity knowledge and expertise. The framework will incorporate some aspects of popular threat modelling frameworks such as STRIDE or DREAD, as well as the MITRE ATT&CK framework. If possible, the new framework will follow an easy to remember mnemonic. The main objectives are (1) to design a framework that is compliant with industry standards, (2) to provide small business stakeholders without a computer/cybersecurity background with an easy-to-use framework that will help them identify the cybersecurity threats to their business and mitigate against them.

1.1.5.2. Web-based threat modelling tool

A web-based application that will be based on the framework designed. It will have an intuitive and easy to use GUI that will help users to identify the threats that their organisation faces. The application will also provide a visual attack tree, calculate an overall cybersecurity rating and suggest mitigation measures for the identified threats.

1.2. Methodology

The project will follow an 7-step methodology:

Step 1: Literature review on the current state of research on cybersecurity in micro businesses.

Step 2: An initial qualitative survey to explore how cybersecurity is handled in micro businesses and the pitfalls they encounter.

Step 3: Analysis of the initial survey results and identification of the problem areas.

Step 4: Identification of threat modelling frameworks that are relevant to micro businesses.

Step 5: Design a non-technical threat modelling framework based on the research done.

Step 6: Design a web-based threat modelling tool based on the framework.

Step 7: Follow-up survey on how micro businesses perceive the new tool and assess its impact on business cybersecurity.

1.2.1. Data Collection and Human Participants

1.2.1.1. Participant Recruitment

The researcher will reach out to micro businesses from around the world using publicly available email addresses (i.e. business websites or business directories, etc.). The outreach email will properly inform the recipient about the research and invite them to respond to an online questionnaire. No third-party services will be used to contact and recruit participants. The researcher will endeavour to contact only micro businesses. However, due to various factors, including the way businesses advertise themselves, some of the contacted businesses may not be relevant in terms of the size of their business. The screening questions in the first questionnaire will help the researcher to determine if the participant is relevant to the study.

1.2.1.2. Data Collection Method

The primary data collection method will be an online questionnaire. Two questionnaires are planned to be conducted. The aim of the first questionnaire is to explore how micro business owners approach cybersecurity and identify the potential shortcomings. The second questionnaire will be conducted in the end of the study after the respondents are introduced to the newly designed threat modelling framework and the tool. The purpose of the second questionnaire is to gather feedback about how the artefacts are perceived by the respondents.

Both questionnaires will be administered online. The reason behind this is to reach out to as much small business owner as possible from all around the world. In this way, the regional challenges that would factor into the small business approach to threat modelling can be offset. In addition, the structure of the questionnaires (i.e., branching and Likert scale questions) lends itself to online survey tools.

As indicated by the information sheet and privacy statement accompanying the questionnaires, no personally identifiable information will be disclosed as part of the study and all data collected will be anonymized. In addition, the right to withdraw from the study is provided to all participants.

1.2.2. Skeleton of the Literature Review

- A summary of available threat modelling frameworks: Discussion of the widely accepted and used threat modelling frameworks.
    - STRIDE
    - DREAD
    - PASTA
    - …
- A critical look at the frameworks in terms of their usefulness for micro businesses
- Current state of research on threat modelling for SMEs
    - Current state of research for SMEs

      SMEs is a frequently visited topic in cybersecurity research. In this section, the current state of research will be explored.
    - Current state of micro businesses in particular

While there is a considerable amount of literature on SMEs, micro businesses are a very specific subset of SMEs that require a very different approach. This section discusses the current state of research in threat modelling at the micro business level.

- Threat modelling challenges for micro businesses

Finally, the challenges faced by micro enterprises in threat modelling will be reviewed.

1.3. Key Literature

In his seminal book, Adam Shostack (2014) points out that threat modelling doesn't have to be a technical process, and even if we're not fully aware of it, we're doing it in our everyday lives. In the book, the readers are walked through easy-to-understand examples. While the author's approach is still somewhat technical and may not be comprehensible to those without a cybersecurity background, the point the author is trying to make is very similar to mine.

The Threat Modelling Manifesto Click or tap here to enter text. is another important document that sets out the principles and values of threat modelling, emphasising that everyone should use threat modelling to protect their systems from threats. As I will be trying to demonstrate that the micro businesses can and should threat model with a non-technical threat modelling framework without cybersecurity expertise, the thoughts mentioned in the manifesto fit very well with the main idea of my study.

