Summary

In this thesis, we have sought to understand cyber security in Danish SMEs. SMEs face increasing regulatory demands and cyber threats from sophisticated malicious actors. At the same time, SMEs have the least resources available to combat these threats. Therefore, we researched the topic further to understand how cyber security is handled in SMEs and which resources are available to them. We also conducted an expert interview, where we gained insight into the challenges SMEs face and which cyber risks they can face in light of technological advancements such as generative artificial intelligence.

To continue our research into the field of IT security in SMEs, we conducted interviews with seven different SMEs. To ensure relevance for our research aim when collecting data, we created criteria for the participating companies. We interviewed only Danish SMEs with no formal IT department to understand their practices. We also chose to speak with IT managers in the companies, as they had the most knowledge about how IT is managed internally. Following the interviews, we conducted a thematic analysis to gain a better understanding of the interviews. The analysis revealed that many managers bear the sole responsibility for IT in their organisations and often hold other areas of responsibility. Additionally, we observed that nearly all interviewed SMEs outsource the management of their IT and IT security to a third party. However, this discovery also exhibited that many managers tended to view the third party as the main holders of responsibility, in the case of a cyber attack. Furthermore, many expressed that they lack the appropriate competencies about IT, making the SMEs very dependent on their service providers. To address these challenges and problem areas in regard to outsourcing and negation of responsibility, we sought to promote feelings of ownership among IT managers. This is also reflected in the research question for this thesis: *How does outsourcing of IT influence IT managers' attitudes toward cybersecurity in Danish SMEs?*

In this exploration, we developed a tangible design along with a tablet application. The goal of our design, titled LockEd, was to support knowledge of IT security and general IT practices, as research finds that this could help empower feelings of responsibility. To implement LockEd, we 3D printed a physical padlock with a servo motor and a tablet application, connected via Bluetooth. The padlock was chosen as a design to create a physical manifestation of security, where the shackle of the padlock can move up and down, representing security. To move the motor, we connected it to an Arduino which was programmed to send signals to the motor at fixed times. The Arduino was connected to our application, which included tasks in the form of multiple choice questions, as well as a reflection question for the user. The content of these tasks and reflections was designed to be relevant for SMEs and derived from interview data. To indicate when the user should engage with the padlock, the shackle would be driven up, to show that it was open. Once the user completed the tasks on the tablet, the shackle moved down, representing that it was physically secured.

To evaluate our system, we conducted a test with one of the participating IT managers. LockEd was installed in their office and was present for one and a half week, where the manager had to use the system twice. To avoid any problems during use, a step-by-step guide was provided to the participant. Finally, to gather insights about the participant's experiences, we held a follow-up interview to learn about their thoughts.

The interview revealed that the participant had a positive experience with LockEd with no difficulties using the system. However, there was a minor delay in the shackle moving down the first time they interacted with the system. The participant stated that they found the system to be fun and engaging to use. They also felt that they learned new things about IT security and

felt the tasks in the system were of appropriate difficulty. Further, the participant stated that they could see the benefits of using the system long term and including other employees in using it as well.

Discussing our results showed that having a tangible design, coupled with a digital application, could be beneficial to support awareness of IT and security. It can be beneficial to separate the system from the other digital clutter, e-mails and other apps, that are often present in an office environment. Additionally, the intuitiveness of the padlock can create interest and curiosity, thus creating engagement in cyber security, which can be intimidating for those with low IT expertise. However, despite these findings, it is important to note that our research was limited by the amount of time that LockEd was tested. To observe more concrete results about how our design can support awareness of responsibility and ownership, longer testing is required. Additionally, more test subjects would also be essential in further validation of results.

Concluding our study, we have discovered that outsourcing in SME environments can affect the feelings of responsibility and ownership in IT managers in the face of cyber threats. Additionally, we learned how this challenge can be mitigated via a tangible design, coupled with a digital application to promote regular learning about IT. In conclusion, the study provides a meaningful foundation for future research on how physical artefacts can support digital systems to increase awareness and a sense of responsibility surrounding IT security in outsourced environments.

Someone Else's Problem? How Cyber Security Outsourcing Influences Security Ownership in SMEs

Emilie Tiina Frost Jakobsen, Nadja Dalgaard Hansen, Tanja Sørensen

Digitalisation and Application Development, Group 5. 2025

Master's Thesis

STUDENT REPORT
AALBORG UNIVERSITY

Title: Someone Else's Problem? How Cyber Security Outsourcing Influences Security Ownership in SMEs
Module: Master's Thesis
Project period: Feb 2025 - Jun 2025

AALBORG UNIVERSITY
STUDENT REPORT

Abstract:

In the research of cyber security, there is a limited research on SMEs that outsource their IT to external providers. This paper researches how outsourcing IT can influence attitudes toward cyber security in these SMEs in a Danish context. Through interviews with seven Danish SMEs and a following thematic analysis, we sought to understand their cyber security practices. Our analysis revealed 24 themes, and a tendency in SMEs to shift responsibility to their IT security providers. To address this, we proposed a tangible design that aims to increase awareness of cyber security which may promote a sense of responsibility among IT managers in the SMEs. Through an evaluation of the design, we found initial indicators that show the benefits of using a tangible interface to enhance awareness of IT security. Furthermore, we discuss the need for further research in this area, specifically the long-term effects of such a design.

Project group participants:

Emilie Tiina Frost Jakobsen
Student no: 20204206

Nadja Dalgaard Hansen
Student no: 20204523

Tanja Sørensen
Student no: 20205381

Supervisor: Alisa Ananjeva
Department: Computer Science
Date: June 5, 2025

Pages: 15
Appendices: 11

Someone Else's Problem? How Cyber Security Outsourcing Influences Security Ownership in SMEs

Emilie Tiina Frost Jakobsen, Nadja Dalgaard Hansen, and Tanja Sørensen

Department of Computer Science, Aalborg University, Aalborg, Denmark

Abstract. In the research of cyber security, there is a limited research on SMEs that outsource their IT to external providers. This paper researches how outsourcing IT can influence attitudes toward cyber security in these SMEs in a Danish context. Through interviews with seven Danish SMEs and a following thematic analysis, we sought to understand their cyber security practices. Our analysis revealed 24 themes, and a tendency in SMEs to shift responsibility to their IT security providers. To address this, we proposed a tangible design that aims to increase awareness of cyber security which may promote a sense of responsibility among IT managers in the SMEs. Through an evaluation of the design, we found initial indicators that show the benefits of using a tangible interface to enhance awareness of IT security. Furthermore, we discuss the need for further research in this area, specifically the long-term effects of such a design.

