Guarding Against Social Engineering Threats: Assessing the Cybersecurity Awareness Impact of Mystery Guest Audits

Jelle Habraken

Master of Information Management (MSc IM)
Faculty of Economics and Business Administration
Tilburg university

SNR: 2108652
Email: j.h.habraken@tilburguniversity.edu

Supervisor:
Prof. dr. Anne-Francoise Rutkowski

Second reader:
dr. Soreangsey Kiv

June 2024

Abstract
This study explores the impact of mystery guest audits on cybersecurity awareness within public sector organisations. The rapid advancement in cybersecurity measures has not fully mitigated human vulnerabilities, with social engineering attacks, such as phishing and tailgating, posing significant threats. Mystery guest audits, involving covert operatives simulating social engineering attacks, provide a practical means to evaluate and enhance organisational security awareness. This research aims to determine the effectiveness of these audits in improving cyber awareness and organisational behaviour towards security. A qualitative multiple case study methodology was employed, focusing on three public sector organisations. Data collection involved two rounds of mystery guest audits, semi-structured interviews with employees and supervisors, and analysis of internal documents. The findings indicate that mystery guest audits significantly enhance employees' cybersecurity-related behaviours. Employees reported increased vigilance and adherence to security protocols, particularly concerning clean desk policies and unauthorised access prevention. The study identified critical factors influencing cybersecurity awareness, including formal controls (e.g., documented policies and training) and informal controls (e.g., cyberculture and peer influence). Formal control recommendations from the audits were particularly effective in fostering a disciplined security environment. However, challenges persist in consistently implementing physical security measures and overcoming social barriers to questioning unfamiliar individuals. The results underscore the necessity for continuous and comprehensive security training programs, integrating both technical and human-centred approaches to effectively mitigate social engineering threats. The findings contribute to the broader field of cybersecurity by providing empirical evidence on the benefits of mystery guest audits, advocating for their inclusion in organisational security strategies to enhance overall resilience against social engineering attacks.

Keywords: Cybersecurity, Social Engineering, Mystery Guest Audits, Cyber Awareness, Public Sector, Physical Controls, Formal Controls, Informal Controls.

Contents

1. INTRODUCTION 5
1.1 PROBLEM INDICATION 5
1.2 PROBLEM STATEMENT 6
1.3 RESEARCH QUESTION 7
1.4 RESEARCH METHOD 8
2. THEORY 9
2.1 CYBER AWARENESS 9
2.1.1 Delivery Methods 10
2.2 CONTROL FACTORS 11
2.2.1 Physical 11
2.2.2 Formal 12
2.2.3 Informal 13
2.3 SOCIAL ENGINEERING 15
2.3.1 (Spear)Phishing 16
2.3.2 Physical Attacks 17
2.3.3 Mystery Guest 17
2.4 PROPOSITIONS 18
2.5 CONCEPTUAL MODEL 20
3. METHODOLOGY 21
3.1 PUBLIC SECTOR 21
3.2 DATA COLLECTION 22
3.3 PARTICIPANTS 23
3.4 PROCEDURE AND PROTOCOL 24
3.4.1 New Mystery Guest Clients 24
3.4.2 Repeated Mystery Guest Clients 25
3.5 INTERVIEW GUIDE 26
3.6 DATA ANALYSIS 27
4. RESULTS 28
4.1 INTERVIEWS 28
4.1.1 Awareness Refreshment 28
4.1.2 Communication Error 28
4.1.3 Difficult to Adhere 29
4.1.4 Formal Controls 30
4.1.5 Informal Controls 30
4.1.6 Physical Controls 31
4.1.7 Change in Awareness 32
4.1.8 Independent Initiatives 32
4.2 MYSTERY GUEST VISIT 33
5. DISCUSSION 34
5.1 POSITIVE INFLUENCE OF MYSTERY GUEST AUDITS ON CYBERSECURITY BEHAVIOUR (P1) 34

5.2 FORMAL CONTROLS (P2) 34
5.3 INFORMAL CONTROLS (P3) 35
5.4 PHYSICAL CONTROLS (P4) 36
5.5 COMMUNICATION CHALLENGES AND SOLUTIONS 38
5.6 INDEPENDENT INITIATIVES 38
5.7 CONCLUSION 39
6. CONCLUSION 40
6.1 KEY FINDINGS 40
6.2 CONCLUSION 41
6.3 LIMITATIONS 42
6.4 FUTURE RESEARCH 42
6.5 RECOMMENDATIONS 43
7. REFERENCES 46
8. APPENDIX 52
8.1 APPENDIX I, COMPANY INFORMATION 52
8.2 APPENDIX II, FLYER MYSTERY GUEST VISIT 53
8.3 APPENDIX III, INTERVIEW GUIDE 54
8.4 APPENDIX IV, CODED INTERVIEW TABLE 54
8.5 APPENDIX V, MYSTERY GUEST VISITS 57

1. Introduction

1.1 Problem Indication

Cybersecurity is a discipline that is expanding quickly. While the efficacy of security protocols to safeguard confidential data is rising, human vulnerability continues to be the weakest link in the security hierarchy (Duman et al., 2023), thus technology by itself is rarely a sufficient defence against information theft. A common organisational threat is social engineering, which exploits human vulnerabilities by means such as deception, manipulation, influence, and inducement to get classified information, hack computer systems and networks, or obtain unauthorised access to restricted areas (Wang et al., 2021). Attacks using social engineering techniques are becoming a more serious security risk (Bakhshi et al., 2009). According to reports from ISACA's State of Cybersecurity, social engineering is the top cyber threat for organisations from 2016 to 2018 (Wang et al., 2020). Furthermore, social engineering attacks were experienced by 85% of organisations in 2018 which is an increase of 16% over one year. These attacks have also risen to an annual cost of 1.4 million (Broadhead, 2018). As technological advances progress, perpetrators of social engineering are progressively employing advanced tools like artificial intelligence (AI) to manipulate their targets effectively(Kaur et al., 2023). With the use of Artificial intelligence Kaloudi and Li (2020) expect future cyber-attacks to be smarter, more powerful, and more likely to create scalable impact by causing a high level of cascading damage.

There are numerous social engineering techniques to orchestrate an attack for example phishing, spear phishing, whaling, pretexting, baiting, tailgating, etc (Krombholz et al., 2015). Phishing is the most common social engineering attack where fraudulent emails or messages that appear to be from a legitimate source are sent to trick individuals into revealing sensitive information(Roy et al., 2022). The tailgating technique is a lesser-used method that involves an in-person interaction by gaining physical unauthorised access to a restricted area (Roy et al., 2022). This tailgating technique was used in 2017 by Ankur Agarwal to physically breach two companies and then install keyloggers on machines to capture employee login credentials. This allowed him to access and steal over 15,000 files related to emerging technology. Agarwal first broke into a company in February 2017, placing hardware keyloggers to gather login information. He then used this access to plant additional keylogging software, exfiltrating sensitive data over several months. He repeated this method in a second company, successfully obtaining and stealing valuable data. The case underscores the critical need for robust physical security and the ability to detect data exfiltration within organisations (Brook, 2019). This case shows that physical security and awareness are necessary to prevent unauthorised individuals from accessing critical infrastructure and sensitive information. Without adequate physical security, even the most advanced technical controls can be bypassed by malicious actors who gain physical access to sensitive areas or equipment (Satvat et al., 2018).

Despite the importance of physical controls, academic research often places more emphasis on technical security measures. Technical controls such as firewalls, encryption, and intrusion detection systems receive significant attention because they directly protect the digital infrastructure against cyberattacks (García et al., 2021). However, physical security measures like access controls, surveillance systems, and secure environments are equally essential for ensuring the integrity and safety of these systems (Disterer, 2013).

To protect against the potential threats of social engineering, it is essential to have employees who are cyber-aware and maintain both formal and informal physical controls (Aldawood & Skinner,

2018; Brody et al., 2012). Cyber awareness is a critical component in defending against these attacks, as it empowers employees to recognise and respond appropriately to social engineering attempts (Aldawood et al., 2020). To test organisations on their cybersecurity BDO uses a mystery guests audit technique which contains all sorts of physical social engineering methods. BDO believes that the mystery guest audit will bring valuable awareness to their client's organisations. However, the problem is that there is no actual evidence of the impact these tests have on the organisations. Understanding the impact of these tests will allow BDO to improve their awareness proposition and deliver a more specific follow-up plan for cyber awareness within the client's company. Furthermore, there is a lack of academic research on how physical social engineering attacks, such as tailgating, affect organisational cyber awareness compared to more researched technical methods like phishing audits. This gap highlights the need for studies examining the unique impacts of physical security breaches.

1.2 Problem Statement

During the mystery guest audits, BDO employs techniques like tailgating in combination with impersonation to enter the client's buildings unauthorised. When inside, the mystery guest wears a concealed camera to capture and document critical information within the organisation. After the intrusion, BDO creates a full report, including a video explaining the process the mystery guest took and recommendations to counter possible cyber threats. The most common recommendations focus on clear screen and clean desk policies (formal controls), accessibility of rooms (physical controls), and fostering a speak-up culture (informal controls). However, there is a major gap in the post-assessment phase, with no ongoing evaluation and analysis to identify the true impact and effectiveness of the applied security measures. The sheer value and impact on the cyber awareness of the mystery guest audit is therefore unknown. Public organisations are for BDO the most common clients for this audit. This shows that the importance of cybersecurity and privacy has grown dramatically for governments and public administration (Dawes, 2008). Even though the acknowledgement of importance has grown, studies indicate a lack of cybersecurity awareness among public employees and supervisors (Stibbe, 2005; Conklin & White, 2006; Smith & Jamieson, 2006). By analysing public sector organisations, this study aims to highlight the gap and importance of comprehensive security audits, including physical controls, to enhance cyber awareness and protect sensitive information.

The academic field reveals a significant gap in the study of physical attacks like tailgating, impersonation, piggybacking, etc. as social engineering techniques. Unlike more extensively researched methods such as phishing (technical), physical attacks have received little to no attention in academics. This lack of scholarly focus highlights a considerable gap in knowledge and understanding, making it challenging for organisations to measure their vulnerability against existing best practices or tailgating-specific standards. While the impact on awareness from technical social engineering audits, like phishing, has been well-documented (Chatchalermpun & Daengsi, 2021), the effect of physical social engineering attacks on cyber awareness remains largely unexplored.

The absence of literature regarding the impact that physical controls have on cyber awareness makes it impossible to know the best possible way to educate people on awareness. Moreover, understanding the strength these different types of social engineering audits have, both physical and technical, on employee cyber awareness is essential. This understanding can significantly contribute to enhancing the resilience of organisations against a diverse array of threats. Furthermore, knowing the impact that this mystery guest audit creates on cyber awareness helps in

developing a holistic approach to security. Knowing the impact that physical controls have on employees broadens the scope of cybersecurity research and promotes an integrated perspective that considers all facets of security. Understanding the effectiveness of different types of social engineering attacks can lead to the development of more targeted and effective training programs. Academically, this can enrich the curriculum of cybersecurity courses by incorporating findings from real-world comparative studies. Practically, organisations can use these insights to design training that better prepares employees for both physical and technical social engineering attacks.

This lack of academic scrutiny further exacerbates the need for BDO and other comparable organisations to take a more comprehensive and long-term approach to security evaluations. The lack of research on physical attacks not only restricts the development of effective countermeasures but also highlights the importance of continuous monitoring and evaluation tailored to this unique social engineering method. Addressing this gap in both industry practices and academic research is critical for several reasons. First of all, understanding the true impact of mystery guest audits helps improve organisations' overall cybersecurity resilience and awareness in the face of a growing landscape of security threats. Also, it enables organisations to assess the effectiveness of their current security measures and make informed decisions about necessary improvements.

1.3 Research Question

The main research question is:

"How do mystery guest audits enhance the cyber awareness and organisational changes in public sector organisations?"

To address the main research questions these three research questions have been formed:

- RQ1: Which factors (e.g. formal controls, informal controls, physical controls) influence cyber awareness within public sector organisations?
- RQ2: How do mystery guest audits influence employees' cybersecurity awareness?
- RQ3: Which control recommendation from the mystery guest or independent initiatives influences the cyber awareness within public sector organisations?

1.4 Research Method

This research consists of a literature review and a qualitative multiple case study. The literature review will dive deeper into the definition and mechanism of cyber awareness, informal controls, formal controls, physical controls, and social engineering. The literature will therefore help with answering RQ1:

Which factors (e.g. formal controls, informal controls, physical controls) influence cyber awareness within public sector organisations?

When the literature review is finished and the theoretical background of the important subjects of this research are identified a multiple case study will start. Based on the principles outlined by Stake (1994) on the multiple case study method, this research employs a qualitative case study approach to comprehensively investigate the impact of mystery guest audits on organisational cyber awareness. By closely examining three public sector organisations, the study provides an intensive analysis of changes in cyber awareness and security practices resulting from the mystery guest audits. This approach is particularly suited because it utilises observations, interviews, and document reviews as data-gathering tools. The observation method will be implemented through a second mystery guest visit. This visit will assess the organisation's controls and determine if any changes have been made since the initial audit. After the audit, semi-structured interviews will take place to examine the effect of the mystery guest and controls on the cyber awareness of employees. By following this methodology the following research questions will be answered:

RQ2: How do mystery guest audits influence employees' cybersecurity awareness?
RQ3: Which control recommendation from the mystery guest or independent initiatives influences the cyber awareness within public sector organisations?