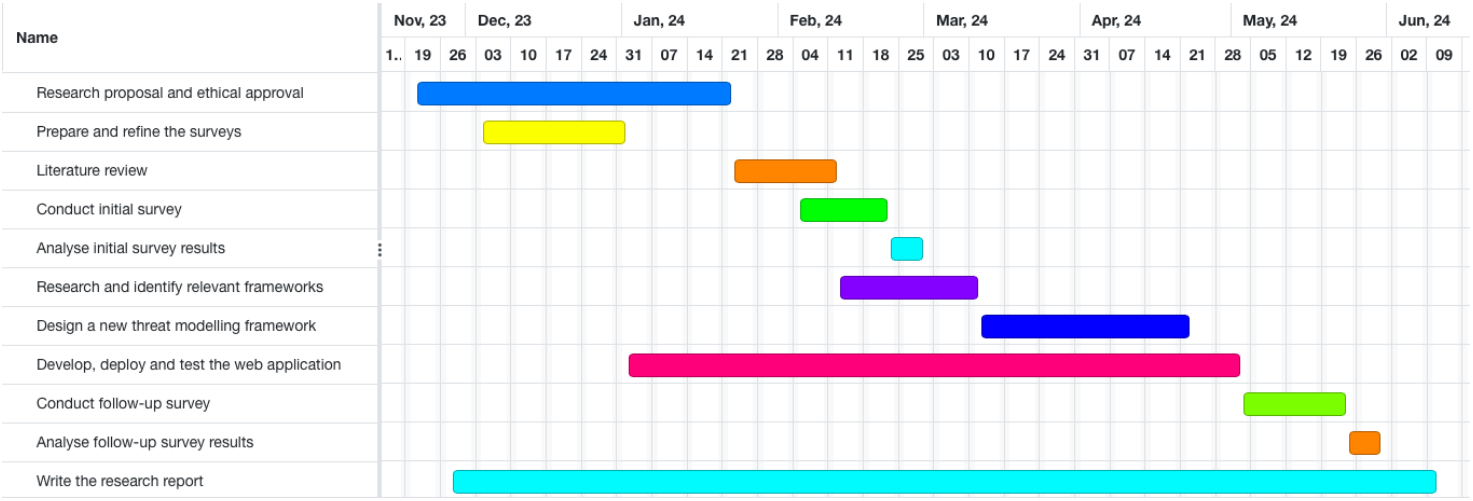
The number of methods available for threat modelling can be daunting, especially for the novice threat modeler. That's why the work by the Carnegie Mellon researchers (Shevchenko et al., 2018), in which they reviewed twelve available methods and demonstrated their use cases, can be useful to many. It will also be a starting point for my project as I try to compile a catalogue of threat modelling frameworks, so that I can incorporate relevant aspects of each into a non-technical framework that can be used by non-technical people.

In addition to these three, the following are some of the more notable literature on the subject:

- Attack Trees, chapter from the book “Secrets and Lies” (Schneier, 2015: 318-333)
- Common Vulnerability Scoring System (CVSS) (FIRST, 2023)
- NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations (NIST, 2018)
- OWASP Threat Model Cookbook (OWASP, 2021)

- Security Development Lifecycle (Howard & Lipner, 2006)

1.4. Project Timeline



References:

Braiterman, Z. et al. (N.D.) Threat Modeling Manifesto. Available from: https://www.threatmodelingmanifesto.org/ [Accessed: 9 December 2023].

Burnap, P. (2021) Risk Management & Governance Knowledge Area Version 1.1.1. Available from: https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf [Accessed: 9 December 2023].

European Commission (2020) *User Guide to the SME Definition*. Luxembourg: Publications Office of the European Union.

Eurostat (2023) Enterprise statistics by size class and NACE. Available from: https://ec.europa.eu/eurostat/databrowser/view/sbs_sc_ovw/default/table?lang=en [Accessed: 9 December 2023].

FIRST (2023) CVSS v4.0 Specification Document. Available from: https://www.first.org/cvss/v4.0/specification-document [Accessed: 3 January 2024].

