Literature Review

Follows the bibliography posted for Tollgate 1 submission.

**Raineri, Ellen M., and Jessica Resig. “Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses.” *The Journal of Applied Business and Economics*, vol. 22, no. 12, 2020, pp. 13–23.**

The text focuses on the impacts and importance of self-efficacy in relation to cybersecurity efforts by small businesses. The conclusion primarily revolves around self-efficacy having a tremendous impact on the efforts made by the business owner, and how training greatly improves self-efficacy. Apart from the fact that lack of education has been identified as a primary issue when dealing with the cybersecurity of small businesses, this text provides a great argument as to why we include an educational element in our approach.

**Cherry, Denny. *Enterprise-Grade IT Security for Small and Medium Businesses: Building Security Systems, in Plain English*. 1st ed., Apress L. P, 2022.**

A whole book on our subject, but I cannot find access to it somehow. If we can get our hands on it, it would probably be worth skimming through.

**Dinkova, Milena, et al. *Should Firms Invest More in Cybersecurity?* Small Business Economics, 2023.**

A more critical text that does not find any relation between increased cybersecurity spending and the profit of the company. It questions the worries that policymakers have when they proclaim that smaller businesses spend too little on cybersecurity. It also notes that an initial increase in spending on cybersecurity efforts lead to an increase in report cybersecurity attacks – something that the authors suggest happens because the system allows for detection of attacks, not because the number of attacks actually increases. Increased spending from then on decreases the number of attacks quite significantly.

This text also has a literature review itself which is quite informative.

**Walsh, Karen. *Security-First Compliance for Small Businesses*. CRC Press, 2024.**

Brand new book on cybersecurity and compliance for small businesses. It identifies in depth the value of trust-building and the duties of companies to protect the data of their customers. It also explains the strain between governmental bodies wanting to punish data beach-victims on behalf of the customers for not having proper security, and the actuality of the situation in which SMBs struggle to gather the necessary resources and knowledge to protect the data. It references a Boehm and McKinsey text (*Why digital trust truly matters*) that describes how important trust is, although I haven’t had the chance to read it yet. But these numbers speak for themselves:

* 85% of respondents say that knowing a company’s data privacy policies before making a purchase is important.
* 46% of respondents say that they often or always consider another brand if the one they consider purchasing from is unclear about how it will use their data.
* 54% of respondents say that they make online purchases or use digital services only after making sure that the company has a reputation for protecting customer data.

Based on this info, we could consider having some kind of certification attached to the use of our system.

The book has a lot of other information as well, but it is 220 pages long, so I haven’t read all of it.

**Njenga, Kennedy. *Information Systems Security in Small and Medium-Sized Enterprises: Emerging Cybersecurity Threats in Turbulent Times*. 1st ed., Nova Science Publishers, 2022.**

Can’t find access, but synopsis sounds relevant.

**Gafni, Ruti, and Yair Levy. *Experts’ Feedback on the Cybersecurity Footprint Elements: In Pursuit of a Quantifiable Measure of SMBs’ Cybersecurity Posture.* Information and computer security (2023).**

Can’t be found online, but I got a PDF from the library :^).

Text has a nice introduction that describes the SMB cybersecurity issue and how relevant it is today (text is from May 2023). Last year 69% of surveyed SMBs reported a data breach, and a third of those reported multiple data breaches in one year. They have tried to make a system for measuring cybersecurity footprint, but it is kind of iffy and the experts don’t really agree on the impact of different breaches. One thing they do conclude is that volume of data is much less important than type!

**Bada, Maria, and Jason R.C Nurse. “Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs).” *Information and computer security 27, no. 3* (2019): 393–410.**

We already have this in the bibliography, but I decided to check it out because the title seems very relevant.

The text directly says that GDPR-compliance is hard for SMBs. Page 4 has some *really* good notes on how and why to build a strong security culture in your business. Text is an absolute goldmine on the existing research and initiatives relating to SMB cybersecurity and how important it is. Also says in quite simple terms that education is key as well as technical security tools. Look up Iyamuremye & Shima, 2018. Bada and Nurse also explain that one important part of the job is actually explaining to the customer why cybersecurity is important, which requires some amount of trust. There’s an excellent overview of these security aspects on page 6. Page 13 has an excellent figure on how to approach SMBs.