2. Theory

This literature review explores cyber awareness, focusing on delivery methods and control factors (informal, formal, and physical). It also examines social engineering and the role of mystery guest audits in cybersecurity strategies. To gather relevant articles, research was conducted using Scite.io, Google Scholar, Tilburg University WorldCat, and ChatGPT. This approach helps find comprehensive cybersecurity strategies that enhance awareness, strengthen controls, and mitigate social engineering risks.

2.1 Cyber Awareness

The term cyber awareness is defined as "the degree of understanding of users about the importance of information security and their responsibilities and act to exercise sufficient levels of information security control to protect the organisation's data and networks" (Zwilling et al., 2020). Cyber awareness is a crucial component in an organisation, involving understanding potential cyber threats and taking necessary steps to reduce these risks. Organisations are increasingly investing in tackling these threats by implementing cybersecurity training programs to enhance the awareness among employees(Hart et al., 2020). The human behaviour plays a crucial role in the enhancement of cyber awareness among employees because they are the central figures in cybersecurity(Kovačević et al., 2020). The employees are the first line of defence because they are responsible for adjusting their security guidelines, changing their privacy settings, and selecting secure passwords. Based on individuals' current awareness of online threats and the technology they use, these decisions demand thoughtful consideration, foresight, and trade-offs. Consequently, increasing the understanding and awareness of non-expert end users is a crucial first step towards cybersecurity (Zhang-Kennedy & Chiasson, 2021). Moreover, the human element is recognised as a key factor in cybersecurity threats, with hackers exploiting the vulnerabilities and a lack of awareness of staff (Aldawood et al., 2020). This shows the importance of cyber awareness training for employees, noting that well-informed employees act as the first line of defence against cyber-attacks (Corradini & Nardelli, 2018).

The growing demand for cyber awareness remains a very important area, and more so in the very area of research focused on knowledge and behaviour change to reduce the chances of risk posed by cyberspace (Zwilling et al., 2020). Recent literature highlights the differences between awareness and behaviour, pointing out that although people tend to perceive the threats the mitigation efforts for these remain inadequate(Kovačević et al., 2020). This discrepancy underscores the critical need for an effective cyber awareness program that not only increases employees' recognition of cyber threats but also ensures they take appropriate actions to mitigate these risks.
Tirumala et al. (2019) conducted the research and argued that a comprehensive awareness program could significantly help develop improved protective behaviour, especially when it is designed with specified target audiences. However, a gap is there in understanding the effectiveness of such programs and how can these change in line with rapidly changing cyber threats.

2.1.1 Delivery Methods

The effectiveness of cybersecurity awareness programs in organisations significantly depends on the choice of delivery methods. Cybersecurity awareness programmes within organisations are not designed to create fear or apprehension but to equip them with contingency plans against cyber-attacks. It serves as a critical platform for disseminating information about emerging cybersecurity threats (Choo, 2011). An organisation's knowledge of cybersecurity is crucial to effectively cope with new internet technologies, changes in organisational behaviour, and the extensive use of online services (Thomson & von Solms, 1998; Whitson, 2009). The effectiveness of a cybersecurity awareness program hinges on the clarity and understandability of the message it conveys. It is vital for these messages to target specific organisational audiences with precision and conciseness, engaging them with real-life examples and employing the most effective delivery methods (May, 2008). Examples of these real-life delivery methods can be mystery guest visits or an evaluation of clicked phishing links. Evidence shows that these methods as security awareness training are the most cost-effective form of security control (Albrechtsen and Hovden 2010).

The following section will examine different methods for delivering cybersecurity awareness within organisations:
Conventional methods, such as posters and newsletters, provide a basic yet essential means of communication. They are particularly effective in environments where they can be prominently displayed and updated regularly to capture the attention of employees with critical and timely information (Wilson & Hash, 2003). However, the static nature of these resources can limit their impact, underscoring the need for more dynamic and engaging approaches.

Instructor-led sessions, such as workshops and seminars led by cybersecurity experts, offer a more interactive experience. These sessions enable real-time feedback and adaptation to the audience's understanding, which can significantly enhance the learning experience. Despite their advantages, these methods are often costly and may not effectively address the constantly evolving landscape of cybersecurity threats due to their less flexible, scheduled nature (Valentine, 2006).

Online delivery methods have become increasingly popular due to their scalability and ability to reach a dispersed workforce. These include email broadcasts, interactive webinars, and multimedia content such as videos and animations, which can be tailored to different learning styles and preferences. Online platforms also facilitate ongoing updates and revisions, allowing organisations to respond quickly to new threats (Kumaraguru et al., 2007).

Moreover, emerging interactive methods like game-based and simulation-based training have shown great promise by combining education with engagement. These methods use realistic scenarios and gamification to not only impart necessary knowledge but also test users' responses to simulated cybersecurity incidents, providing a practical and impactful learning experience (Fung et al., 2008; Jagatic et al., 2007).

Each of these delivery methods has its strengths and limitations. Selecting the right combination can enhance the overall effectiveness of cybersecurity awareness programs, ensuring that they are not only informative but also compelling and relevant to the employees' daily responsibilities and the organisation's specific security needs (Abawajy, 2012).

2.2 Control Factors

Control is defined as any attempt to align individual behaviours with organisational objectives(Wiener et al., 2016). These controls are often implemented throughout organisations for security purposes to motivate employees to comply with the desired behaviour (Boss et al.,2009). Furthermore, controls refrain from policies, procedures, and technical measures implemented by organisations to manage cybersecurity risks (Framework For Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018b). Moreover, this chapter will dive deeper into the formal, informal, and physical controls each addressing different facets of cybersecurity.

2.2.1 Physical

Physical security is crucial for organisations due to various reasons supported by scholarly works. One key aspect highlighted in the literature is the role physical security plays in safeguarding an organisation's assets, both tangible and intangible (Satvat et al., 2018). Without adequate physical security, it becomes challenging to ensure the logical security of an organisation's information and resources(García et al., 2021). Physical security also acts as a deterrent to potential threats and intrusion thereby reducing the risk of unauthorized access and breaches (Disterer, 2013). To protect against the potential threats of social engineering, it is essential to have employees who are cyber-aware and maintain both formal and informal physical controls (Aldawood & Skinner, 2018) (Brody et al., 2012).

Physical security also has an essential role in the realm of cybersecurity due to the interconnected nature of cyber-physical systems (CPS). Cyber-physical systems are advanced systems that integrate computational technologies with physical processes and objects. These systems utilize computer networks and sensors to collect process data, facilitating the control and optimisation of physical machinery and infrastructure. CPS are vulnerable not only to cyber-attacks on data management and communication layers but also to physical infrastructure failures and attacks (Pasqualetti et al., 2013). To effectively protect cyber-physical systems, security concerns must be addressed across multiple layers of control design and embedded systems (Zheng et al., 2016). The integration of physical and cybersecurity strengths is crucial for ensuring the security and resilience of critical infrastructure like smart grids (He & Yan, 2016). By jointly addressing security in both cyber and physical domains, threats to cyber-physical systems can be promptly detected and mitigated (Rubio-Hernan et al., 2018).

The security of cyber-physical systems against cyber-attacks is a challenging yet crucial issue (Wang et al., 2019). Traditional security measures alone are insufficient, necessitating integrated security solutions that encompass all components within the cyber-physical systems network and operational scenarios (Alguliyev et al., 2018). Moreover, the development of cyber-physical systems is impeded by security and privacy threats arising from their open and interconnected network structure (Min et al., 2019). To prevent cyber-induced irreversible physical damage to cyber-physical systems, solutions like Trusted Security Modules (TSM) have been proposed to enhance resilience even in compromised operating systems (Yang et al., 2015).

The research by Mirza, Georgakopoulos, and Yavari (2023) highlights the integral role of physical controls within the broader framework of a Cyber-Physical-Social Awareness (CPSA) platform. The inclusion of physical components, particularly IoT sensors, is essential for monitoring and responding to changes in the physical environment, thus forming the backbone of effective situational awareness systems. These physical controls are not only pivotal in gathering real-time

data but also in ensuring the accuracy and reliability of the information that supports cyber and social awareness responses.

The CPSA platform detailed by Mirza et al. (2023) demonstrates that physical controls serve as critical points of data collection and actuation, directly influencing the system's ability to integrate and interpret diverse data streams from cyber and social sources. By reinforcing physical security measures with interconnected IoT devices, the platform ensures a robust defence mechanism that can proactively detect and respond to potential security breaches or environmental changes, thereby mitigating risks before they escalate into more significant threats.

This approach illustrates the vital importance of physical controls in maintaining comprehensive security and situational awareness. It emphasizes that without strong physical monitoring and response mechanisms, the effectiveness of cyber-physical-social systems could be compromised, underlining the need for continuous development and integration of advanced physical controls within security infrastructures. Research does not however acknowledge any correlation between physical control and the increase of awareness it provides.

2.2.2 Formal

Formal controls in cybersecurity refer to documented policies, standards, guidelines, and procedures established by an organisation to ensure the confidentiality, integrity, and availability of information systems and data (Kwak et al., 2021)(Khansa et al., 2017). These controls are typically mandated by organisational governance frameworks and are enforced through various mechanisms including access controls, password management, and incident response protocols (Ifinedo, 2012). Formal controls play a significant role in deterring cyber threats by instilling a fear of punishment, contributing to the overall cybersecurity strategy (Lee & Lee, 2021). These controls are often derived from established frameworks and standards such as COBIT®, CIS®, ISA/IEC 62443, ISO/IEC 27002, and NIST, providing a structured approach to cybersecurity management (Malatji & Solms, 2021). They help organisations define and update their IT strategies, conduct self-assessments, and ensure compliance with governance frameworks and budget controls (Islam et al., 2018). With the use of internal or external audits organisations can check and implement these frameworks but also check their legal compliance. Research indicates that auditors have demonstrated increased awareness of cybersecurity risks within organisations and are better able to implement procedures to manage the aftermath of cybersecurity incidents (Rosati et al., 2020). Moreover, audits help in identifying technology users who may not comply with formal cybersecurity policies, thereby enhancing enterprise risk management (Stafford et al., 2018).

Although organisations implement information security policies there are still users who do not fully comply with the policies (D'Arcy & Lowry, 2017). Not complying with the company's information security policies and unintentional or intentional leaking of confidential information can cause serious issues for all parties involved (Barlow et al., 2013). Research on cybersecurity has shown that security regulations do not always benefit employees (Han et al., 2017) (Ifinedo, 2012). Even when they receive written security policies and instructions, some employees tend to ignore the information security policies of their company, and others tend to underestimate the risks associated with information security.

Cybersecurity training is another form of formal control. Firstly, research indicates that cybersecurity training for employees is effective in reducing security incidents. A systematic literature review found that well-trained employees are less likely to fall victim to cyberattacks and

promote a culture of cybersecurity awareness (Tolossa, 2023). Additionally, empirical evidence suggests a negative relationship between the frequency of cybersecurity training and the number of incidents in organisations. This means that more and better-organised training leads to fewer cyber incidents (Kweon et al., 2019).

Furthermore, cybersecurity training through gamification, where employees learn through interactive and playful elements, has proven to be particularly effective in increasing knowledge and awareness. This not only enhances employee engagement but also improves their skills in recognising and responding to cyber threats (Nagarajan et al., 2012). Companies that invest in such training benefit from better protection of their networks and data. This not only reduces the number of attacks but also improves response and recovery during incidents, minimizing the impact of potential attacks (Buil-Gil et al., 2020). Although most studies show that cybersecurity training has a significant impact on an organisation's awareness Ng and Xu (2007) show that those who have received sufficient information security training do not always behave more cybersecurity-awarely.

In contrast to other research, Ahmad et al. (2015), Moon et al. (2018), and Ng et al. (2009) all show that an organisation's security management efforts are likely to guide employees in taking the right steps to protect against cyber threats and gain experience in dealing with cybercrime. Research from Li et al. (2019) shows that organisations with no explicit cyber security policy have lower opinions on their organisation norms and are less adaptive to cyber threats than employees of companies that have policies. The research also finds that information security policy awareness will have a positive effect on employees' beliefs about information security and information security protection behaviour(Li et al., 2019). But to achieve this positive effect formal controls need specification of desired behaviours or outcomes thus making it clear for the employees what to do in certain situations (Boss et al., 2009).

2.2.3 Informal

The dynamic landscape of cybersecurity necessitates not only formal control mechanisms but also the adoption of subtle, behaviour-influencing informal controls(Monteiro et al., 2022). These controls are embedded within the organisational culture and are crucial for the internalisation of cybersecurity best practices among employees, thereby reinforcing the organisation's overall cybersecurity framework. Informal controls in cybersecurity refer to the unstructured methods that influence employee behaviour towards enhanced security practices, including organisational culture, norms, peer influence, and leadership style (Kreutzer et al., 2016). These controls, although intangible, significantly contribute to shaping an organisation's security posture by fostering a proactive cybersecurity culture.