Howard, M. & Lipner, S. (2006) *The security development lifecycle: A process for developing demonstrably more secure software*. Redmond: Microsoft Press.

Hutton, G. (2022) Business statistics. Available from: https://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf [Accessed: 9 December 2023].

NIST (2018) *NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations*. DOI:10.6028/NIST.SP.800-37r2.

Office for National Statistics (2021) Micro enterprises by employee size and industry. Available from: https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/adhocs/13728microenterprisesbyemployeesizeandindustry [Accessed: 9 December 2023].

Office of Advocacy (2017) The Role of Microbusiness Employers in the Economy. Available from: https://advocacy.sba.gov/2017/08/01/the-role-of-microbusiness-employers-in-the-economy/ [Accessed: 1 January 2024].

OWASP (2021) OWASP Threat Model Cookbook. Available from: https://github.com/OWASP/threat-model-cookbook [Accessed: 9 December 2023].

Schneier, B. (2015) *Secrets and Lies*. Indianapolis: Wiley. DOI:10.1002/9781119183631.ch21.

Shevchenko, N., Chick, T.A., O'riordan, P., Scanlon, T.P. & Woody, C. (2018) Threat Modeling: A Summary of Available Methods. Available from: https://insights.sei.cmu.edu/documents/569/2018_019_001_524597.pdf [Accessed: 9 December 2023].

Shostack, A. (2014) *Threat Modeling: Designing for Security*. Indianapolis: John Wiley & Sons.

UK Government (N.D.) Prepare annual accounts for a private limited company: Micro-entities, small and dormant companies. Available from: https://www.gov.uk/annual-accounts/microentities-small-and-dormant-companies# [Accessed: 9 December 2023].

Section 2 Ethical approval

Use the following headings to describe and discuss how you intend to deal with ethical issues in relation to your research. You should consult the university guidelines and project module content to help you to do this. Acknowledge how you propose to address the issues if your research or part of your research is going to take place online. (**No more than 2000 words**)

1. Consent

How do you intend to seek informed consent from participants?

As part of the project, participants will be asked to respond to two questionnaires (i.e., “Initial questionnaire” and “Follow-up questionnaire”). At the beginning of each questionnaire, there is a project brief and a privacy statement in order to inform the participants about the project, privacy policy, and their rights.

The project brief informs users about the project title, the researcher (including contact details), the purpose, what is expected from participants and the outcome of the project.

On the other hand, the privacy statement informs users about their rights (including the right to withdraw), the data to be collected, the use of the data collected, the use of the data, and the data retention period.

Finally, users are reminded that x clicking "Next" to proceed to the questionnaire, they acknowledge the information provided and agree to participate in the survey.

2. Right to withdraw

How do you intend to inform participants of their right to withdraw?

Participants will be allowed an opt-out period of 7 days after the data collection. Participants can withdraw from the study at any time, but their right to withdraw may vary depending on when they exercise it:

Before the opt-out period: The participants can withdraw from the study before the opt-out period ends. In this case, their data, including their email address and responses, will be deleted, and they will no longer be communicated in regard to the follow-up survey.

After the opt-out period: The participants can still withdraw from the study after the opt-out period. In this case, their email address will be deleted, and you they will no longer be communicated in regard to the follow-up survey. However, in this case, it will not be possible to delete their responses due to the anonymised nature of the data.

The participants exercise their right to withdraw from the project by contacting the researcher by email.

This information will be provided to participants in (1) the privacy statement before they begin to answer the questionnaire, and (2) the debrief section after the questionnaire.

3. Confidentiality

How do you intend to maintain confidentiality?

The following measures will be taken to ensure confidentiality:

1. Only email addresses will be collected from the participants. The email address is necessary to reach out to the participants for the follow-up survey. Other personally identifiable information (such as name, surname, address, etc.) will not be collected. Instead, the participants will be assigned a number to facilitate the data management.
2. The data will be anonymised after 7 days of collection so that there will be no direct association between the participant's email address and the data collected from them.
3. The data will be stored on encrypted disks (256-bit key encryption with Apple FileVault 2) and will not be stored online.
4. The data will not be shared with any 3rd parties under any circumstances.

4. Harm

How do you intend to protect participants from harm?