Keywords: cyber security, SMEs, outsourcing, responsibility, tangible systems

1 Introduction

Danish small and medium-sized enterprises (SMEs) are far advanced in the digitalisation of their business practices [8], making them more dependent on IT systems and more vulnerable to the rising threat of cyber attacks [8]. However, SMEs often lack access to help and information regarding cyber security [6], which makes the threat of cyber attacks towards SMEs a serious issue. Additionally, new and extended regulations, such as the NIS2 Directive [28] and the General Data Protection Regulation [13], place growing demands on how businesses and their suppliers should manage cyber security. These regulations are often more challenging to comply with for smaller businesses that lack the necessary IT expertise and resources. As a result, SMEs risk being passed over as suppliers in favour of companies with greater resources, which could cost them important business opportunities (Cyber security expert, interview 03.03.25).

Faced with the increasing demands of regulations and the increasing cyber threats [8], many SMEs choose to outsource their IT operations to external providers [9]. Outsourcing to third parties can have great benefits [10] and let the SMEs focus their resources on core business operations [27]. It can also bring in the necessary technical expertise and technologies to meet evolving regulatory demands and changes in applications [27]. However, some consequences can also arise as a result of outsourcing. Literature suggests that outsourcing may increase dependence on providers [18], leaving them vulnerable if their security providers are attacked (Cyber security expert, interview 03.03.25). However, SMEs would still be the ones affected if something happened to their suppliers, particularly if they are unaware of how their IT has been managed.

Although some literature exists on the effects of outsourcing on SMEs ([18]; [2]), research in this area remains limited. Therefore, we aim to understand this further, as reflected in our research question:

How does outsourcing of IT influence IT managers' attitudes toward cybersecurity in Danish SMEs?

To answer this research question, we conducted interviews with seven Danish SMEs across different industries, along with a thematic analysis [4]. Based on these findings, we have developed a physical design aiming at enhancing the awareness of IT and promoting responsibility among IT managers.

2 Background

2.1 Cyber Security in SMEs

Cyber security can be defined as: *"[...] the collection and concerting of resources including personnel and infrastructure, structures, and processes to protect networks and cyber-enabled computer systems from events that compromise the integrity and interfere with property rights, resulting in some extent of loss."* ([31] p. 11). While there are various alternative definitions of cyber security [7], this interpretation highlights the importance of resources in protecting businesses against cyber threats. The view that cyber security is comprised of resources, such as personnel (e.g. employees with IT expertise) and infrastructure (e.g. two-factor authentication, antivirus software), helps us in understanding cyber security in SMEs as they often face significant limitations in terms of both financial and human resources [6].

SMEs face unique challenges in addressing cyber threats ([21]; [20]). When compared to larger enterprises, SMEs are at greater security risks as they have limited cyber security knowledge and allocate a lower, if any, budget to handling security and cyber attacks [21]. Consequently, this may lead to the neglect of preventive security measures and an insufficient level of IT security [21]. Another challenge lies in the fact that SMEs often underestimate how attractive a target they are for malicious actors [20]. These SMEs feel they are uninteresting due to their size, and that their security measures are adequate [20]. However, a risk analysis of Danish SMEs regarding cyber security finds that they are increasingly vulnerable to cyber attacks (e.g. ransomware and spoofing) [8], which highlights the need for effective yet affordable security measures [17].

To apply these measures and mitigate cyber security challenges, various studies ([17]; [26]; [15]) present a range of recommendations for SMEs. It is recommended that SMEs should establish a comprehensive information security policy that includes guidelines for employee training [17]. Additionally, SMEs should identify critical assets, secure accounts and data, and implement monitoring and security systems to detect threats early [26]. Employees should be trained to recognise threats such as phishing and social engineering, as human error is often a significant risk factor ([15]; Cyber security expert, interview 03.03.25). SMEs should also establish a documented incident response and recovery plan in case of a cyber attack [15].

Thus, there is a wide range of recommendations for SMEs, which can be challenging to navigate, especially given their limited resources. This lack of resources is also a significant reason why SMEs choose to outsource IT security [18].

2.2 IT Outsourcing in SMEs

Outsourcing IT operations enables SMEs to concentrate on their core business operations [27]. Having third parties manage IT and security allows SMEs to *"[...] limit IT expenditures, reduce the* *need for specialized personnel, and focus on core areas of expertise to help maximize profits."* ([27], p. 29) Thus, outsourcing can help SMEs combat the limitations in available resources for managing IT and mitigating cyber threats. However, despite the benefits that outsourcing IT security can offer [10], it can also pose risks. As an expert in cyber security explains: *"[...] once you have handed it over, it's also somewhat out of your hands how it is actually managed. Especially in the case of SMEs, which might not have the resources to thoroughly investigate: What is the security of their providers and how much risk are they exposing themselves to?"* (Cyber security expert, interview 03.03.25) This shows that involving third parties can lead to increasing operational uncertainty. Furthermore, it can also lead to failures in safeguarding sensitive information (e.g. the security provider may leak the SME's sensitive data to outsiders) [10]. This can be problematic for SMEs, as they still bear full legal and financial responsibility in the event of a security breach caused by the third party provider [10]. Correspondingly, Lair (2012) [25] emphasises that while organisations can outsource tasks to external parties, they cannot outsource the responsibility for data. Therefore, outsourcing IT security does not exempt companies from being held accountable for potential data losses and breaches [10].

3 Method

3.1 Data Collection

Relating to the research aim of our paper, we sought to understand how the outsourcing of IT influenced the attitudes toward cyber security among IT managers in SMEs. Therefore, we conducted interviews with IT managers from seven Danish SMEs. We decided to conduct the interviews with those responsible for managing IT in SMEs (referred to as IT managers), as they had the most information regarding current practices within the companies. The interviews aimed to gather information on their cyber security practices and their attitudes towards this. Since there is a general lack of research on cyber security practices in SMEs [22], it was important for us to understand more about them and the role that outsourcing played in these businesses.

Before interviewing, we applied the principles of purposive sampling [5] to ensure the selection of relevant interviewees who could inform our research question. The purposive sampling included the following criteria:

1. The SMEs had to be Danish.
2. The SMEs had to represent different industries.
3. The SME could not have a formal IT department.

