IT University of Copenhagen **Date:** September 28th  
**Course:** Software Engineering **Supervisor:** Renata  
**Group:** 16 **Version:** 2  
**Document nr:** 3 **Tollgate:** 1  
**Responsible:** Peter **Status:** Ready for TG1

Portfolio document 3

Explore your case

A person and person holding a large arrow

Description automatically generated

**Students:** **Student ID:** **Email:**  
Carl Villads Dissing Fristam 17950 [cavf@itu.dk](mailto:cavf@itu.dk)Cecilie Malmberg 20963 [cecm@itu.dk](mailto:cecm@itu.dk)Luca Giannini 22150 [lgia@itu.dk](mailto:lgia@itu.dk)Peter Klarskov 19517 [pekd@itu.dk](mailto:pekd@itu.dk)Victoria Hinley Deng 17952 [vide@itu.dk](mailto:vide@itu.dk)

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change | Author | Date |
| 0 | Drafted initial version for review | Peter | 15.09 |
| 1 | Added ChangeLog | Peter | 22.09 |
| 2 | Added features, qualities and extended research sections | Victoria | 27.09 |
| 3 | Reviewed and resolved comments | Peter & Luca | 28.09 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Context and Motivation**

Small businesses are increasingly using technology for different parts of their enterprise. This poses security risks to the business owners as well as their customers, as cyber-criminals view these companies as increasingly attractive targets. Due to the nature of their scale, however, these small businesses have very limited resources and budgets for cyber-security measures. Apart from just financial limitations, small businesses have trouble safe-guarding themselves due to issues presented in some of our additional material (Hall et al. 2021):

* Research and data relating to cyber-security is usually derived or obtained from non-representative, larger enterprises and is not translatable (ibid. 3-4).
* Many cyber-incidents are “symptom-less” to the normal user and only detectable via active traffic monitoring that few small businesses can afford (ibid. 5).
* Current cyber-security solutions favor larger organizations as they have historically been the targets of famous cyber-incidents and are ideal customers (ibid. 6).
* Proper cyber-security solutions rely on separate testing environments, requiring “substantial technical knowledge, time and ongoing maintenance” which is unfeasible for smaller businesses (ibid. 6).
* Mixed-use devices are common in small businesses, which makes the intrusive qualities of MDM software undesirable (ibid. 7)
* Lack of human resources with technical knowledge, “The small IT budgets of small businesses do not cover the salary of an IT administrator” (ibid. 7)
* Cyber-security assessment *cannot* be done effectively by a novice (ibid. 8)
* Many small businesses are short-lived and do not focus on processes in the inception and survival stages of the company (ibid. 8)
* Non-technical small business owners feel a low sense of control in relation to the complexity of cyber-security, possibly leading to inaction (ibid. 8)

**Existing Research and Products**

Some researchers have taken an interest in the cybersecurity issues of small businesses in recent years. This includes research for Australian small business needs (Hall et al. 2021) and analyses of different security approaches to cyber security in smaller systems (Zvereva and Loshchenko 2022, Bada and Nurse 2019). The research is not exactly extensive, as is also highlighted and criticised by Hall et al., but it does exist, and solutions are sorely needed.

Apart from traditional anti-virus services, platforms such as [vanta.com](https://www.vanta.com/) focus entirely on compliances, confidentiality, trust building and risk assessment. Optimally, a one-stop security offer would incorporate both considerations in one.

Some small business owners do not see the value of investing in cyber-security perceiving it as more of an inside-cost than a means for more revenue (Feagin 2015). This is a fallacy because low security can put their own, and customers information at risk in the event of a security breach (ibid.). When working with confidential data, it is vital to not only protect it, but also build trust with the business owners, so they keep continuing using the services (Yu et al. 2015). This is also evident in other domains with high confidentiality such as internet banking (ibid.). Trust can be fostered through various means. In the journal article ‘Banking System Trust, Bank Trust, and Bank Loyalty‘ by van Esterik-Plasmeijer and van Raaij (2017) they identified six drivers of trust in banking, namely; integrity, transparency, customer orientation, and competence. Taking inspiration from bank trust, we now have a starting point for how trust could be incorporated in the context of cyber security.

**Idea contribution**

We want to provide an automated digital security assistant that checks the customers system for possible insecurities. As highlighted in some of the research, the app would have to both check for technical vulnerabilities in the system, but also serve as a form of educational tool for the user, as many cyber-attacks are of a social nature such as phishing attacks. Most current options on the market consist mostly of anti-malware software which neglects the user education. The assistant would need to be usable by technical novices and accommodate many different system setups, as there is no de facto way of doing IT at a small business level. The assistant helps users comply with relevant data protection and security regulations of our targeted regions (TBD).

**Features**

**Onboarding**

To ensure successful software adaptation there should be an onboarding process for new users. The process should encompass an introduction to the core functionalities and how to use them when accessing the application for the first time.

**Risk assessment & solutions**

The application should provide a user-friendly overview of security vulnerabilities within their system, accompanied by detailed explanations of recommended solutions. Solutions could be in the form of a suggestion to modify parts of their system for better security, or for better infrastructure. The change is only implemented if it has been manually accepted. In the case where the security risks prove to be too complex, the application should offer suggestions for consulting an IT-professional.

**Compliances assessment**

The application should assess if their system adheres to compliances and security regulation. Additionally, it should provide suggestions for achieving them. Compliance laws such as GDPR emphasises a need for IT managers in small businesses to protect the information of their customers from not just outside attacks, but also from individuals within the company getting unwanted access to confidential information.

**Anti-virus service**

The application should incorporate conventional anti-virus features to detect malicious activity and mitigate them. These features should be running in the background and only notifying in the event of significant threats.

**Educational**

The application should have educational features. This could be tips from the digital assistant, courses or the assessment overviews.

**Customer Service as a Feedback Mechanism**

To facilitate the ongoing enhancement of the services, the implementation of a feedback mechanism is crucial. Such a system not only signifies our commitment to valuing our customers but also serves as a crucial avenue for obtaining valuable insights.

**Qualities**

Based on the case and research we listed some essential qualities to deliver a good product. They are listed as separate but are inter-related.

**Security**

As an IT-security service it is essential that the product is secure to use. It should mitigate cyberattacks, protect information assets as well as sensitive information from their system and their customers. Their information assets should not be compromised when the service is in use.

**Trustworthy**

Trust is important to maintain customer relationships. In the realm of cyber security this means that there should be transparency on how their data is being used. They should be orientated of any changes and as a service provider, business should be conducted with high integrity. Furthermore, by demonstrating competence in the service that is provided, trust is further strengthened and access to small business infrastructure becomes easier. Positive experiences help keep and gain new businesses as customers.

**Educational**

In many cases, the user is the first line of defence against cyber-attacks – e.g., Phishing attacks. Educating business owners on how to navigate could therefore prove vital in strengthening security and maintain trust. This can also manifest in the explanations formed from the various assessments, which can help them understand their system better.

Other possible qualities: Userfriendly/usability