In order to protect the privacy of the respondents, minimal personal information (i.e. only email address) will be collected. The data will be stored on encrypted disks in order to prevent unauthorised third parties from tampering with the data.

In addition, the data collected will only include what is strictly necessary for the study (e.g. educational background, cybersecurity knowledge and will not include sensitive data that requires stronger legal protection according to the UK Data Protection Act (2018) and the EU General Data Protection Act (2016).

Finally, participants have the right to withdraw from the study at any time.

5. Data access, storage and security

Please confirm that all personal data will be stored and processed in compliance with the General Data Protection Regulation (GDPR). Describe the arrangements for storing and maintaining the security of any personal data collected as part of the project.

All personal data collected as part of the study will be stored and processed in compliance with the UK Data Protection Act (2018). The following measures are taken to ensure the safe storage and processing of data:

1. The data collected will be stored on encrypted disks (256-bit key encryption with Apple FileVault 2).
2. The data will only be accessed by the researcher.
3. The data will not be shared with any 3rd parties under any circumstances.
4. The device used to store the data will be behind a firewall, regularly updated with latest security patches and protected by up-to-date anti-virus software.
5. In order to minimize the risks, the researcher will only access and work on the data in their home environment.

6. Other issues

Identify any specific ethical issues relating to this research, for example if your research involves vulnerable groups like young children, or pupils who have SEND (special educational needs/disability).

The study does not involve any vulnerable groups, and no other ethical issues specific to the research have been identified.

Section 3 Risk Assessment

If your research does not involve human participants, you are able to enter "N/A" in the comment box.

1. Are there any potential risks, for example physical, psychological, social, legal or economic, to participants or subjects associated with the proposed research?

YES / ~~NO~~

Please provide full details of the potential risks and explain what risk management procedures will be put in place to minimise the risks:

Risk: Survey respondents' private/sensitive information compromised

Mitigation:

- The measures and safeguards set out in the Data Protection Act (2018) will be implemented to the highest extent possible.
- Minimal Personally Identifiable Information (PII) will be collected during the survey (only email address).
- The data collected will be anonymized.
- The data collected will be stored on encrypted disks (256-bit key encryption with Apple FileVault 2). The device used to store the data will be behind a firewall, regularly updated with latest security patches and protected by up-to-date anti-virus software.

2. Are there any potential risks to researchers as a consequence of undertaking this proposal?

YES / ~~NO~~

Please provide details and explain what risk management procedures will be put in place to minimise this.

Risk: Privacy of the researcher violated during the reach-out campaign and/or questionnaires

Mitigation:

- A separate Google account will be created for the outreach campaign.
- The questionnaire will be administered using this Google account.
- The account will be deleted once the research is complete.

Risk: Fatigue due to excessive working hours

Mitigation:

- A Gantt chart will be used to break the project down into manageable steps, with sufficient time allocated to each step to avoid excessive working hours, especially towards the end of the project.
- Project management software (Trello) will be used to track project progress on a Kanban board.
- Supervisors will be updated on the progress of the project and regular supervisory meetings will be held.

3. Are there any potential reputational risks to the University of Essex Online as a consequence of undertaking this proposal?

~~YES~~ / NO

Please provide full details and explain what risk management procedures will be put in place to minimise this.

4. Will the research involve individuals below the age of 18 or individuals of 18 years and over with a limited capacity to give informed consent?

~~YES~~ / NO

(If yes, a Disclosure and Barring Service disclosure (DBS check) may be required. Please attach as part of your application). Give further details of participants below.

5. Are there any other ethical issues that have not been addressed, which you would wish to bring to our attention?

~~YES~~ / NO

Give details below:

Section 4 Confirmation Statements

The results of research should benefit society directly or by generally improving knowledge and understanding. I confirm that my research project has a potential benefit. (If you cannot identify a benefit, you must discuss your project with your supervisors to help identify one or adapt your proposal so the study will have an identifiable benefit.)

I confirm that I have read the Research Ethics Policy and the relevant sections of the Research Ethics Procedures and will adhere to these in the conduct of this project.

(These statements must be ticked in the form.)

University of Essex Online

Signature

Date and Signature space are available in the form.

Attachments

You are required to attach the following documents to this form:

1. An example of your participant information sheet and consent form, if applicable.

2. Consent document from the organisation your research is taking place, if applicable.