We limited the research to a Danish context for the purpose of narrowing our scope. Including SMEs from different industries could help represent the broad scope of Danish SMEs, as well as their different IT practices. In the process of contacting SMEs for interviews, we reached out to a large number of businesses. However, many were not able to allocate time or were not interested in participating. As a result, the sample of participating SMEs was predominantly composed of cultural institutions. We focused our research on SMEs without a formal IT department, as we wanted to focus on SMEs with the least amount of internal expertise. When contacting the companies, we learned that many IT managers had other areas of responsibility in their companies. In some cases, there was no direct IT manager assigned, rather, there was an employee who had the responsibility for IT in addition to their other roles. This is visible in Table 1, showing which roles our interviewees held in the companies as well as the business's industries. However, I7 will not play a prominent role in the rest of this paper as, according to our interview, they do not outsource any of their IT.

ID	Professional Role	SME Industry
I1	IT Coordinator	Cultural Institution 1
I2	IT Manager & Marketing	Cultural Institution 2
I3	Finance & Administration Manager	Cultural Institution 3
I4	Sales & Marketing Manager	Cultural Institution 4
I5	IT Manager	Design Company
I6	CEO	Production Company
I7	Head of IT	Recruitment Agency

Table 1: Roles of interviewees

To collect data from our participants, we chose narrative interviewing [19], allowing the interviewees to articulate their lived experiences [19] and attitudes towards cyber security and outsourcing. An interview guide [24] served as a framework to ensure consistency across interviews, while still allowing the interviewees to speak freely and share their narratives. The interview guide was comprised of three main parts:

1. A presentation of the interview structure and introductory questions regarding IT setups, practices, and the manager's responsibilities
2. Presentation of a fictional scenario, involving a cyber attack which disables the company's critical functions
3. Prompting a narrative from the manager relating to the scenario, and follow-up questions

A significant part of the interview was based on the fictional scenario that we developed and adapted to each company. For example, in the case of a cultural institution, we described an attack where the institution's ticketing system was down. We chose to use a scenario as it could allow the interviewees to share their attitudes [30] toward their IT security and external providers by reflecting on how they would respond to the cyber attack. Furthermore, the attack was triggered by a colleague rather than the interviewee. We made this decision because being responsible for a cyber attack is often associated with feelings of shame and guilt [29]. We therefore assumed that it would be easier for the interviewee to engage with the scenario and speak more openly if a colleague triggered the attack. The interviews were conducted in Danish to allow the interviewees to express themselves freely without any language barriers.

Following each interview, audio recordings were transcribed, with filler words, repetitions, and non-verbal communication removed. This process also included anonymisation by changing names and other identifiers. The transcriptions were furthermore translated into English, whilst keeping closest to the original meaning.

3.2 Data Analysis

After transcribing the interviews, we began analysing the data according to the principles of thematic analysis [4]. During the analysis, we created codes that reflected the IT practices in the

SMEs and the managers' attitudes toward cyber security. An example of some of the codes are 'Lack of control' and 'Lack of information from IT security providers' which we derived from the quote: "*I don't know exactly what they do, but they save things and then they can see what exactly they do and then I think they just delete it. It's kind of out of our hands what they do.*" (I3). Based on the codes, we identified themes that emerged across multiple interviews. Initially, related codes were grouped to form preliminary themes. These groupings were then reassessed, and the themes were named based on their contents and patterns within the codes. As the aim of our research was to explore the attitudes toward cyber security in SMEs outsourcing their IT, this analysis allowed us to gain insight into their current IT practices and the influence outsourcing has on their attitudes.

4 Findings

Our thematic analysis of the seven interviews with IT managers led to the discovery of 24 themes. These themes encompassed a variety of IT related topics, including codes about general knowledge of the managers' responsibilities and work routines. Additionally, the themes included codes relating to attitudes towards cyber security and the practices in place to ensure IT security. As our research aimed to understand the influence of outsourcing on SMEs, we explored findings from themes that could contribute to this goal. Along with these findings from the interviews, we also derived design considerations which can help guide a physical design to support IT managers in light of the challenges they face. The key findings from our analysis are summarised in Table 2.

4.1 Internal IT Responsibility

A consistent finding across all the interviews was that the internal responsibility for managing IT and cyber security in the SMEs was assigned to one employee. The IT managers often had multiple roles within the organisation. For instance, one interviewee shared: *"I'm a sales and marketing manager with responsibility for IT. So I wouldn't say everything that's powered, but everything that's business-critical is my area of expertise. Everything that is sold online, all internal systems are my responsibility."* (I4) This example shows some of the IT managers' multiple roles and responsibilities that may not be directly related to IT.

This multifunctional nature of the IT managers' roles meant that the IT manager handled a mix of responsibilities. Another interviewee noted: *"Whether it's security, whether it's phones, computers, printers, internet, intranet, I'm in charge of. And I make sure that it works."* (I2) Because of this wide-ranging workload, time and resources dedicated specifically to IT security were often limited. One manager admitted: *"I probably spend 10% on IT and IT security and the remaining 90% I spend on finance and financial management."* (I3) This additionally meant that preventative measures in regard to cyber security were not prioritised. Furthermore, they expressed that the measures were often informal and they relied on "common sense" rather than on documented guidelines when informing employees about cyber security. One interviewee emphasised this approach by stating: *"No, first of all, if I get such an email from a customer, I will never download it. Never, ever."* (I3) Another described a more practical workaround: *" [...] if in doubt, we open on the phone to see if it's something real [...] so it's not something that goes in the system here."* (I6). While some had IT security policies in writing, they also expressed that *"[...] many* *people are busy and don't prioritise it [reading the policy]."* (I1) Thus, SMEs that had documented security policies also struggled with getting their employees to read them and engage in security.

When considering the limited amount of time that SMEs can devote to IT management, particularly cyber security, a design that supports IT managers should be convenient and flexible. This is essential so as not to interfere with their everyday work routines and many other areas of responsibility.

4.2 IT Expertise

In connection with the limited allocation of time and resources, some SMEs also acknowledged a lack of IT expertise and that they did not feel confident handling their IT security independently. One interviewee stated at the beginning of the interview that *"I'm not an IT technician."* (I3) while another commented: *"I don't know anything about that. There are some people who are a bit better than me."* (I6) We also found that this was a large reason for the SMEs to outsource their IT and security, as explained by one IT manager: *"[...] we are so dependent on our partners and we have chosen to outsource and chosen to buy these services, because then we know that we get all the specialists we need."* (I5) This lack of internal expertise made the SMEs very reliant on their IT providers.

Considering the lack of expertise among IT managers, a design that aims to support them, needs to account for their lack of IT knowledge. A design should be accessible to accommodate for the feelings of insecurity that exist in relation to their IT competencies.