The security culture plays a pivotal role in safeguarding organisations against cyber threats. According to Da Veiga et al. (2020) a security culture can be defined as the social, cultural, and ethical measures implemented within an organization to enhance the security-related behaviour of its members. It is considered a subculture of the organisational culture, encompassing the thoughts, emotions, and daily activities of employees (Wen et al., 2019). Moreover, Da Veiga et al. (2020) elaborate that to have a sound information security culture, every employee should precisely understand and know the cause of the significance of information security, and how they should treat sensitive information. The better employees get knowledgeable on this subject, the better it is for the security culture as a whole within an organisation. At the same time, information security culture has a positive effect on employees' knowledge, attitude, and consequently behaviour (Vroom & Von Solms, 2004). According to Parsons et al. (2014), a strong and encouraging security

culture ensures that workers are well-protected at all organizational levels and that they can turn to their peers for assistance when needed. Workers' perceptions of the organisation's information security culture influence and align their information security behaviour (Da Veiga et al., 2020). Also, if co-workers act in good ways, and the practices of the whole of the organisation demonstrate the established security values, an organisation will be motivated to act in line accordingly (Leach, 2003). However, employees begin to make sure they don't comply when the upper management also disregards organisational practices and principles (Moody et al., 2018). That means the upper management has to set an example for the rest of the organisation. This way it can be suggested that organisations having a strong culture of information security also show compliance with existing policies (Da Veiga et al., 2020).

Boss et al. (2009) discuss that organisations can motivate individual information security behaviours through informal controls, focusing on the concept of 'mandatoriness'. 'Mandatoriness' is defined as the extent to which individuals perceive compliance with existing security policies and procedures to be compulsory or expected by organisational management. The study finds that specifying policies and evaluating behaviours are effective in convincing individuals that security policies are mandatory. If individuals believe that management is monitoring, they are likely to comply. This suggests that it is crucial for management to specify clear information security policies and evaluate behaviours to strengthen the perception of mandatoriness, thereby promoting compliance with information security measures.

Furthermore, employees are more likely to recognise and assess the severity of security threats when the organisational environment and IT security awareness are in alignment(Li et al., 2019). According to Ahmad et al. (2015), employees are better able to manage the conflict between experimenting with novel ideas for information security and making use of established procedures for information compliance when working in an organisational context. Users anticipate that compliance culture will benefit from the lessons learnt from security incidents, which makes this experience feature very helpful (Ahmad et al., 2015).

2.3 Social Engineering

In the context of cyber security, social engineering describes a type of attack in which the attacker exploits human vulnerabilities by means such as deception, manipulation, influence, and inducement to get classified information, hack computer systems and networks, or obtain unauthorised access to restricted areas (Wang et al., 2021). Research shows that social engineers could breach even those organisations that consider themselves knowledgeable about social engineering techniques (Grazioli, 2004). While these organisations recognise the serious risks associated with social engineering, they often have a limited understanding and control over these threats (Kvedar et al., 2010). This shortfall may be partly due to the complexity of human behaviour, which often fails to identify attackers (Algarni et al., 2017). Adding to the severity, recent data indicates that social engineering is not only prevalent but also significantly damaging. Currently, the biggest threats facing cybersecurity are social engineering attacks, with 84% of cyber-attacks reported to have also cost companies billions of dollars, far surpassing the financial impact of natural disasters (Senkyire & Kester, 2021). Social engineering attacks can lead to a wide range of financial costs for organisations, varying significantly depending on the nature and severity of the attack. The cost of an social engineering attack often go beyond financial loss, such as reputational damage and loss of customer trust (Tam et al., 2010). Some of the most common types of costs that organisations may incur following an social engineering attack are:

- **Ransom payments:** In a ransomware attack organisations may be forced to pay a substantial amount to regain access to their encrypted data. These payments can range from thousands to millions of dollars, depending on the value of the compromised information (Oz et al., 2022).
- **Data recovery cost:** Recovering lost or corrupted data can be a complex and expensive process. This includes the cost of employing data recovery specialists, restoring backups, and verifying the integrity of recovered data (Alshaikh et al., 2020).
- **Legal fines:** Depending on the jurisdiction and the nature of the data breach organisations may face legal penalties and regulatory fines (Kanter et al., 2021).
- **System reinstallation:** Organisations often need to reinstall compromised systems and software following an attack (Low, 2017). This involves technical work as well as the cost of downtime during which systems are unavailable.

As technological advances progress, perpetrators of social engineering are progressively employing advanced tools and techniques to manipulate their targets effectively. Among these tools, generative artificial intelligence (AI) has emerged as a significant area of focus, attracting considerable scholarly and industry attention in recent years (Kaur et al., 2023). Benefits for the cybersecurity domain is that AI enhances detecting threats faster, automating responses, and analysing vast amounts of data for vulnerabilities, ultimately improving protection and reducing the risk of cyberattacks (Kaloudi & Li, 2020). Research supports that AI-driven cybersecurity can make the cybersecurity process more automated and intelligent than conventional security systems, thus enhancing threat detection and response capabilities (Sarker et al., 2021). The use of AI is not only effective on improving systems and software but also the human behaviour. Phished.io for example is an AI-driven platform that focusses on the human side of cybersecurity. By combining fully automated training software with personalised, realistic simulations of cyberattacks, Phished teaches employees how to correctly and safely deal with online threats (Phished, 2021). As stated AI provides substantial benefits in identifying and mitigating social engineering threats. However with the malicious use of AI it increases the speed, success rate, and capabilities of cyberattacks. With the expansion of information and communication technologies (ICT) and AI, criminals are given more opportunities to expand their criminal tactics and attack organisations(Kaloudi & Li, 2020).

Kaloudi and Li (2020) expect future cyber-attacks to be smarter, more powerful, and more likely to create scalable impact by causing a high level of cascading damage. Already existing AI-supported social engineering platforms are FraudGPT, and WormGPT, where it is harnessed to enhance the believability and efficacy of social engineering attacks (Wang et al., 2020)(Falade, 2023).
There are numerous ways to orchestrate a social engineering attack, each with its own type, operator, and channel, see Figure 1. In the following paragraphs, this research will address the most frequently used attacks, outlining their methods, situations in which they are most frequently used, and overlap with the mystery guest service:

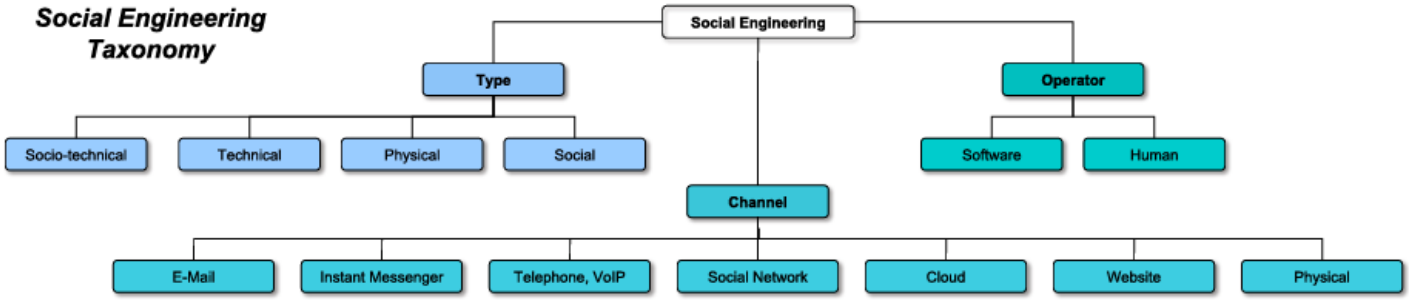


Figure 1: Social Engineering Taxonomy

2.3.1 (Spear)Phishing

Phishing is the most common social engineering attack where fraudulent emails or messages that appear to be from a legitimate source are sent in mass to trick individuals into revealing sensitive information (Roy et al., 2022). These emails can contain malicious attachments or URLs that redirect users to fake websites which exposes their information or download malware. This information can then be used by the social engineer to gain access to accounts or servers. Phishing attacks impose significant threats to businesses and individuals (Caputo et al., 2014). Technological measures such as spam filters and security toolbars are used to block, filter, and spread alerts regarding phishing emails. However, there is no perfect technological defence, since scammers move one or two steps ahead of technologies, making the latter less effective(J. Wang et al., 2017). The last line of defence against phishing mails is the training of employees on what phishing is, how to identify phishing messages, and what to do in case they come across such messages. However, it is hard to educate people on security because of overconfidence in protecting oneself against cyber threats, lack of motivation to learn security, and often treating security as a secondary duty (Kumaraguru et al., 2010). Nevertheless, the education of user security continues to be a crucial part of the fight against phishing attempts because, as technology advances and gets more widely used, people continue to be the most attractive target for potential attackers(J. Wang et al., 2017).
As phishing attacks an broad range of individuals, spear phishing is a more targeted form of social engineering where the attacker tailors the fraudulent messages to specific individuals or organisations based on detailed research (Bullee et al., 2017). The effectiveness of spear phishing lies in its ability to exploit contextual information about the victim, making the attack more powerful than a usual phishing mail (Chetioui et al., 2022). A form of spear phishing is whaling which focuses on individuals who hold a significant positions within a company like a CEO or senior executive and have access to privileged information or resources (Huang et al., 2018).

2.3.2 Physical Attacks

Social engineering attacks do not only occur digitally, sometimes physical techniques can be more effective. Physical social engineering attacks exploit human interaction and psychological manipulation to gain access to confidential information or secure areas without the use of technology (Heartfield & Loukas, 2015). Below are some common methods and techniques frequently used in physical-social engineering attacks: Tailgating is a social engineering technique wherein an individual with malicious intent follows an unsuspecting person who possesses authorised access to a restricted area. This infiltration strategy might involve the perpetrator politely requesting the target to hold the door open, or finding an opportunity to slip through the door unseen (Breda et al., 2017). With tailgating a moral conflict arises because the employee has the obligation to follow a security policy, but also feels obligated to assist another individual at the cost of breaking the security policy (Myyry et al., 2009). As with tailgating, piggybacking tries to gain unauthorised entry to restricted areas, but with piggybacking they acquire permission from the person with legitimate access by impersonating business entities(Conteh & Schmick, 2021).
Impersonation is as the name implies, the threat actor creating a false identity to gain credibility as a basis to carry out malicious actions. Impersonation can be as simple as printing fake business cards, or as elaborate as creating counterfeit identification cards or security badges. Nevertheless, the necessity for realistic-looking false credentials is mitigated if the impersonator can effectively weave and present a convincing narrative to support their assumed identity (Y. Wang et al., 2023). Social engineering attacks often involve a combination of deception tactics, with impersonation being a key element (Naidoo, 2020). Combing tailgating with an impersonation plan can for example help with staying undercover after successfully entering a building unauthorised. After successfully tailgating a social engineer can use the shoulder surfing tactic by covertly watching over the shoulders of legitimate personnel. Ultimately aiming to gather confidential information. Through this seemingly innocuous act, the perpetrator can acquire a range of sensitive details, including passwords and critical documents, especially if the target is inattentive or unaware of the observer's presence (Applegate, 2009).

2.3.3 Mystery Guest

In the academic landscape of social engineering the concept of mystery guests is not recognized or prevalent. It is however a known phenomenon within the hospitality industry, where it involves an undercover evaluator posing as a regular guest to objectively assess the service quality and overall customer experience of a hotel, restaurant, or other service provider(Anderson et al., 2001)(Bichler et al., 2020). In practice, mystery guest attacks have not occurred frequently.
The audit form however is more known, as it gives the company a great insight into vulnerabilities such as:

- Unauthorised access into the building, workstations, server rooms, and logged-in computers.
- Handling physical information on desks and near printers
- Cyber awareness of employees
- Technical breaches such as password strength

The mystery guest audit contains numerous social engineering techniques. The journey of the mystery guest starts by doing research about the premises to find the best way to infiltrate the company by either tailgating, impersonation, and/or shoulder surfing. When inside the mystery guest tries to obtain as much classified information by either shoulder surfing, baiting or casually obtaining and making pictures of classified information. After the mystery guest visit a report will

be constructed containing the findings and recommendations to enhance the cyber awareness and security of the organisation.

2.4 Propositions

The following section presents propositions that explore the role of mystery guest audits in enhancing cyber awareness within public sector organisations. Researching these propositions helps identify exact behavioural changes and adjustments following the audits. The following propositions are formulated to answer the main research question stated in section 1.3

P1: Mystery guest audits positively influence employees' cybersecurity-related behaviour
Rationale: Abawajy (2012a) shows that with using a simulation and video-based delivery method employees are better able to avoid attacks and with the interactive video that the mystery guest audit provides it will give a more effective learning medium for the participants. Therefore this research believes that mystery guest audits do not only serves evaluation but also change the cyber awareness in organisations. The audit tests the sufficiency of existing controls for possible attacks and the current cyber awareness in a controlled and safe manner. This exposure is believed to lead to improvements in both the awareness and the control mechanisms that safeguard the organisational information. Research from Rosati et al. (2022) shows that auditors have demonstrated increased awareness of cybersecurity risks within organisations and with the use of the mystery guest audit it is believed that this will serve the same effect on organisations. The real-life element of the mystery guest audit will also have an impact on the cybersecurity-related behaviour of the employees (May, 2008).

P2: Formal control recommendations from mystery guest audits do enhance the cyber awareness in public sector organisations.
Rationale: Formal recommendations, which often involve changes to policies, procedures, and compliance requirements, directly contribute to an organisation's structured approach to cybersecurity. Implementing these recommendations can lead to improved regulatory compliance and a more disciplined security environment(Ahmad et al., 2015; Moon et al., 2018). Moreover, the use of these mystery guest audits, which are formal controls, will help in identifying technology users who may not comply with formal cybersecurity policies. Which according to Stafford et al. (2018) will enhance the enterprise risk management and the cyber awareness of organisations.

