**Project/product idea – Case 3: Technical Security Analysis for Small Businesses**

A digital security consulent that analyses the given business' software and detects security threads within the business. The application will provide suggestions for how to improve the security.

**Article summary:**

Summary of *The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses*

Small businesses employ a significant portion of the workforce (half of Australian private sector) and have become attractive targets for cyber-criminals (Tam et al. 2021, 1). Modern cyber-security measures involve not just the protection of information systems and data, but also non-technical aspects such as security culture surrounding the users of the information (ibid. 2). According to an assortment of studies, a “one-size-fits-all cyber-security solution does not exist” (ibid. 2).

While small businesses previously tended to avoid having an online presence due to security factors, market forces and developments mean that online sales continue to increase in attractiveness (ibid. 2)

Small businesses struggle to safeguard themselves due to:

* 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)
* Cybersecurity measures cannot be copy-pasted from larger business to smaller ones. (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)
* Smaller businesses’ move towards cloud infrastructure renders traditional cyber-security products, such as general network scanning, unsuitable (ibid. 7)
* Mixed-use devices are common in small business, 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)

Advantages and possibilities for small businesses:

* Small businesses are shown to be very agile and fast-changing when needed (ibid. 10)
* A zero trust model could be implemented for small business by standardizing the model for implementation in components (ibid. 11)
* Using OSSH can be very beneficial to small businesses (still need technical knowledge) (ibid. 11)

Some numbers:

“[…] the average business cyber-security spend in European countries for organisations with 9 or less employees was US$7,000.” (ibid. 2)

(ChatGPT generated software qualities based on the case)

**User-Friendly Interface:** Develop an intuitive and easy-to-navigate platform to cater to small business owners with varying levels of technical knowledge.

**Multi-Level Assessment:** Provide basic and advanced security assessments to accommodate users with different technology awareness levels.

**Customization and Flexibility:** Allow users to input specific business details for tailored security recommendations.

**Security Information and Education:** Offer easily understandable information about common security threats and mitigation strategies through text, videos, and interactive guides.

**Privacy Protection:** Robust data encryption and secure storage practices to protect user information and ensure privacy.

**Trust-Building Features:** Incorporate trust-building elements like user testimonials, security certifications, and transparent data handling policies to gain user trust.

**Access Control:** Minimize intrusive access by utilizing non-invasive assessment techniques like network scanning.

**Time Efficiency:** Streamline the assessment process to account for the time constraints faced by small business owners.

**Legal Compliance:** Ensure compliance with relevant data protection and security regulations, particularly in Switzerland and target regions.

**Scalability:** Plan for regular updates and improvements to accommodate a growing user base and evolving security threats.