4.3 Uncertainty of External IT Management

Another theme that emerged was uncertainty about their internal IT setup and security provided by their external partners, such as data storage, and backup routines. One manager expressed: *"I don't know exactly what they do, but they save things and then they can see what exactly they do and then I think they just delete it. It's kind of out of our hands what they do."* (I3) This shows that some managers are uncertain about their backups, specifically when these are needed in case of a cyber attack. Furthermore, some IT managers feel unsure about the steps their providers take in the event of an attack. Consequently, the IT managers rely on their providers to handle security without fully understanding how they do it or what that entails. Many managers expressed that they left it to their provider because they lacked sufficient knowledge about the subject.

The lack of uncertainty IT managers feel in regard to how their providers manage their IT needs to be taken into account when creating a design to support them. A design should aim to provide the managers with a better understanding of how their providers manage their cyber security, for example, in case of an attack. This could help alleviate the feelings of uncertainty some feel about the actions their providers take.

4.4 Dependence on External Providers

The strong reliance on external IT providers was a recurring theme across the interviews. Many SMEs described a strong feeling of dependency on their external providers and often lacked a sense of ownership of their IT systems. This was revealed in the follow-up questions relating to the cyber attack scenario in the interviews, where several managers indicated that their first action would be to contact their IT provider: *”So the first thing I do is contact them and ask them.”* (I2) Some managers did describe actions that the company could take itself, before contacting their providers, however, one interviewee remarked: *”So when such an attack comes, we actually have a company hired to handle that task, and they should know before we do, and they should see what's happening.”* (I4) This example indicates that some felt that the majority of the responsibility for recovering from an attack would lie with their external providers.

One of the main findings from our analysis was that many of the IT managers expressed a confidence in their providers handling any IT issue, as expressed by one manager: *”In my world, I think that *IT supplier* will take care of that, so my back is clear and I strongly assume that our security is okay.”* (I6) Thus, they not only delegate their IT management, but also the responsibility for it. While one interviewee acknowledged an internal responsibility: *”It's still our responsibility, but we use them to help us with everything. Because we don't have that knowledge at all.”* (I5), many expressed that the primary responsibility lied with their IT providers.

Considering the delegation of IT management responsibilities to security providers present among managers, a design should aim to provide them with more knowledge about general IT practices and cyber security. As many managers cited a lack of expertise as the reason for negating responsibility, increasing IT knowledge could strengthen their feelings of responsibility for their cyber security. In addition, a better understanding can help reduce overreliance on external providers, not by replacing them, but by enabling managers to engage more critically with third parties and remain aware of their security practices.

Key Findings
Internal IT Responsibility IT is managed by one person who has a mix of responsibilities - IT management is a supplementary task. Their limited time results in limited preventative measures in regard to cyber security. *Design consideration*: To accommodate for the lack of time dedicated to IT management, a design should be convenient and flexible to the managers' work schedules.
IT Expertise IT managers in SMEs generally feel that they have a low level of understanding and knowledge about IT security and IT in general. *Design consideration*: To address the limited knowledge of IT and security, a design should be accessible to users with a low level of IT expertise.
Uncertainty of External IT Management SMEs are unsure of their internal IT setup and the external management of their cyber security. *Design consideration*: To address this uncertainty of external IT management, a design should aim to provide IT managers with an understanding of IT practices of their security providers.
Dependence on External Providers IT managers delegate both management and responsibility to external providers. *Design consideration*: To address dependence on external providers, a design should aim to provide IT managers with more knowledge about general and security-related IT practices.

Table 2: Summary of key findings and design considerations

The findings revealed that there is limited internal expertise and a heavy reliance on external providers for IT and cyber security management across the SMEs. Although some had a level of policy or protocol in place, these were often informal or underutilised. Outsourcing their IT emerged as a solution to address gaps in IT knowledge and resources. However, this also showed a negative effect on managers' awareness surrounding cyber security, and a shifting of responsibility to their providers.

Some of our key analysis findings can be related to research on how outsourcing IT affects SMEs. Literature suggests that different attitudes exist toward cyber security and their service providers [2]. While some attitudes in organisations express confidence concerning security, feelings of insecurity and lack of IT knowledge can lead to the shifting of responsibility to third party providers [2]. This can be related to the phenomenon of responsibility diffusion in an organisation, which can result in employees and decision makers believing that *"[...] they are employed to do a specific task and not to address IT issues, such as cyber security. Moreover, they are not familiar with such tasks and believe that these are the responsibility of the IT service provider, who is paid for this and is an expert in the field."* ([2], p. 40). This understanding of responsibility diffusion aligns with its psychological definition, which denotes that the presence of other people makes an individual *"[...] feel less responsible for the outcome of group decisions, especially those with negative consequences."* ([3], p. 138) In an organisational context, employees can shift IT responsibility to their managers, while these managers can in turn shift responsibility to their IT providers, believing that they will take responsibility and solve any IT issues or threats [2]. This diffusion among managers or employees in businesses can be especially prevalent in the case of a cyber attack, where the risk of a negative outcome is increased [3].

In addition to the responsibility diffusion, the lack of internal IT expertise can increase the SMEs' dependency on their service providers [18]. By outsourcing all IT security-related tasks to service providers, internal knowledge and skills can be depleted, leaving SMEs vulnerable. To mitigate this co-dependency, SMEs can increase internal IT expertise to reduce the dependency on third parties [18]. However, increasing internal IT expertise to reduce this dependency can be challenging, particularly when considering the limited resources in SMEs [6].

5 Design

5.1 Tangible Systems

As cyber security is a complex and often invisible concept involving a vast range of technical, organisational, regulatory and human factors [34], it can be perceived as intangible. Physical design can help make such concepts more relatable by translating them into concrete experiences [36]. Zhou et al. (2024) explain: *"People often use embodied metaphors to describe intangible concepts [...] These metaphors originate from real-life embodied experiences and are influenced by cultural contexts".* (p. 431) Therefore, we find that using an embodied metaphor may help represent cyber security and responsibility in a more tangible manner for IT managers. This aligns with the concept of tangible user interfaces, which *"[...] computationally augment physical objects by coupling them to digital data. Serving as direct, tangible representations of digital information [...]"* ([32], p. 4). Tangible user interfaces can convey digital information to users regarding an action, via physical objects [32] (e.g. inputting coins into a piggy bank leading to an increase in digitally displayed funds). Furthermore, as another study highlights, interacting with physical objects engages multiple senses [16]. This sensory engagement can increase learning in users by creating physical embodiments and interactions [32].