P3: Mystery guest audits form informal controls and they do enhance the cyber awareness in public sector organisations.
Rationale: Informal recommendations usually focus on cultural and behavioural changes within the organisation. These can include promoting a security-first mindset among employees and fostering an environment where security practices are openly discussed and valued. By addressing these recommendations it is believed that it will positively affect the cyber awareness because studies like Ahmad et al. (2015) and Rahim et al. (2015) show that having a clear cyber security awareness message that is also related to the organisation will positively affect the cyber awareness.

P4: Physical control recommendations from mystery guest audits do not enhance the cyber awareness in public sector organisations.
Rationale: While physical security is a critical component of an organisation's overall security posture, adjustments in physical security measures alone may not significantly enhance cyber awareness unless coupled with comprehensive training and procedural updates (Sas et al., 2021). This proposition suggests that without a holistic approach, physical enhancements might not yield

improvements in cyber awareness as effectively as when combined with other types of interventions (McCrohan et al., 2010). Research on cybersecurity has shown that security regulations do not always benefit employees (Han et al., 2017; Ifinedo, 2012). Even when they receive written security policies and instructions, some employees tend to ignore the information security policies of their company, and others tend to underestimate the risks associated with information security.

BDO is curious about how to improve its mystery guest service. They want to know which recommendations from BDO are implemented and which implementations the company themselves implement after seeing the mystery guest report. Therefore, this paper will also include a recommendation section which will provide BDO with insight into improving the mystery guest service. These propositions will therefore return in the recommendations section.

Question from BDO: Which recommendations from the mystery guest audit are being implemented by the clients?
P5: Public sector organisations implement/adjust their physical controls and use the mystery guest to increase awareness.
Rationale: The direct aftermath of a mystery guest audit often exposes deficiencies in physical security controls and the overall security awareness of personnel. Organisations are likely to respond by tightening physical security measures, such as access controls and surveillance, enhancing training programs to address specific vulnerabilities revealed during the audits, and utilizing the incidents as case studies for ongoing education to cement the learning experience.

Question from BDO: Do the companies implement other initiatives to tackle cybersecurity? If so what initiatives are being implemented?
P6: Public sector organisations independently implement additional awareness training.
Rationale: Even beyond the direct recommendations from a mystery guest audit, organisations may proactively expand their security training initiatives to prevent similar vulnerabilities in the future. This proactive approach indicates a shift towards a more robust security culture, where lessons learned from audits are integrated into regular training cycles and awareness programs. This paper believes that these awareness trainings will combine the mystery guest results with other events close to the organisations in question.

These propositions collectively underscore the multifaceted impacts of mystery guest audits and the need for a comprehensive, all-encompassing approach to enhancing cyber awareness in public sector organisations. Each addresses different aspects of the response to security audits, from immediate physical adjustments to long-term cultural and behavioural shifts.

2.5 Conceptual Model

This conceptual model is designed to explore the pathways through which mystery guest audits influence cybersecurity awareness and the control factors within public sector organisations. It identifies the variables involved, their interrelations, and the theoretical underpinnings that guide the expected outcomes of the audits. The three research questions are all integrated into the conceptual model. RQ1 represents the impact that control factors have on the cybersecurity awareness of organisations. This research question will be answered through the literature review. RQ2 will represent how the mystery guest audit influences the cyber awareness of the organisation excluding the independent initiatives that were implemented by the organisation. Lastly, RQ3 will include the independent initiatives and the recommended controls from the mystery guest audit

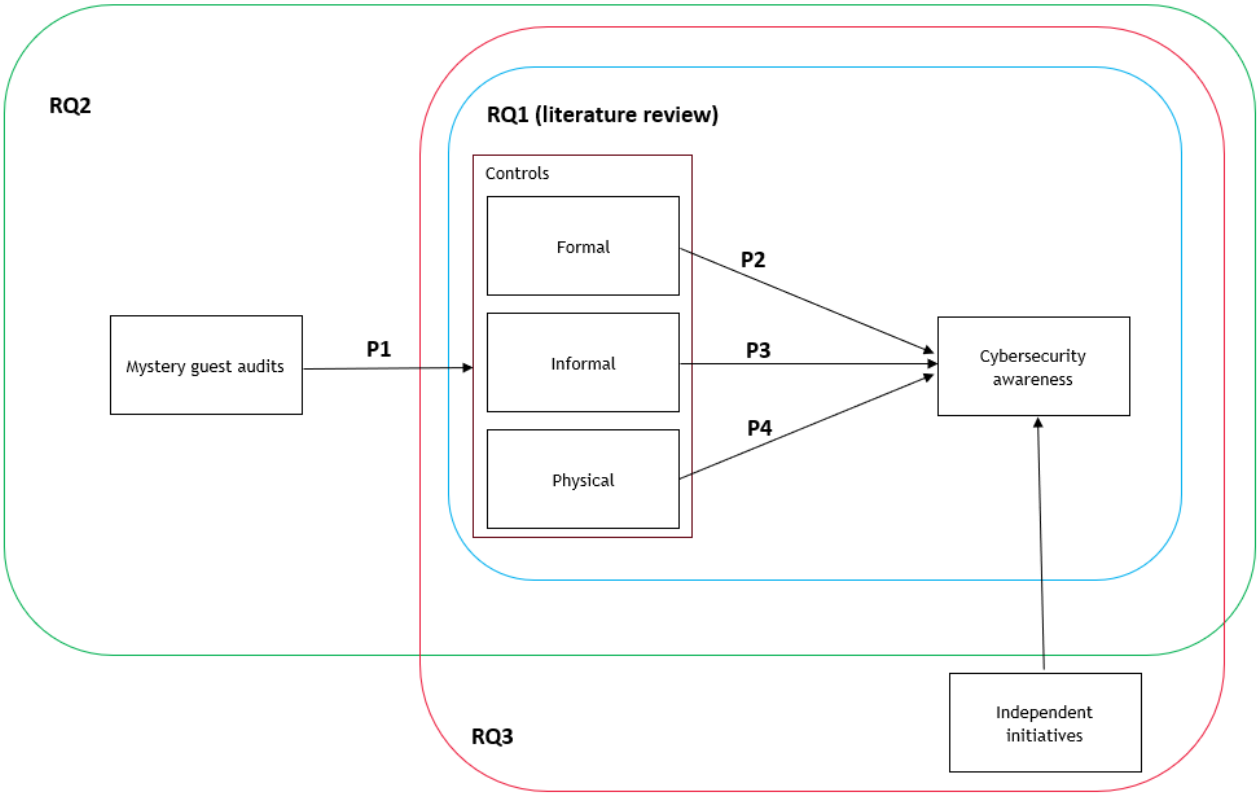


Figure 2: conceptual model

3. Methodology

Based on the principles outlined by Stake (1994) on the multiple case study method, this research will employ a qualitative case study approach to comprehensively investigate the impact of mystery guest audits on organisational cyber awareness. By closely examining three organisations, the case study will provide an intensive analysis of the changes in cyber awareness and security practices resulting from the mystery guests. This approach is particularly suited because the researchers exploit observation, interview and document review as data-gathering tools.

This research focuses on the public sector, emphasising entities that are already clients of BDO. Among these clients, some have previously experienced a mystery guest visit, while others have not. For the new clients, they will receive two mystery guest visits. Conversely, for the returning clients, the study will assess the impact of the initial mystery guest interaction by conducting a subsequent visit. This approach allows for a comparative analysis of the experiences and outcomes across different client engagements.

3.1 Public Sector

As mentioned earlier the companies that will be analysed in this study will be within the public sector. The importance of cybersecurity and privacy has grown dramatically for practitioners and scientists alike. Cybersecurity and privacy concerns are among the most important fields of concern for governments and public administration, particularly in the context of e-government and IT networks(Dawes, 2008; Wirtz & Weyerer, 2016).

Studies regarding the awareness of employees within the public sector show that there is a lack of cybersecurity awareness for public employees and also among public sector supervisors. Prior research has demonstrated that, despite the belief that security awareness is rising at all administrative levels (Stibbe, 2005), staff members' ignorance of cybersecurity-related issues, particularly at the executive level, is crucial when discussing cybersecurity in the public sector(Conklin & White, 2006; Smith & Jamieson, 2006).

Two of the three public sector organisations are municipalities and the other organisation is a medical group of general practitioners. Because of the possible damage to the image of the organisations their names and interviews will be anonymised. Despite the anonymisation of the organisations, an anonymised overview is provided in appendix I to give a clear understanding of the organisations justifying why the research findings can be considered as a cohesive whole.

3.2 Data Collection

The data will be collected from multiple sources to ensure triangulation, a key aspect of Stake's (1994) method. The data sources include:

- Observations (2nd mystery guest visit)
- Interviews
- Documents

A widely used methods for assessing cyber awareness are surveys (Garba et al., 2022), but they lack real-world interactions and behaviours that truly reflect an organisation's preparedness against cyber threats (Camm & Fox, 2018). The reflection of a real-world interaction and behaviour is measurable with a second mystery guest visit. The choice of using reoccurring mystery guest audits comes from the need for an evaluation technique that is dynamic and interactive to replicate the unpredictability of social engineering attacks. By conducting a reoccurring mystery guest within an organisation, it is possible to evaluate the changes of the first audit on the organisation's response methods and the cyber awareness of employees. This approach facilitates an empirical assessment of whether the organisation has implemented effective strategies to mitigate vulnerabilities discovered in the first audit. During the mystery guest visit the researcher himself will be the mystery guest and will observe the compliance with recommendations that were given by BDO. The recommendations usually concern physical accessibility, a clear screen & clean desk policy, and a speak-up culture. The researcher will study previous mystery guest visits to BDO to understand the tips and tricks of being a mystery guest and remaining undetected.

To further analyse the effect of the mystery guest the use of semi-structured interviews will be used. The structure of conducting, analysing, and reporting semi-structured interview data will be followed according to Adeoye-Olatunde and Olenik (2021), and the COM-B model to ensure the validity and reliability of the interviews. The COM-B model will provide a taxonomy of cyber awareness questions (Paul & Whitley, 2013) and simultaneously help improve their awareness (Galinec & Luić, 2020). The semi-structured interview data collection method is proven to be both versatile and flexible (Kallio et al., 2016). The main advantage of semi-structured interviews is enabling reciprocity between the participant and interviewer (Galletta, 2012) which will enable the interviewer to ask follow-up questions and allow the participant to speak freely during the interview. All the interviews will also be recorded if agreed with the interviewee, and later transcribed.

Because the researcher was not present at the first mystery guest visits previous mystery guest documentation of company A and B will be studied. Examining the previous mystery guest documentation will help to understand the cybersecurity maturity of organisations A and B and the recommendations that were given to improve cyber awareness. By establishing the baseline of organisation A and B the researcher can compare the differences observed during the second mystery guest visit. This comparison will reveal whether the recommendations have been effective and if they have impacted the cyber awareness of the employees.

The mystery guest and interviews will not bear any financial burdens on the customer because this might influence the availability of the respondents and affect the sample pool.

3.3 Participants

As mentioned earlier this paper will include three organisations operating within the public sector, for further explanation about the organisation see appendix I. Participants were selected from three public sector organisations based on their roles and responsibilities related to cybersecurity and information management. The selection criteria included:

- Supervisors: Individuals holding positions such as Data Protection Officer (DPO), Information Security Officer (ISO), or Chief Information Security Officer (CISO), who have a comprehensive understanding of cybersecurity measures and the mystery guest audits.
- Employees: A diverse group of employees from various departments within each organisation, chosen by the supervisors to ensure a broad representation of perspectives and experiences.

Recruitment Process

Participants were recruited through direct invitations facilitated by their supervisors. The supervisors selected employees from different departments to participate in the study, aiming to gather a wide range of insights and experiences.

Sample Size

A total of 19 interview participants are included in the study, with each organisation contributing at least six participants. This sample size was deemed sufficient to capture diverse perspectives and provide comprehensive insights into the impact of mystery guest audits. The data saturation when interviewing the 5th to 6th participants also acknowledged the sufficient sample size that has been taken.

3.4 Procedure and Protocol

To achieve a valid data collection, several procedures must be established. These procedures are essential for conducting the mystery guest visit effectively, carrying out the interviews, and presenting the findings of the mystery guest visit to the employees of the new clients. This chapter will be divided into the different procedures taken regarding the new mystery guest client and repeated mystery guest clients.

3.4.1 New Mystery Guest Clients

Company C has not yet had a mystery guest visit. Therefore, two mystery guest visits will be conducted, spaced one month apart. During the first encounter, the mystery guest will attempt unauthorised entry in the morning, and if successful, will proceed to systematically collect information according to a predetermined checklist. The mystery guest will also visit during the busiest days of the office to ensure a thorough assessment. After the mystery guest's investigation, interviews will be conducted with the designated supervisor of that organisation to better understand their organisation and information systems. Following this phase, a report will be compiled in the form of a flyer, which will be distributed throughout the organisation, containing recommendations and findings aimed at addressing specific risks. The flyer will be posted on intranet, on tables in the cafeteria, and on workspaces. This will present a valuable opportunity to raise awareness of the visit and its insightful observations. According to Abawajy (2012), this conventional delivery method is a good method to remind people of specific actions and improve their security poster. See appendix II for the flyer that has been sent throughout the organisation.

One month thereafter, a new mystery guest will visit, and the aforementioned process will be repeated to assess the impact and changes resulting from the initial mystery guest. Subsequent to the completion of the mystery guest's investigation, interviews will be conducted with the designated supervisor and a selection of employees who are assigned by the supervisor. These interviews will examine both control changes and the effect of these controls on cyber awareness. All interviews will be fully anonymised. The last task of this cycle will be creating another report detailing the findings and recommendations of the visits. This report will purely be for the client. Figure 3 visualizes the process for new mystery guest clients that must be completed to achieve results for the research.

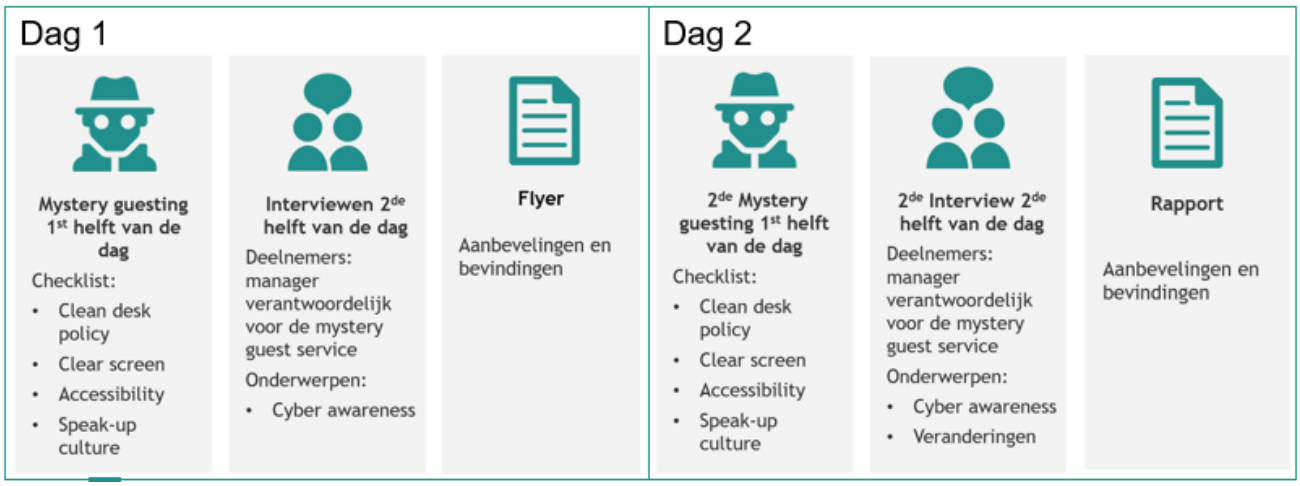


Figure 3: mystery guest process new client

3.4.2 Repeated Mystery Guest Clients

Companies A and B already have gotten a mystery guest visit thereby their procedure will also differentiate. The data collection of the repeated clients will be conducted over the course of one day, during which the mystery guest will attempt unauthorised entry in the morning, subsequently proceeding to systematically collect information according to a predetermined checklist upon successful entry. Following the completion of the mystery guest's investigation, interviews will be conducted with the designated supervisor and a select group of employees who are appointed by the supervisor. These interviews will examine both control changes and the effect of these controls on cyber awareness. All interview data will be fully anonymised. Subsequent to this day, the company will receive a report containing recommendations and findings aimed at addressing specific risks. The recommendations and findings of the first mystery guest visit will be examined and used during the interviews so that the findings are reliable and valid. Figure 4 shows the process for repeated mystery guest clients.

Figure 4: mystery guest process repeated clients

3.5 Interview Guide

In shaping the semi-structured interviews the comprehensive framework developed by Adeoye-Olatunde and Olenik (2021) was used, which emphasises the importance of structured flexibility within interviews. This approach allows to design questions that do not only focus on the direct impacts of the mystery guest audits, but rather also open discussions related to the motivations underneath and changes related to the mystery guest audits.

As suggested by Adeoye-Olatunde and Olenik (2021) the interview questions are structurally categorised based on the roles and responsibilities of the respondents in their organisation. Questions 1 through 5 are specific for the executives who had initiated the mystery guest audit and those related to the organisational changes of the audit.
Questions 6 through 9 are for all respondents. These questions are intended to gather insights into the experiences of the control changes and their impact on the employees' cyber awareness. The full interview questions can be found in appendix III

The interview is structured into several sections. The first section includes an icebreaker combined with an explanation of the first mystery guest visit. By starting with an icebreaker the researcher tries to familiarise the respondents with the context of the interview by engaging them in a straightforward query about the first mystery guest visit. The icebreaker will also help with creating a relaxed atmosphere where participants feel free to provide answers to sensitive topics like the mystery guest visit (Bouwmeester, 2023). The question also enables the respondent to easily start the discussion by clearly indicating his or her experience directly, thereby setting the base to understand more details and in-depth exploration of the subject.

After the icebreaker, the supervisors will receive questions aiming to collect detailed information about the organisation’s post-audit actions. In order to establish a clear connection between the audit recommendations and organisational responses this question aims to determine the type and extent of efforts that were used to tackle the mystery guest findings. This information is necessary to give accurate recommendations toward BDO about the usage of recommendations and the possible out-of-the-box implementations the companies implement on their own initiative.

The last four questions are presented to all the participants. The questions will address the aspects of control, cyber awareness, and influence of the mystery guest audit. For example questions six and seven questions the formal and informal changes, that the mystery guest recommended, and the effect it has on their cyber awareness. Tolossa (2023) acknowledged that well-trained employees show a better cyberculture and improved cyber awareness. Although research shows that informal and formal controls raise awareness there is no research on the increase of awareness regarding physical controls. Thereby, the last four questions examine whether the mystery guest has influenced the cyber awareness of the employees, and if so, which types of controls—physical, informal, or formal—have influenced the employees.

Validity and reliability

Interviews are anonymised to protect the privacy of respondents and to enhance the validity of the results. Anonymisation ensures that interviewees can speak freely without fear of repercussions, leading to more honest and accurate responses (Grassegger & Nedbal, 2021). This practice is crucial for obtaining reliable data, as it minimises the potential bias introduced by respondents who might otherwise alter their answers due to concerns about confidentiality or potential negative outcomes.

3.6 Data Analysis

After gathering the qualitative data from the semi-structured interviews the data will be processed through the qualitative analytic method by Braun and Clarke (2006). This technique is useful because it provides a flexible and systematic approach to identifying patterns and themes within qualitative data, allowing for rich, detailed, and nuanced interpretations (Braun & Clarke, 2006). The six steps outlined by Braun & Clarke (2008) are:

Step 1, Familiarisation with the Data: This initial phase involves immersing in the data by re-reading the dataset, and noting down initial ideas and potential codes.

Step 2, Generating Initial Codes: Systematically code interesting features of the data across the entire dataset, collating data relevant to each code.

Step 3, Searching for Themes: Group the different codes into potential themes and gather all data relevant to each potential theme.

Step 4, Reviewing Themes: Check if the themes work in relation to the coded extracts and the entire dataset, generating a thematic map of the analysis.

Step 5, Defining and Naming Themes: Refine each theme, and analyse the data within them to generate clear definitions and names for each theme.

Step 6, Producing the Report: The final step involves selecting vivid, compelling extract examples, final analysis of selected extracts, relating the analysis back to the research question and literature, and producing a scholarly report of the analysis.

The six steps of Bruan & Clark (2008) will be implemented using ATLAS.ti. The computer-assisted qualitative data analysis tool called ATLAS.ti makes the process simpler to analyse qualitative data in research projects.

4. Results

This section presents the findings of the mystery guest audits, structured to address the research question while integrating insights from multiple organisations. The results include the observations from the second mystery guest audit and interviews with supervisors and employees. The interview section will be structured according to the themes that were selected by analysing the data.

4.1 Interviews

While analysing the interviews the researcher concluded the following themes; Awareness refreshment, Change in awareness, Communication error, Difficult to adhere, Formal controls, Informal controls, Physical control, and Recommendations. This section is based on the output of the coded interviews which can be examined at appendix IV

4.1.1 Awareness Refreshment

The implementation of mystery guest audits has led to significant changes in cybersecurity awareness among employees. Employees have generally become more aware of cybersecurity threats and the importance of addressing these issues. As one employee noted, *"Good action to be more aware of awareness and to address each other and strangers."* This indicates a heightened vigilance and a proactive approach to identifying and addressing potential security risks. The report of the mystery guest audit also proves to be helping with maintaining the cyber awareness of organisations. An employee remarked, *"Well, that mystery guest flyer did help me refresh the clear screen and clear desk policy."* Similarly, the reinforcement of specific policies was noted:
"Well, the clear screen and clean desk policy has simply been brought back for refreshment, so I have seen a change in that." These statements underscore the importance of continuous education and reminders to ensure ongoing compliance with security protocols. With the shift from remote work to on-site work has led to a relaxation in the adherence to cybersecurity protocols and an increase in cyber risks. One employee observed, *"And you notice that some people did not yet know about the recommendations because people often work from home and missed it, so the flyer helps some colleagues, but I already knew about them."* This indicates that while some employees are well-informed, others, may have missed cyber awareness programs or just did not pay attention to them because of their safe environment. Overall, the mystery guest audits have been successful in refreshing awareness and prompting behaviour changes. *"Everyone has become more aware of it, but you do notice it. That some things. Yes, it can sometimes slip through."* This reflects the overall improvement in awareness while acknowledging that perfect adherence is challenging and ongoing efforts are needed.

4.1.2 Communication Error

The choices of delivery methods used by the organisations to communicate the mystery guest audits have revealed communication errors within the organisation. Several employees highlighted these issues, providing insight into the current state of internal communication and its effectiveness. One employee mentioned*, "No, I don't know anything about a mystery guest visit.*" It is particularly concerning that this person was unaware of the mystery guest's visit, as they work as a receptionist, a role that serves as one of the primary barriers to preventing unauthorised individuals from entering. This indicates an ineffective use of communication channels or methods. The decision of Company A was to not make the recommendations public on their intranet page but rather make an awareness training for all employees. The reason for not putting the mystery guest video online was *"The video also needs explanation"(Interview 5).* However, they forgot to consider the

receptionists in this plan. Another employee from company B expressed, *"I think there is sufficient communication internally, but there is a lot of communication about many topics. So what sticks with you, huh?"* This suggests that while there is ample communication within the organisation, the sheer volume of information on various topics may overwhelm employees, making it difficult for them to retain and prioritize critical security information. Additionally, one employee admitted, *"I was busy and didn't look at the intranet because it doesn't really contain the most important information and I certainly don't go through the entire intranet to see if I missed something."* This highlights a significant issue with the delivery method of information. The intranet, which should be a reliable source of important updates, is perceived as ineffective and not user-friendly. As a result, employees may miss crucial updates simply because they do not engage with the platform regularly.

4.1.3 Difficult to Adhere

Despite processing and acknowledging the recommendations from the mystery guest audits, employees still encounter significant challenges in consistently adhering to security protocols. One employee admitted, *"Of course I don't always succeed because I will undoubtedly have forgotten it, but I think about it much more often now."* This reflects the ongoing struggle to remember and apply the clear screen and clear desk policy, despite improved awareness.

A common difficulty expressed by employees is the awkwardness of stopping and questioning strangers. One remarked, *"It's always a little awkward to stop someone and ask who they are, especially when it seems like they're just there to do their job."* This sentiment is echoed by another employee who stated, *"Yes I have that too. I have certainly become more aware of the physical checks within our company, but to be honest, I sometimes find it difficult to approach people about this."* The social discomfort associated with questioning others poses a significant barrier to enforcing physical security protocols effectively. The sheer number of people working in the organisation further complicates adherence to these protocols. One employee explained, *"Yes indeed, and so many people work here, I know many of them, but I certainly don't know them all, so that is difficult, yes, even though I keep an eye on my laggard every morning when I enter."* This challenge is compounded by the presence of higher-ranking individuals, as another employee noted, "*Yes, that is quite difficult because there are sometimes some higher placed people walking around and I see people just hesitate to approach them."* The hesitation to confront possible higher-ups underscores the complexity of enforcing security measures uniformly across different hierarchical levels within the organisation.

Moreover, the constant movement of people within the workspace makes it difficult to monitor and enforce security checks. An employee mentioned, "Well, I find that very difficult, because there are so many people walking around." This constant flow of individuals makes it challenging to ensure that all security protocols are followed consistently.

Overall, while there is a clear increase in awareness and an intention to adhere to security measures, practical difficulties in implementation persist. As one employee succinctly put it, "I try to check who it is, but I find it difficult to ask where the person comes from and whether he or she works here because that seems strange." This highlights the need for continued efforts to support employees in overcoming these barriers and fully integrating security practices into their everyday routines.

4.1.4 Formal Controls

The mystery guest audits have led to noticeable improvements in the adherence to formal controls within the organisations. Employees have reported significant changes in their behaviour and the overall office environment. One employee noted, *" After the mystery guest visit I never actually see anything un the bureau's when I leave. I'm usually one of the last, but there's no stuff lying around or papers or anything."* This indicates a shift towards maintaining a cleaner and more secure workspace. Another employee observed, *"That is a difference from before because the mystery guest visited us. You now notice that everyone closes their screen as much as possible, even though this does not always happen, but it is of course not waterproof either."* This highlights the increased diligence in following the clear screen policy, though it also acknowledges that compliance is not yet perfect.