Our analysis found that IT managers in SMEs often do not feel a strong sense of responsibility when it comes to their organisation's IT infrastructure and security. While they are formally tasked with overseeing IT, our analysis revealed that many lack insight into how their IT providers operate and respond to various security-related situations. We argue that by learning more about their providers and cyber security, the managers may strengthen their sense of ownership. Greater insight into the practices of external providers, combined with basic knowledge of IT infrastructure and security, may contribute to a more active engagement with the responsibilities they formally hold [2].

5.2 LockEd

To implement this as a design, we propose a solution, titled LockEd, that aims to support the learning and thereby the awareness of IT and cyber security in SMEs. LockEd consists of an application that includes a series of tasks in the form of multiple-choice questions, and a question prompting the IT manager to reflect on some of their organisation's IT practices. To structure the presentation of the system's tasks, we also created a theme for each week, related to the tasks. The questions and themes for LockEd are listed in Table 3. The application is paired with a physical 3D printed padlock to symbolise security. At weekly intervals, the padlock unlocks automatically, prompting the IT manager to engage with a new set of tasks. By completing the tasks, the padlock will automatically lock itself.

System Access and Responsible Network Use
Question 1 What is the primary function of a VPN (Virtual Private Network)?
Question 2 Why is it important to keep logs of login attempts and system access?
Reflection question You're on vacation and receive an email saying your company email has been used to send spam. What steps would you take, and would you have access to the necessary tools or contacts?
Data Management and Data Breach Liability
Question 1 How can sensitive data be unintentionally exposed in a cloud solution?
Question 2 What should you ensure when using an IT provider that handles customer data?
Reflection question If a customer asked how their data is protected, what would you be able to tell them? Would you feel confident explaining it?

Table 3: Questions in LockEd (translated to English)

To ensure that using the system was not too time-consuming for IT managers, we designed the tasks to include a few questions, which only required the IT manager to choose an answer

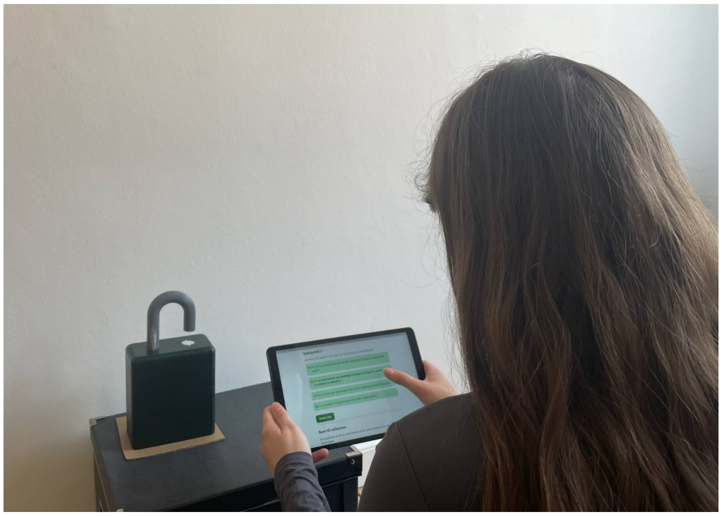

Fig. 1: LockEd

to complete. Additionally, the tasks had a flexible time window for completion. This is essential, as many IT managers in SMEs have many different areas of responsibility and job functions. To ensure regular interaction with LockEd, it was designed to be used on a weekly basis.

To ensure engagement with the system's tasks, we aimed to make the multiple-choice questions and reflection questions relatable for SMEs. For example, some questions related to how other employees have access to internal systems. Additionally, we derived some questions from a datapoint from our interviews, where managers expressed uncertainty about data storage.

We chose to create a tangible user interface to provoke an intuitive reaction from our users. By creating a physical symbol of security, a padlock, we hoped to appeal to the user's rationale, as the padlock resembles a recognisable, real-world object [36]. Furthermore, by allowing the padlock to be locked and unlocked, the user would be prompted to interact with the system to 'lock' the padlock again, which we deem to be an intuitive interaction [36].

5.3 Implementation

To implement LockEd, we developed the application using the Flutter framework [11] and the programming language Dart [12]. To create our padlock, we 3D printed its body and shackle separately, as well as a holster to ensure stability for the shackle. To move the shackle up and down, we used a micro servo motor, which was connected to an Arduino Nano 33 BLE [1]. This can be seen in Figure 2. Using an Arduino sketch, we configured the servo motor to move 60 degrees to push the shackle up and down. To push the shackle using the motor, a small peg was attached to the arm of the motor and the side of the shackle.

The application and Arduino were connected via Bluetooth, which was established as soon as the user opened the application. To initiate the opening and closing of the padlock, a command from the application was sent to the Arduino when the user finished their tasks. Hereafter, the servo motor moved the shackle down to lock the padlock, and moved up again after a fixed weekly interval.

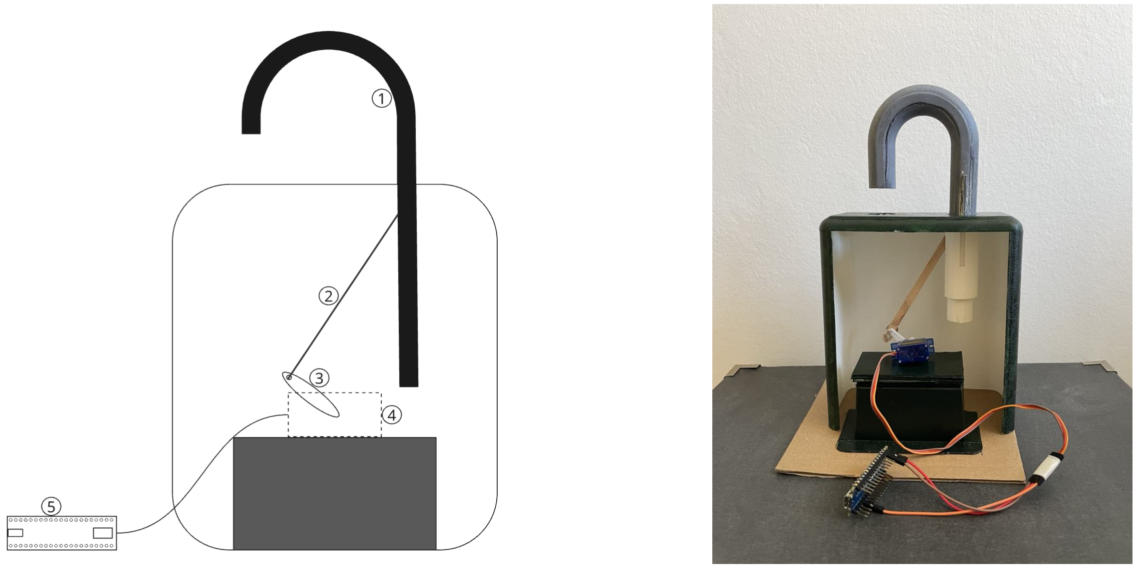

Fig. 2: Setup of Padlock: 1) Shackle, 2) Peg to connect motor and shackle, 3) Arm of servo motor, 4) Servo motor, 5) Arduino Nano 33 BLE board