Employees have also taken on the responsibility of passing on these practices to new hires. As one employee explained, *"Every time I leave my desk, I close everything and keep it clean and I try to pass that on to new employees."* This demonstrates the spreading of good practices throughout the organisation, reinforcing the importance of maintaining formal controls. The impact of the mystery guest visits has been profound on individual behaviours as well. An employee shared, *"But I do believe that since then, well, really, because of the Mystery Guests, I have been a little quicker to enable my Windows lock and then walk away."* This shows how the audits have encouraged employees to adopt more secure habits, such as locking their screens.
Another significant change is reflected in the statement, *"Well, lock the screen, yes, because as I just said, I have never done that before, so that is what I have become most aware of and also generally more aware."* This indicates a newfound awareness and commitment to following security protocols that were previously neglected.

Communication materials have played a crucial role in reinforcing these practices. *"Well, that flyer report did help me refresh the closing screen,"* said one employee, emphasizing the importance of regular reminders and educational materials. Another noted, *"Well, the clear screen and clean desk policy has simply been brought back for refreshment, so I have seen a change in that,"* highlighting the effectiveness of reintroducing and reiterating formal controls to ensure they are followed.

4.1.5 Informal Controls

The mystery guest audits have fostered a culture of mutual support and informal controls within the organisations, impacting employees' behaviours and attitudes towards cybersecurity. One employee mentioned, *"I wasn't there when the first mystery guest arrived, so it was nice that (the name of the person) helped me with the rules and such."* This highlights the importance of peer support in understanding and adhering to security protocols. The influence of key individuals in promoting a culture of security is evident. As one employee noted, *"It is true that (Name) did indeed help us with the culture of turning your screen black and keeping your desk clean."* This underscores how leadership and role models can drive the adoption of secure practices. Employees have also taken it upon themselves to pass on good practices to new hires. *"Every time I leave my desk, I close everything and keep it clean and I try to pass that on to new employees."* said one employee. This behaviour helps ingrain security measures into the daily routines of all staff members. The influence of colleagues is significant in promoting adherence to security measures. *"I have the same thing because I am more aware of shutting down my computer, but that is more because of employees like you (pointing to his colleague) who tell me that I have to do it,"* said an employee. This peer pressure helps maintain a high standard of security awareness and behaviour.

Peer enforcement is a crucial aspect of informal controls within organisations. As one employee described, *"If someone does not lock their screen, an email will be sent to everyone on the team to ensure that the sausage roll must be collected."* This humorous yet effective method of peer accountability serves as a reminder of individual responsibilities. Instead of treating your colleagues with a sausage roll, some employees use visual reminders to reinforce security practices. An employee shared*, "A 'forget-me-not' post-it will be put on the screens if it was not locked,"* illustrating the creative strategies employed by different organisations. They also use direct communication and feedback within departments. One employee noted, *"Within my department, if someone leaves a computer unlocked, they will always be spoken to if someone else sees it there or if key cards are visible somewhere, such as during a meeting or a restroom break. This is also discussed afterwards."* This approach ensures that security lapses are promptly and constructively addressed. These findings emphasize the various ways employees collectively help each other adhere to security protocols, including humorous reminders and direct feedback.

4.1.6 Physical Controls

A notable physical control outcome is the increased vigilance among employees regarding who is allowed entry into the premises. As one employee recounted, *"Then I heard that someone came in and was addressed by… from ICT. He says, Gosh, who are you and why do you come here?"* This anecdote underscores the heightened awareness and proactive questioning that has become more common after the spreading of the mystery guest flyer. Employees have become more conscious of unfamiliar individuals in the workplace. One employee noted, *"It's just that you are even more aware of that when you just see people you don't know. That you just ask."* This increased vigilance is echoed by another employee who stated, *"Yes, I do see that I and others are paying more attention to who we let in."* These comments reflect a broader cultural shift towards questioning and verifying the presence of unknown individuals. The audits have also prompted employees to reflect on and improve their own behaviours. *"But I think you pay a little more attention now than you did before, But I would especially when I'm alone,"* remarked one employee, indicating a personal increase in vigilance. Another employee shared, *"Well, I honestly never thought about the fact that someone walks around like that, so I do plan to do something about it,"* showing a proactive response to a previously unknown phenomenon. Another employee mentioned that the recommendations of the mystery guest visit help with promoting better security practices. "*It is true that the tips to look behind me do help me. When I walk in, I do look behind me*". There is also a recognition of the balance between politeness and security. One employee pointed out, *"Politeness is one thing, but if you have doubts about whether a colleague is a colleague, you can simply say so in a friendly way."* This approach helps maintain a secure environment without causing unnecessary offence.
The impact of these changes is evident in everyday practices. An employee noted, "I don't let people tag along if I don't know them. Even though I don't know everyone here," demonstrating a firm commitment to verifying identities and preventing unauthorised access.

However, some employees still find it challenging to approach and question others. *"Yes, I have that too. I have certainly become more aware of the physical checks within our company, but to be honest, I sometimes find it difficult to approach people about this,"* admitted one employee. A common difficulty expressed by employees is the awkwardness of stopping and questioning strangers. One remarked, *"It's always a little awkward to stop someone and ask who they are, especially when it seems like they're just there to do their job."* This sentiment is echoed by another employee who stated, *"Yes I have that too. I have certainly become more aware of the physical checks within our company, but to be honest, I sometimes find it difficult to approach people about this."* The social discomfort associated with questioning others poses a significant barrier to

enforcing physical security protocols effectively. The sheer number of people working in the organisation further complicates adherence to these protocols. One employee explained, *"Yes indeed, and so many people work here, I know many of them, but I certainly don't know them all, so that is difficult, yes, even though I keep an eye on my laggard every morning when I enter."* This challenge is compounded by the presence of higher-ranking individuals, as another employee noted, *"Yes, that is quite difficult because there are sometimes some higher placed people walking around and I see people just hesitate to approach them."* The hesitation to confront possible higher-ups underscores the complexity of enforcing security measures uniformly across different hierarchical levels within the organisation.

4.1.7 Change in Awareness

The implementation of mystery guest audits has led to changes in cybersecurity awareness among employees. Employees have generally become more conscious of cybersecurity threats and the importance of addressing these issues. As one employee noted, "Yes, you now see a lot more black screens when you walk around, that wasn't the case before." This indicates a heightened vigilance and a proactive approach to identifying and addressing potential security risks.

Another employee expressed a sense of responsibility towards new employees, stating, "Yes, certainly, as I just said, I also try to emphasize this to new employees, so to speak, because you feel kind of responsible." This shows that the increased awareness is not only affecting individual behaviour but also fostering a culture where experienced employees feel accountable for educating their peers.

Despite this overall improvement, challenges remain. One employee highlighted the difficulty in maintaining constant vigilance: "But I think you pay a little more attention now than you did before, but I would especially when I'm alone." This suggests that while awareness has increased, consistent application of security measures can still be a struggle.

4.1.8 Independent Initiatives

The research has identified several potential improvements for the mystery guest service based on independent initiatives taken by the organisations. These recommendations aim to enhance the impact of the service and the effectiveness of delivery methods. One improvement involves the possible implementation of a visitor registration system. *"We have been working on a system so that people have to register. This allows you to better check who is who, which is also useful because I am emergency response officer."* noted one employee. This system would help in verifying identities, ensure more physical security, and safety of employees.

Training sessions have received positive feedback, indicating their value. An employee remarked, *"Well we figured it out, oh yes, it really was a really good training."* Awareness training, incorporating practical examples from the mystery guest visits, has been effective. *"We conducted an awareness training about Information Security and Privacy through the mystery guest and it actually explains what happened to the mystery guest. This is done by also showing the video with the recommendations in it,"* shared an employee. Positive feedback on these trainings highlights their importance: *"Yes, we get good feedback on the training that it is at least a bit fresh and not long-winded."* Company A took a slightly different approach to the training of company B. They created a more engaging activity, a pub quiz, which has been beneficial in promoting information security and privacy*: "That pub quiz helped bring information security and privacy. It was really fun."*

Additionally, technological enhancements, such as the use of cards to automatically lock laptops, have been suggested: *"In any case, those cards can also give a kind of signal when they are within a certain distance of the laptops, so that the laptop will also be automatically locked."* Implementing these key cards could tackle both physical and formal controls.
Visual reminders, such as the clear screen and desk policy displayed on screens, have also been effective. *"What's funny is the clear screen and desk policy is on your screen when you close your screen, so you remember it better,"* noted an employee. Besides visualising the clear screen and desk policy it also shows tips to improve employee's passwords and physical security reminders.

4.2 Mystery Guest Visit

The data in this results section is derived from observations made during recent mystery guest visits, compared with older documents from the initial visits, to assess changes and improvements in organisational security practices. The detailed information supporting these findings is provided in appendix V.

There was a notable improvement in adherence to the clean desk and clear screen policies. During the undercover operations, it was observed that employees were generally more diligent about securing their workspaces, with only a few instances of screens being left unlocked. This positive change indicates that the training and awareness programs implemented over the past two years have been effective. However, physical security still presents challenges. Similar to the first visits, the mystery guests were able to enter all three organisations by tailgating employees, highlighting that the efforts to foster a speak-up culture and restrict unauthorised access have not fully succeeded. Inside the buildings, manoeuvring was more challenging due to the installation of additional doors with keypads, which added a layer of security. Nevertheless, critical areas such as management offices were found to be unlocked, allowing easy access to sensitive documents. Employee vigilance has shown some improvement. In a few instances, staff members questioned unfamiliar individuals, indicating a growing awareness and willingness to address potential security breaches. Despite this progress, the overall vigilance was inconsistent, with the mystery guests often able to move around without being challenged.
In conclusion, the second mystery guest visits demonstrated a positive shift in the enforcement of clean desk and clear screen policies, but there is still room for improvement in physical security measures within organisations. These findings suggest that while progress has been made, continued efforts are necessary to enhance both formal and physical security aspects.

5. Discussion

This chapter assesses the effectiveness of mystery guest audits in enhancing cyber awareness and driving organisational changes within public sector organisations, guided by the research questions and explored through specific propositions derived from the study.

5.1 Positive Influence of Mystery Guest Audits on Cybersecurity Behaviour (P1)

The results indicate that mystery guest audits enhance employees' cybersecurity-related behaviours and therefore support proposition one. Employees reported increased awareness and vigilance towards cybersecurity threats following the audits.

"They certainly become more aware of it through the mystery guest visit"

This finding aligns with Abawajy's (2012) assertion that interactive and simulation-based training methods are effective in improving cybersecurity behaviours. The real-life element of the mystery guest audits provided a practical and impactful learning experience, reinforcing the theoretical framework proposed by Rosati et al. (2022), which emphasizes the role of auditors in increasing cybersecurity awareness. Employees noted that such audits helped refresh their knowledge of policies like the clean desk and clear screen protocols, which had lapsed during periods of remote work.

"That is a difference from before the mystery guest visited us. You now notice that everyone closes their screen as much as possible"

This finding supports May's (2008) argument that real-life security exercises can have a tangible impact on behaviour.

5.2 Formal Controls (P2)

The implementation of mystery guest audits has significantly influenced cybersecurity awareness and behaviour among employees in various organisations. This study explored several propositions to assess the effectiveness of these audits and provided insights into the practical challenges and improvements in cybersecurity practices.

Formal control recommendations from mystery guest audits have been shown to effectively enhance cyber awareness in public sector organisations. This structured approach leads to improved regulatory compliance and a more disciplined security environment, confirming the critical role formal controls play in cybersecurity management as highlighted by Ahmad et al. (2015) and Moon et al. (2018).

The practical impact of mystery guest audits on employee behaviour is evident from their feedback. Employees reported significant improvements in maintaining clean desk policies and locking screens after the audits. For example, one employee noted, *"After the mystery guest visit I never actually see anything on the bureau's when I leave. I'm usually one of the last, but there's no stuff lying around or papers or anything."* This indicates a shift towards maintaining a cleaner and

more secure workspace, which aligns with the principle that clear policies and consistent enforcement improve compliance and security (Lee & Lee, 2021).
Another employee observed, *"That is a difference from before because the mystery guest visited us. You now notice that everyone closes their screen as much as possible, even though this does not always happen, but it is of course not waterproof either."* This highlights the increased diligence in following the clear screen policy, acknowledging that while compliance has improved, it is not yet perfect. This aligns with findings by Ifinedo (2012), who noted that while formal controls are critical, some employees might still ignore policies, underlining the need for continuous reinforcement. Another significant change is reflected in the statement, *"Well, lock the screen, yes, because as I just said, I have never done that before, so that is what I have become most aware of and also generally more aware."* This indicates a newfound awareness and commitment to following security protocols that were previously neglected, emphasizing the role of formal controls in fostering a security-conscious culture (Barlow et al., 2013). Research by Tolossa (2023) also supports this statement because they found that well-trained employees are more likely to promote a culture of cybersecurity awareness.