6 Evaluation

We conducted a user evaluation [33] to gain insights into whether LockEd could support awareness of IT security among IT managers. The evaluation was conducted with the production company (I6) from the initial interviews. Here, we had observed that they delegated responsibility, which made them a relevant case. The test setup involved placing the system in the company’s office for one and a half weeks. We installed the system on a Friday, with the padlock intentionally left open, ready for use the following Monday. The participant was instructed to interact with the system twice. During the first interaction, a slight technical issue occurred, resulting in a delay in the padlock locking. However, after the participant had concluded the second set of tasks, the padlock locked as expected, providing instant feedback. During the testing period, the participant had to use LockEd independently, as we were not physically present. To ensure successful interaction with LockEd, we provided a step-by-step guide for the participant. We also provided the participant with a sheet of follow-up questions to support recall of thoughts or experiences, as the test period spanned just over a week.

Following the test period, we conducted a semi-structured [24] follow-up interview with the participant, which was later transcribed. The purpose was to explore the participant’s overall experience of using LockEd.

6.1 Evaluation Results

Engagement

In general, the participant expressed a very positive view of the system, stating that *”[...] I think it’s [using the system] a lot of fun with that, so I could do it [on a weekly basis]. I was actually kind of looking forward to Monday, and I was going to start again to see what would happen.”* This shows a high level of engagement with the system and a sense of anticipation. They emphasised that it was fun and sparked their interest in a way that an e-mail, for example, with the same questions would not.

Another important point from the interview was that the physical and tangible system increased the participant's engagement. For example, they were curious about the design itself: *"I was a bit curious if it closed the shackle or not. [...] It was a fun gimmick."* The quote highlights how a physical design can create engagement by including something interactive. Further, it is supported by the statement: *"Yes, I could have played with it a bit to see how it goes up and down. I've restrained myself and stayed away from it."* This illustrates how the design's tactile and mechanical elements sparked the participant's curiosity and encouraged involvement. Furthermore, the physical interface made the content more memorable. When asked about the physical design, they expressed that: "*I certainly remember it.*" This suggests that the tangible design helped make the experience more memorable and easier to recall compared to a purely digital solution.

Convenience and Accessibility

The participant expressed a clear interest in interacting with the system, noting that *"It wouldn't have mattered if there had been 3-4 more questions."* This highlights that the interaction with the system was not perceived as too time-consuming. According to the participant's assessment of the tasks' level of difficulty, they were suitably challenging. While using LockEd, the participant answered three of the four multiple-choice questions correctly. When asked if the tasks were too easy, they stated that *"I don't think it was too easy. You still had to think."*. This indicates that the participant regarded the tasks as appropriately difficult and sparked awareness of cyber security topics.

General IT Knowledge

In general, the participant's interaction with the system has sparked a positive interest and awareness of IT security. They stated: "*I've seen it. I've been thinking about what are the next questions. [...] But I also think that if you keep getting questions, I think you'll think about it more.*" This indicates that they have reflected more about IT security, and suggests that they could benefit from having the system integrated into their daily routines. The participant also expressed that the system supported learning: *"Yes, the one I got wrong, I learned something new."* This suggests that the tasks were not too easy, as the participant encountered content providing new knowledge.

Another insight from the interview was the importance of the feedback and explanations of the answers. As the participant expressed: *"[...] the first time I was a little doubtful that it was right. Then I wanted to see why it was right."* This indicates that the participant needed to be validated in their answers, both when they were correct and when they were wrong. This validation was an important factor in their learning, underscoring the importance of feedback in the learning process.

In addition to the IT manager's personal use, the participant discussed the idea of sharing the system with other employees. They mentioned that " *We always open or not always open, but many times you just open an email and take a look. I think in some way it's healthy to get a refresher or a little reminder of how things work behind the scenes in relation to IT and IT security, which you don't normally think about.*". Therefore, the employees would also benefit from learning more about IT security. However, according to the participant, sharing this information can be difficult, as merely sending employees an email or a piece of paper does not compel them to spend time learning about IT security. Additionally, the participant felt that the physical design could help facilitate knowledge sharing among other employees.

7 Discussion

Considering cyber security and the growing demands on organisations to ensure best practices (Cyber security expert, interview 03.03.25), SMEs find themselves in a difficult position; regulatory demands and increasing vulnerability, whilst lacking resources and capital to combat this [21]. Therefore, outsourcing is a solution for many SMEs to help mitigate this challenge and bring in much needed IT expertise [9]. However, research is lacking on how outsourcing can influence attitudes toward cyber security among those responsible for IT in SMEs, reflected in the research question for this paper: *"How does outsourcing of IT influence IT managers' attitudes toward cybersecurity in Danish SMEs?"*. Interviews with seven IT managers in Danish SMEs revealed how cyber security is managed and regarded in practice. Many IT managers have a wide range of responsibilities beyond managing IT, and often feel unsure or unknowledgeable about what and how their security providers handle their IT, for example, in regard to their backups, firewalls, etc. (I1, I3, I6). Through narratives explaining how the business would respond in the case of a critical cyber attack, many managers felt that the third party providers should fully handle the attack, with limited measures taken by the SME themselves. A lack of IT expertise was found to be a contributor to these responses, where one manager felt that *"There are some people [IT provider] who are a bit better than me."* (I6). This negation of responsibility due to a lack of expertise, can be related to the concept of responsibility diffusion [2], where Aschwanden et al. (2024) found that cyber security responsibility can be shifted due to a psychological response, where responsibility is given to others, as more actors are involved [3]. Our analysis found that IT managers tend to lack accountability for their IT in the event of a cyber attack and often turn to their service providers, thereby shifting the responsibility outside of their own business. However, the diffusion of responsibility in this case appears not only to lie in the presence of the providers, but a lack of expertise and insecurity also seems to contribute. This finding suggests that a lack of expertise can contribute to responsibility diffusion among SMEs, where Aschwanden et al. (2024) attribute the issue to the absence of defined roles and areas of responsibility, overlooking the role of knowledge. The diffusion of responsibility due to a lack of internal IT competencies among IT managers, and uncertainty about how security providers handle IT for SMEs, we argue, can be an influence of outsourcing cyber security in SMEs.