The improvement in adhering to the formal controls showed during 2nd mystery guest visit. During every mystery guest visit, there were a maximum of two screens unlocked and unattended. This is a significant difference in contrast to the first mystery guest visit where the formal controls are even less well respected.
Formal recommendations from mystery guest audits have been shown to effectively enhance cyber awareness in public sector organisations. The structured approach to implementing changes in policies and procedures has led to improved regulatory compliance and a more disciplined security environment. This is consistent with findings from Ahmad et al. (2015) and Moon et al. (2018), which highlight the importance of formal controls in cybersecurity management. The success of these audits in identifying non-compliant users and enhancing enterprise risk management further supports Stafford et al. (2018) conclusions. Employees mentioned improvements in maintaining clean desk policies and locking screens, demonstrating the effectiveness of these formal recommendations in promoting security-conscious behaviours.

"Every time I leave my desk, I close everything and keep it clean and I try to pass that on to new employees"

5.3 Informal Controls (P3)

The informal control recommendations focusing on cultural and behavioural changes have positively contributed to cyber awareness within organisations and therefore proposition three is accepted. Employees demonstrated a heightened security-first mindset and engaged in open discussions about security practices. This outcome supports the research by Ahmad et al. (2015) and Rahim et al. (2015), which emphasize the importance of a clear and relatable cybersecurity awareness message in promoting positive security behaviours, which the mystery guest service provides. The security culture plays a pivotal role in safeguarding organisations against cyber threats. According to Da Veiga et al. (2020), a security culture includes the social, cultural, and ethical measures implemented within an organisation to enhance security-related behaviour. This subculture of the organisational culture encompasses the thoughts, emotions, and daily activities of employees (Wen et al., 2019).

In practice, the mystery guest audits fostered a culture of mutual support and informal controls within the organisations, impacting employees' behaviours and attitudes towards cybersecurity. For example, two employees mentioned,

"I wasn't there when the first mystery guest arrived, so it was nice that (the name of the person) helped me with the rules and such."

"It is true that (Name) did indeed help us with the culture of turning your screen black and keeping your desk clean."

This highlights the importance of peer support in understanding and adhering to security protocols. As Da Veiga et al. (2020) elaborated, peer influence is critical in promoting a security culture where employees turn to their peers for assistance when needed. This also underscores how leadership and role models can drive the adoption of secure practices. The creation of a strong and encouraging security culture also ensures that workers are well-protected at all organisational levels (Parsons et al., 2014). This behaviour helps ingrain security measures into the daily routines of all staff members, demonstrating how informal controls can perpetuate positive security behaviours (Leach, 2003). It demonstrates that peer enforcement is a crucial aspect of informal controls within organisations. One employee described,

"If someone does not lock their screen, an email will be sent to everyone on the team to ensure that the sausage roll must be collected."

This peer pressure helps maintain a high standard of security awareness and behaviour, aligning with the concept of 'mandatoriness' discussed by Boss et al. (2009). The humorous yet effective method of peer accountability serves as a reminder of individual responsibilities, reinforcing the idea that security is a shared responsibility.

The dynamic and ongoing nature of these informal controls, supported by a culture of mutual accountability and continuous reinforcement, effectively promotes a security-first mindset among employees. This collective approach aligns with the findings of Li et al. (2019), which highlight the importance of alignment between the organisational environment and IT security awareness in recognizing and addressing security threats. By fostering a supportive security culture and leveraging peer influence, organisations can significantly enhance their overall cybersecurity posture.

5.4 Physical Controls (P4)

Physical control measures alone were found to be less effective in enhancing cyber awareness in contrast to formal and informal control. In practice, the mystery guest audits led to increased vigilance among employees regarding who is allowed entry into the premises.

"Then I heard that someone came in and was addressed by… from ICT. He says, Gosh, who are you and why do you come here?"

"It's just that you are even more aware of that when you just see people you don't know. That you just ask."

"It is true that the tips to look behind me do help me. When I walk in, I do look behind me."

These anecdotes underscore the heightened awareness and proactive questioning that became more common after the mystery guest flyer was distributed. Employees became more conscious of unfamiliar individuals in the workplace. The recommendations from the mystery guest audit also sparked a proactive response from some employees an unknown phenomenon.

Despite these improvements in a few employees, others reported ongoing challenges in consistently applying physical security measures. One of the challenges is the sheer number of people working in the organisation which complicates adherence to these protocols. One employee explained,

"Yes indeed, and so many people work here, I know many of them, but I certainly don't know them all, so that is difficult, yes, even though I keep an eye on my laggard every morning when I enter."

Employees also mentioned the social discomfort associated with questioning others, posing a significant barrier to enforcing physical security protocols effectively. Social discomfort in questioning strangers and the presence of higher-ranking individuals were also significant barriers. This reflects findings by Myyry et al. (2009) and Leach (2003) on the difficulties of enforcing security protocols uniformly across hierarchical levels.

"It's always a little awkward to stop someone and ask who they are, especially when it seems like they're just there to do their job."
"Yes, I have that too. I have certainly become more aware of the physical checks within our company, but to be honest, I sometimes find it difficult to approach people about this."
"Yes, that is quite difficult because there are sometimes some higher placed people walking around and I see people just hesitate to approach them."

These challenges highlight the need for additional training and support to help employees feel more comfortable with these interactions. Physical security measures alone were less effective in enhancing cyber awareness unless coupled with comprehensive training and procedural updates. This aligns with the literature by Sas et al. (2021) and McCrohan et al. (2010), which suggest that a holistic approach combining physical and cyber controls is necessary for significant improvements in cyber awareness. Recent literature highlights these findings, pointing out that although people tend to perceive the threats the mitigation efforts for these remain inadequate (Kovačević et al., 2020). The 2nd mystery guest visit shows that employees still struggle to approach unknown personnel. Combining the three mystery guest visits that have taken place the mystery guest was approached a total of three times and was never kicked out of the facilities.

In conclusion, while physical security measures are essential, their effectiveness in enhancing cyber awareness when coupled with the mystery guest audit is only improved for a minority of the employees. The mystery guest audits have demonstrated a slight increase in vigilance and a cultural shift towards questioning and verifying individuals which can improve physical security practices. However, ongoing support, training, and the integration of physical and cybersecurity measures are necessary to address the challenges and ensure consistent application of security protocols. The additional help is necessary for the majority of employees who seem to be struggling to adhere to the physical controls because of the social discomfort they face when approaching an unknown person. Only providing the mystery guest recommendation on physical security does not seem to be enough as the mystery guest was able to enter all organisations for a 2nd time. Some organisations even more than once on the same day. These findings conclude that proposition three is accepted, as it gives the majority of employees an increased understanding of threats they do not act accordingly to protect the information and data which is a crucial aspect of the cyber awareness definition. The three to four employees who showed an increase in cyber awareness because of physical control recommendations are not enough to reject the proposition.

5.5 Communication Challenges and Solutions

The choice of communication methods for delivering the mystery guest audit findings revealed significant challenges. Employees reported issues with the intranet, which was perceived as ineffective and not user-friendly.

"I was busy and didn't look at the intranet because it doesn't really contain the most important information and I certainly don't go through the entire intranet to see if I missed something."

This aligns with the literature suggesting that traditional communication methods may overwhelm employees and fail to prioritize critical information (Wilson & Hash, 2003). Even though the choice of delivery method from company B did not reach the whole audience the employees that did see the message formed a cyberculture that informed unknown employees. This shows the importance of a thought-out delivery method to target specific organisational audiences with precision and conciseness, engaging them with real-life examples(May, 2008).

Company A showed a more interactive method of delivering the mystery guest recommendations. The need for more engaging and dynamic communication strategies is evident, as supported by Kumaraguru et al. (2007) and Fung et al. (2008). Training sessions and practical examples from the audits were noted as effective, with employees suggesting improvements like the use of visual reminders and interactive training sessions to reinforce security messages.

"Well we figured it out, oh yes, it really was a really good training"

5.6 Independent Initiatives

Reflecting on the outcomes of the company-implemented projects derived from the mystery guest visits, there is only one instance where an organisation independently created a project to tackle cyber-related threats. This initiative involved a training program introduced by Company A, which incorporated the recommendations of the mystery guest audit. Although it is not measurable from the results whether this training had a direct impact on increasing the organization's cyber awareness, the recommendations from the mystery guest audit did show a positive effect. The training program was well-received, indicating that the manner in which the mystery guest's findings were communicated was positively impactful.

"It really was a really good training"

This suggests that the approach of combining the mystery guest recommendations with interactive training was effective and appreciated.

5.7 Conclusion

In conclusion, the findings of this study have successfully addressed research questions 2 and 3.

RQ2: How do mystery guest audits influence employees' cybersecurity awareness
RQ3: Which control recommendation from the mystery guest or independent initiatives influences the cyber awareness within public sector organisations?

RQ2 reveals that the mystery guest audit influences the employee's cyber awareness by providing practical, real-life experiences that reinforce cybersecurity protocols and policies. For RQ3 is concluded that mystery guest audits and their associated control recommendations have significantly influenced cybersecurity awareness and behaviour. Formal controls ensure regulatory compliance and disciplined security practices, while informal controls are created by employees and foster a supportive security culture. Physical controls however did not influence the cyber awareness of employees, it only increased their understanding of the physical threats. The one and only independent initiative from company A has not been proven to increase the awareness of employees although the initiative helped with communicating the message of the mystery guest audit.

6. Conclusion

6.1 Key Findings

This study has provided significant insights into enhancing cybersecurity awareness and the effectiveness of various security measures within organisations. By implementing mystery guest audits, the research demonstrates the importance of a multifaceted approach that includes formal, informal, and physical security measures, all supported by effective communication strategies to foster a culture of security awareness and compliance.

The mystery guest audits were effective in raising cybersecurity awareness among employees. These audits, which involved practical and engaging methods to identify and address security lapses, led to a noticeable increase in vigilance among staff. Employees became more aware of potential threats and proactive in adopting security measures, reinforcing the importance of these audits in maintaining robust security protocols. Formal control recommendations from the mystery guest audits played a crucial role in improving cybersecurity practices. These recommendations often involved structured changes in policies and procedures, which resulted in better regulatory compliance and a more disciplined security environment. The study aligns with existing literature that emphasizes the importance of formal controls in maintaining a strong cybersecurity framework. The mystery guest audit also fostered informal controls creating a more advanced cyber culture among employees. The mystery guest's recommendations encouraged open discussions about security practices and fostered a supportive security culture. Peer support and the influence of key individuals were crucial in promoting adherence to security protocols. This finding supports the idea that a strong security culture, where employees are encouraged to share and reinforce good practices, is essential for effective cybersecurity.

Physical security measures were shown to be necessary but insufficient on their own to enhance cyber awareness. While the mystery guest audits led to increased vigilance regarding who was allowed entry into the premises, consistently applying these measures remained challenging. This is because of the awkwardness and fear of approaching a possible unauthorized person.

The effectiveness of communication strategies emerged as a critical factor in the successful delivery of mystery guest audit findings. The study revealed that the intranet, commonly used for communication, was perceived as ineffective and not user-friendly, leading to important updates being overlooked. Conversely, traditional methods such as flyers and more interactive training sessions proved to be more effective. For instance, in Company C, the use of a flyer was well-received, demonstrating that straightforward and direct communication methods can effectively convey important security messages.

6.2 Conclusion

By employing a comprehensive methodology that included a second round of mystery guest visits, documentation analysis, and interviews with employees about their perceived changes, this research aimed to answer the main research question:

How do mystery guest audits enhance the cyber awareness and organisational changes in public sector organisations?

To answer the question de definition of cyber awareness is described as “the degree of understanding of users about the importance of information security and their responsibilities and act to exercise sufficient levels of information security control to protect the organisation’s data and networks” (Zwilling et al., 2020). The mystery guest audits have proven to be a valuable tool in enhancing cybersecurity awareness and behaviour among employees. By combining formal and informal control recommendations from the mystery guest audit organisations enhanced their cyber awareness and created a robust cybersecurity culture. The mystery guest visit had such an impact on the employees that they naturally fostered a culture where employees began holding each other more accountable for security practices. As shown by Da Veiga (2020) and Parsons (2014) the peer support and the influence of key individuals became crucial in promoting adherence to security protocols and therefore bolstering the overall security posture of the organisation. This research concluded that conform the definition of cyber awareness physical controls do not enhance the cyber awareness of employees within a public organisation. Cyber awareness is defined as understanding and acting The findings highlight the need for continuous efforts to support employees in overcoming practical barriers to security adherence and integrating physical security measures with comprehensive training programs. Continued emphasis on clear, engaging communication strategies and the promotion of a supportive security culture are essential for maintaining and improving cybersecurity awareness in organisations. It has also shown that the method of delivering the mystery guest recommendations is crucial for reaching the right audience, which is also supported by research from May (2008). Organisations also showed change in creating their own approach to tackle the weaknesses that the mystery guest audit discovered. Some interventions are cyber awareness training, smart key cards that lock screens at a certain distance, and an attendance log to prevent unauthorised access.

6.3 Limitations

Despite the careful establishment of the validity and reliability of this research, there are several limitations that must be considered when interpreting the results.

First of all, the research employed a qualitative case study approach focusing on a limited number of public sector organisations. While this method allows for an in-depth understanding of specific contexts, it limits the ability to generalize findings across different types of organisations and sectors. The insights gained are highly contextual and may not be universally applicable. The unique characteristics and constraints of public sector organisations, such as regulatory requirements, data type, and organisational culture, may influence the applicability of the results to other settings. The study may not even be generalisable for large public sector organisations as this research performed a multiple case study for organisations with around 200-500 employees. The results may differ if an organisation like the municipality of Amsterdam was involved which has 15000 employees.