LockEd demonstrated how engagement with a tangible design may increase interest in learning about IT security. Furthermore, in addition to expressing curiosity about the physical padlock, our evaluation revealed that the participant had gained new knowledge about IT and security by using the system. This finding prompts further questions about the potential long-term effects on IT knowledge and responsibility. It suggests that increasing IT expertise in this manner may foster a stronger sense of ownership over IT security.

Relating back to the tangible design of the padlock, it appeared to foster increased interaction and curiosity. This could show that in settings where there is an abundance of digital stimulation, tangible visual interfaces can provide feedback to users [23]. This feedback was, in our case, manifested in a physical representation, for when a task is completed and when another needs to be solved. For example, had the system merely been implemented as a standalone app, it might have been lost in the digital clutter already present in an office environment. This finding can be related to a post-pandemic preference for physical over digital tools [35]. As many workplaces have become more digitally oriented following COVID-19, there may now be a renewed appreciation for tangible systems that can break the monotony of screen-based interaction. Reintroducing physical elements could therefore serve both practical and psychological purposes.

7.1 Limitations

A limitation of our evaluation results lies in the limited number of participants and the short duration of the evaluation. LockEd was only tested with one participant, who used the system twice. While the results are promising and offer an interesting starting point for further research, broader testing involving multiple participants and longer-term testing would be necessary to draw more concrete conclusions about the effects on IT knowledge and responsibility. Additionally, questions can be raised about the longevity of the system's novelty and its potential for engagement. While our participant currently described LockEd as 'fun' and evoking curiosity, it remains uncertain whether this interest will persist over time or diminish.

Despite these limitations, our design succeeded in creating a very positive response from the participant, who enjoyed using LockEd and would have been willing to spend more time with the system; a testament to the engagement and curiosity the design can create.

7.2 Future Research

An important takeaway for future research is the importance of testing with a wider range of participants [33]. As the system aims to promote awareness among IT managers and provide them with knowledge, it would also be necessary to conduct evaluations over longer time periods, as this may show how learning is improved over time [14]. Further testing would allow us to gain more information about how the system is perceived, specifically in regard to engagement and novelty. In the long run, it could also be possible to learn more about how increasing IT security knowledge can help lessen the responsibility diffusion in SMEs. Another avenue for further research could be exploring the sharing of LockEd with other employees. Currently, the IT manager bears the full IT responsibility, but sharing the system with other employees could help engage them more in IT security practices. In our evaluation interview, the participant noted that they sometimes forget to communicate and share IT security-related information with other employees. This could suggest that sharing the system could help alleviate some of the workload for IT managers and share IT security information in a manageable and time-efficient format.

To involve the third party providers more and increase knowledge of their practices, future iterations could include them in the design of the tasks and content in LockEd. In this way, SMEs could learn more about the specific practices taking place in their third party providers, perhaps lessening the insecurity many managers feel about how IT is managed among their providers.

8 Conclusion

In this paper, we have sought to understand how attitudes toward cyber security among IT managers are influenced by outsourcing IT security in Danish SMEs. Through interviews with seven IT managers, we discovered that they often have the sole responsibility for cyber security, whilst also holding other roles in the businesses. Additionally, we found that this combination of responsibilities internally meant that IT managers often lack time to allocate to IT management. Along with the lack of time, IT managers felt that they lacked IT expertise and were therefore very dependent on their external providers. This lack of expertise, along with dependency and insecurity, resulted in a tendency to diffuse responsibility to external security providers. This negation of responsibility could be problematic in the case of an attack on themselves or their providers. Specifically, it could prevent the SMEs from controlling how their security is handled (e.g. sensitive data handling) while still being liable in the event of a breach. Although some literature suggests that this diffusion can be combated by defining roles [2], we find that supporting awareness and increasing expertise could help alleviate the insecurity many IT managers feel, potentially allowing them to take on more responsibility in the future. To explore this, we developed a tangible design to promote awareness of IT security.

A preliminary evaluation with an IT manager found that such a design can have a positive effect in supporting awareness of a digital topic like cyber security through a physical representation. While our discussion found that the design succeeded in creating an interest and curiosity in IT security, our findings were limited by the short evaluation time and involvement of only one participant. Although our design showed promise in promoting awareness about cyber security, future research should investigate how the interest in tangible designs can be retained and whether supporting awareness can help IT managers take on more responsibility for their cyber security.

References

1. Arduino Docs. n.d. Nano 33 BLE. Accessed 28-05-2025. https://docs.arduino.cc/hardware/nano-33-ble/
2. Aschwanden, Rahel, Claude Messner, Bettina Höchli, and Geraldine Holenweger. 2024. "Employee behavior: the psychological gateway for cyberattacks". Organizational Cybersecurity Journal: Practice, Process and People 4 (1): 32–50. https://doi.org/10.1108/OCJ-02-2023-0004
3. Beyer, Frederike, Nura Sidarus, Sofia Bonicalzi, and Patrick Haggard. 2017. "Beyond selfserving bias: diffusion of responsibility reduces sense of agency and outcome monitoring". Social cognitive and affective neuroscience 12 (1): 138–145. https://doi.org/10.1093/scan/nsw160
4. Braun, Virginia, and Victoria Clarke. 2006. "Using thematic analysis in psychology". Qualitative Research in Psychology 3 (2): 77–101. https://doi.org/10.1191/1478088706qp063oa
5. Bryman, Alan. 2016. "Sampling in Qualitative Research". Chap. 18 in Social Research Methods, 5th ed. Oxford: Oxford University Press
6. Chaudhary, Sunil, Vasileios Gkioulos, and Sokratis Katsikas. 2023. "A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises". Computer Science Review 50 (3). https://doi.org/10.1016/j.cosrev.2023.100592
7. Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. "Defining Cybersecurity". Technology Innovation Management Review 4 (10). https://doi.org/10.22215/timreview835
8. Emborg, Rasmus. 2022. Cyberangreb kan blive en dyr omgang for SMV'erne. Accessed 12-02-2025. https://smvdanmark.dk/analyser/temaanalyser/cyberangreb-kan-blive-en-dyr-omgang-for-smverne
9. Erhvervsstyrelsen, Deloitte for Monitor. 2018. IT-sikkerhed og datahåndtering i danske SMV'er. Accessed 29-05-2025. https://erhvervsstyrelsen.dk/sites/default/files/2019-03/it-sikkerhed_og_datahaandtering_i_danske_smver.pdf
10. Feng, Nan, Yufan Chen, Haiyang Feng, Dahui Li, and Minqiang Li. 2020. "To outsource or not: The impact of information leakage risk on information security strategy". Information & Management 57 (5). https://doi.org/10.1016/j.im.2019.103215
11. Flutter. n.d. Flutter Frontpage. Accessed 28-05-2025. https://flutter.dev
12. Flutter Docs. n.d. Intro to Dart. Accessed 28-05-2025. https://docs.flutter.dev/get-started/fundamentals/dart

13. GDPR-Info.eu. n.d. General Data Protection Regulation (GDPR). Accessed 02-06-2025. https://gdpr-info.eu/

14. Godwin, Karrie E., Howard Seltman, Ma Almeda, Mandi Davis Skerbetz, Shimin Kai, Ryan S. Baker, and Anna V. Fisher. 2021. "The elusive relationship between time on-task and learning: not simply an issue of measurement". In Educational Psychology (Dorchester-on-Thames), 41(4), 502–519. https://doi.org/10.1080/01443410.2021.1894324

15. Harsch, A., S. Idler, and S. Thurner. 2013. "Assuming a State of Compromise: A Best Practise Approach for SMEs on Incident Response Management". In Eighth International Conference on IT Security Incident Management and IT Forensics, 76–84. https://doi.org/10.1109/IMF.2014.13

16. Hornecker, Eva. 2011. "The Role of Physicality in Tangible and Embodied Interactions". Interactions 18 (2). https://doi.org/10.1145/1925820.1925826

17. Ilca, L.F., O.P. Lucian, and T.C. Balan. 2023. "Enhancing Cyber-Resilience for Small and Medium-Size Organizations with Prescriptive Malware Analysis". Detection and Response Sensors 2023 23 6757. https://doi.org/10.3390/s23156757

18. Johnsen, Jarle Nordby, and Christian Kittilsen. 2022. "Outsourcing and its Influence on Cybersecurity in SMEs: An Exploratory Study in Norwegian Context". https://hdl.handle.net/11250/3033951

19. Jovchelovitch, Sandra, and Martin W. Bauer. 2000. "Narrative Interviewing". In Qualitative Researching with Text, Image and Sound: A Practical Handbook, 57–74. London: Sage

20. Junior, C. R., I. Becker, and S. Johnson. 2023. "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity". https://doi.org/10.48550/arxiv.2309.17186

21. Kappe, M., R.-C. Härting, C. Karg, and D. Deffner. 2023. "Cybersecurity in SMEs – Drivers of Cybercrime, Insufficient Equipment and Prevention". Procedia Computer Science 225. https://doi.org/10.1016/j.procs.2023.10.358

22. Kocksch, Laura, and Torben Elgaard Jensen. 2024. "The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small- and Medium-Sized Enterprises". Proceedings of the ACM on Human-Computer Interaction. https://doi.org/10.1145/3686893

23. Krestanova, Alice, Martin Cerny, and Martin Augustynek. 2021. "Review: Development and Technical Design of Tangible User Interfaces in Wide-Field Areas of Application". Sensors 21 (13). https://doi.org/10.3390/s21134258

24. Kvale, Steinar, and Svend Brinkmann. 2015. Interview: Det kvalitative forskningsinterview som håndværk. 3. udgave. København: Hans Reitzel

25. Lair, Craig D. 2012. "Outsourcing and the Contracting of Responsibility". Sociological Inquiry 82 (4). https://doi.org/10.1111/j.1475-682X.2012.00419.x

26. López, Miguel Ángel, Juan Manuel Lombardo, Mabel López, Carmen María Alba, Susana Velasco, Manuel Alonso Braojos, and Marta Fuentes-García. 2020. "Intelligent Detection and Recovery from Cyberattacks for Small and Medium-sized Enterprises". International Journal of Interactive Multimedia and Artificial Intelligence 6 (3). https://doi.org/10.9781/ijimai.2020.08.003

27. Nero, Richard L. 2018. "Risks, Benefits, and Perceived Effectiveness of Outsourcing IT Network Security in Small Businesses: A Multiple-Case Study". https://www.proquest.com/dissertations-theses/risks-benefits-perceived-effectiveness/docview/2039579703/se-2

28. Nis 2 Directive. n.d. The NIS 2 Directive — Updates, Compliance. Accessed 02-06-2025. https://www.nis-2-directive.com

29. Renaud, Karen, Rosaling Searle, and Marc Dupuis. 2021. "Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?". In New Security Paradigms Workshop 2021. ACM. https://doi.org/10.1145/3498891.3498896

30. Sampson, Helen, and Idar Alfred Johannessen. 2020. "Turning on the tap: the benefits of using 'real-life' vignettes in qualitative research interviews". Qualitative research : QR 20 (1): 56–72. https://doi.org/10.1177/1468794118816618

31. Schiliro, Francesco. 2023. "Towards a Contemporary Definition of Cybersecurity". https://doi.org/10.48550/arxiv.2302.02274

32. Shaer, Orit, and Eva Hornecker. 2009. "Tangible User Interfaces: Past, Present, and Future Directions". Foundations and Trends in Human-Computer Interaction 3: 1–137. https://doi.org/10.1561/1100000026

33. Sharp, Helen, Jennifer Preece, and Yvonne Rogers. 2019. "Introducing Evaluation". Chap. 14 in Interaction Design: Beyond Human–Computer Interaction, 5th. Wiley

34. Veale, Michael, and Ian Brown. 2020. "Cybersecurity". Internet Policy Review 9 (4). https://doi.org/10.14763/2020.4.1533

35. Zaban, Roy, and Pnina Plaut. 2024. "The relationship between activities performed in the physical and digital spheres: Lessons learned from the COVID-19 pandemic". Sustainable Cities and Society 106:105370. https://doi.org/https://doi.org/10.1016/j.scs.2024.105370

36. Zhou, Nianmei, Steven Devleminck, Luc Geurts, Jonas Fritsch, Christopher A. Le Dantec, Anna Vallgårda, Li Jönsson, and Sarah Fdili Alaoui. 2024. "Tangible Affect: A Literature Review of Tangible Interactive Systems Addressing Human Core Affect, Emotions and Moods". In Proceedings of the 2024 ACM Designing Interactive Systems Conference, 424–440. https://dl.acm.org/doi/10.1145/3643834.3661608

Note: The interview guide, transcriptions of all interviews, the analysis codes and themes, and the Arduino sketch can be found in the attached zip file. The code for the application can be found in the Github repository: https://github.com/NadjaDH/LockEd