One notable limitation involves the scheduling of interviews by supervisors at two of the three companies where the mystery guest audits took place. In these instances, the supervisors were responsible for selecting and scheduling employees for interviews, which raises the possibility of selection bias. It is conceivable that the supervisors may have chosen employees who were more likely to provide positive feedback about the organisation in order to portray their company in a favourable light. This could have influenced the results, potentially skewing the findings towards a more positive outlook on the impact of the mystery guest audits. The decision to have supervisors schedule these interviews was primarily driven by time constraints. It was more time-efficient for the researcher to have interviews pre-arranged rather than approaching unknown individuals and scheduling interviews on the spot, which was the approach taken at company B. While this approach facilitated the completion of interviews within a shorter timeframe, it may have compromised the objectivity of the responses. Future research should consider alternative methods to ensure a more unbiased selection of interview participants.

6.4 Future Research

Future research should aim to address the limitations identified in this study to provide a more comprehensive understanding of the impact of mystery guest audits on cybersecurity awareness. One key area for further investigation is the potential selection bias introduced by having supervisors schedule interviews. Future studies should consider using random sampling methods to select interview participants to ensure a more representative sample of employees and reduce the risk of bias. Additionally, expanding the research to include a larger and more diverse sample of organisations from different sectors and sizes would enhance the generalisability of the findings. Longitudinal studies could also provide valuable insights into the long-term effects of mystery guest audits on cybersecurity awareness and behaviour. By tracking changes over an extended period, researchers can better understand the sustainability of the improvements observed in this study.

Another important area for future research is the integration of physical and cybersecurity measures. Exploring how these controls can be effectively combined and reinforced through comprehensive training programs would provide a more holistic approach to organisational security. Further investigation into the most effective communication strategies for delivering critical security messages is also needed. Comparing the efficacy of different methods, such as digital platforms, traditional media, and interactive training sessions, would help identify the best practices for ensuring that important information is communicated effectively and retained by employees.

An additional avenue for future research is to compare the effectiveness of different audit forms in creating cybersecurity awareness. Specifically, comparing the impact of mystery guest audits versus phishing campaigns can provide valuable insights into which method is more effective in raising awareness and promoting secure behaviours. Mystery guest audits involve real-life scenarios where an unknown individual tests the security practices of an organisation, which can highlight physical and procedural weaknesses. In contrast, phishing campaigns simulate cyber-attacks through deceptive emails to assess and improve employees' ability to recognise and respond to cyber threats.

6.5 Recommendations

This chapter aims to provide comprehensive recommendations to BDO on refining its approach to mystery guest audits. It also provides insight into the questions BDO had about the mystery guest audit. The questions were:

- Which recommendations from the mystery guest audit are being implemented by the clients?
- Do the companies implement other initiatives to tackle the cybersecurity? If so what initiatives are being implemented?

The results show that clients try to implement all the controls recommended by the mystery guest. This includes adding keypads to doors, restricted entrance to doors, clear screen and clean desk policy, and speak-up culture. The results from the second question of BDO show that there has only been one independent initiative implemented derived from the mystery guest audit. This initiative is a training addressing cyber threat which also includes the mystery guest recommendations. In addition to the implemented training, BDO's clients have considered their own initiatives. For instance, Company B is working on creating a keycard that locks the screen when it moves beyond a certain radius from the laptop. This addresses the clear screen policy and is intended for every employee to wear. This way, it is easy to identify who belongs to the organisation, and if someone is not wearing the keycard, they can be approached more quickly. Company C is because of the mystery guest audit trying to install a visitor registration system to tackle possible unauthorised visitors.

Now that the researcher has conducted multiple mystery guest visits and processed all the results, the researcher has the following recommendations for the mystery guest audit: The focus is on enhancing the delivery and communication of audit outcomes, introducing the USB drop tests. By addressing these areas, BDO can significantly amplify the impact of their audits, leading to a more secure and aware organisational environment.

1. **Improving Delivery Methods for Cybersecurity Awareness**

BDO should adopt a multi-channel communication strategy to ensure the comprehensive spreading of mystery guest audit findings and related security training materials. The results show the importance of a clear and effective delivery method. Therefore the researcher advises creating an option for the mystery guest audit where BDO will explain their findings by giving awareness training. In this training, the importance of cybersecurity and social engineering threats will be explained in combination with the real-life results of the mystery guest audit. These training sessions would also allow employees to discuss the content in-depth, ask questions, and engage in meaningful dialogue about the implications of the audit findings. Key components of these sessions include:

Real-time feedback and clarification by providing a platform for employees to get immediate clarification on any uncertainties, ensuring that all participants have a clear and accurate understanding of the training material and audit findings.
It also enhances learning through engagement by having interactive discussions and problem-solving sessions which can enhance the learning process, making it more likely that employees will retain and apply the information learned.
Scenario-based learning will bring real-life scenarios or hypothetical situations during these sessions which can help employees understand the practical application of policies and procedures, which improves their ability to respond to real incidents.

BDO can even combine the mystery guest with a phishing attack to tackle all sorts of social engineering attacks, physical and technical. The findings of these attacks can then be further explained in the training sessions to give the employees knowledge of different types of social engineering attacks.

Financial benefits
The financial benefits for BDO in implementing such a strategy include:
Client retention and satisfaction: Improved communication strategies lead to more effective security training and compliance, which in turn can reduce client vulnerability to cyber threats. Satisfied clients are more likely to continue their partnership with BDO, enhancing client retention and stable revenue streams.
Enhanced reputation: Effective communication strategies that lead to demonstrable security improvements can enhance BDO's reputation as a leader in cybersecurity consultancy. This reputation can translate into new client acquisitions and expansions into new markets.
Increased service offerings: BDO can package these interactive sessions as part of an enhanced service offering.

2. **Expanding Service Capabilities: USB drops**

To further enhance the effectiveness and realism of the mystery guest audits, BDO can integrate a USB drop as part of its service offerings. This involves strategically placing USB drives in common areas or near targeted employees within the client's organisation. These USBs would contain a benign script that simulates a network disruption or locks the system temporarily, demonstrating the potential consequences of inserting unverified USB drives into company devices.

Implementation Strategy
Controlled Simulation: The USB drives used in the drop test would contain a non-malicious, controlled script that, upon activation, simulates a significant system disruption but does not actually harm the system or steal data. For instance, the script could trigger a screen lock that can only be unlocked with a code provided by the Chief Information Security Officer (CISO).
Notification and Deactivation: To prevent actual disruption to work, the system would display a message explaining the simulation's purpose and instructing how to contact the CISO or IT department to deactivate the script and resume normal operations.

Educational Objectives

Awareness of Risks Associated with Unknown USBs: This test serves to educate employees about the dangers of using unknown USB drives, which could potentially carry malware capable of crippling organisational IT systems.

Promoting Secure Practices: Reinforces the need for policies regarding the use of external devices and encourages employees to report found USB drives to the IT department rather than inserting them into their computers.

Table 1: conclusion

Research Questions	Method	Output	Conclusion
RQ1: Which factors (e.g. formal controls, informal controls, physical controls) influence cyber awareness within public sector organisations?	Literature review conducted on the basket of the top 8 journals in the field of Information System (IS) Keywords used: "social engineering" "cyber awareness" "formal controls" "informal controls" "physical controls" "mystery guest"	350 articles, read the abstract selected 15 and went snowballing 4 articles, read fully and went snowballing	Formal and informal controls influence the cyber awareness of employees. No evidence found that physical controls enhance cyber awareness. No evidence was found on the existence of mystery guest audits in the cybersecurity realm
RQ2: How do mystery guest audits influence employees' cybersecurity awareness?	Qualitative research using three cases. Data collection through 2nd mystery guest, semi-structured interviews, and documents. Interview 19 participants.	Three successful mystery guest visits, gain access and not being revealed. Coding framework for interviews	The mystery guest audit influences the employee's cyber awareness by providing practical, real-life experiences that reinforce cybersecurity protocols and policies.
RQ3: Which control recommendation from the mystery guest or independent initiatives influences the cyber awareness within public sector organisations?	Qualitative research using three cases. Data collection through 2nd mystery guest, semi-structured interviews, and documents. Interview 19 participants.	Three successful mystery guest visits, gain access and not being revealed. Coding framework for interviews	Both formal and informal controls positively influence cyber awareness. Physical controls did not raise cyber awareness they only educated employees about the threats. No evidence was found that independent initiatives have increased the employee's cyber awareness.

7. References

- *Abawajy, J. (2012b). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248. https://doi.org/10.1080/0144929x.2012.708787*
- *Adeoye-Olatunde, O. A., & Olenik, N. L. (2021b). Research and scholarly methods: Semi-structured interviews. JACCP: Journal Of The American College Of Clinical Pharmacy, 4(10), 1358–1367. https://doi.org/10.1002/jac5.1441*
- *Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal Of Information Management, 35(6), 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001*
- *Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does Awareness of Social Engineering Make Employees More Secure? International Journal Of Computer Applications, 177(38), 45–49. https://doi.org/10.5120/ijca2020919891*
- *Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. IEEE. https://doi.org/10.1109/tale.2018.8615162*
- *Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. Computers in Industry, 100, 212–223. https://doi.org/10.1016/j.compind.2018.04.017*
- *Alshaikh, H., Ramadan, N., & Ahmed, H. (2020). Ransomware Prevention and Mitigation Techniques. International Journal Of Computer Applications, 177(40), 31–39. https://doi.org/10.5120/ijca2020919899*
- *Anderson, D., Groves, D., Lengfelder, J., & Timothy, D. J. (2001). A research approach to training: a case study of mystery guest methodology. International Journal of Contemporary Hospitality Management, 13(2), 93–102. https://doi.org/10.1108/09596110110381906*
- *Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. European Journal Of Information Systems, 26(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y*
- *Applegate, M. S. D. (2009). Social Engineering: Hacking the Wetware! Information Security Journal: A Global Perspective, 18(1), 40–46. https://doi.org/10.1080/19393550802623214*
- *Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. Information Management & Computer Security, 17(1), 53–63. https://doi.org/10.1108/09685220910944768*
- *Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers & Security, 39, 145–159. https://doi.org/10.1016/j.cose.2013.05.006*
- *Bichler, B. F., Pikkemaat, B., & Peters, M. (2020). Exploring the role of service quality, atmosphere and food for revisits in restaurants by using a e-mystery guest approach. Journal Of Hospitality And Tourism Insights, 4(3), 351–369. https://doi.org/10.1108/jhti-04-2020-0048*
- *Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal Of Information Systems, 18(2), 151–164. https://doi.org/10.1057/ejis.2009.8*

- *Bouwmeester, O. (2023). Lowering social desirability bias: Doing Jokes-Based interviews. Management Consulting Journal, 6(2), 78–90. https://doi.org/10.2478/mcj-2023-0010*
- *Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa*
- *Breda, F., Barbosa, H., & Morais, T. (2017). SOCIAL ENGINEERING AND CYBER SECURITY. INTED Proceedings. https://doi.org/10.21125/inted.2017.1008*
- *Brook, C. (2019, 1 november). Hacker faces jailtime after stealing employee, company data at two firms. Digitalguardian. Geraadpleegd op 2 juni 2024, van https://www.digitalguardian.com/blog/hacker-faces-jailtime-after-stealing-employee-company-data-two-firms*
- *Bullee, J., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information & Computer Security/Information And Computer Security, 25(5), 593–613. https://doi.org/10.1108/ics-03-2017-0009*
- *Chatchalermpun, S., & Daengsi, T. (2021). Improving cybersecurity awareness using phishing attack simulation. IOP Conference Series. Materials Science And Engineering, 1088(1), 012015. https://doi.org/10.1088/1757-899x/1088/1/012015*
- *Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science, 198, 656–661. https://doi.org/10.1016/j.procs.2021.12.302*
- *Conklin, A., & White, G. (2006). e-Government and Cyber Security: The Role of Cyber Security Exercises. IEEE. https://doi.org/10.1109/hicss.2006.133*
- *Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks. In Advances in information security, privacy, and ethics book series (pp. 19–31). https://doi.org/10.4018/978-1-7998-6504-9.ch002*
- *D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, 29(1), 43–69. https://doi.org/10.1111/isj.12173*
- *Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713*
- *Dawes, J. (2008). Do data characteristics change according to the number of scale points used? An experiment using 5-Point, 7-Point and 10-Point scales. International Journal of Market Research, 50(1), 61–104. https://doi.org/10.1177/147078530805000106*
- *Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal Of Information Security, 04(02), 92–100. https://doi.org/10.4236/jis.2013.42011*
- *Duman, Ş. A., Hayran, R., & Soğukpınar, İ. (2023). Impact Analysis and Performance Model of Social Engineering Techniques. IEEE. https://doi.org/10.1109/isdfs58141.2023.10131771*
- *Falade, P. V. (2023). Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. International Journal Of Scientific Research in Computer Science, Engineering And Information Technology, 185–198. https://doi.org/10.32628/cseit2390533*
- *Floridi, L. (2017). The Unsustainable Fragility of the Digital, and What to Do About It. Philosophy & Technology, 30(3), 259–261. https://doi.org/10.1007/s13347-017-0280-4*
- *García, J. E., Encinas, L. H., & Domínguez, A. P. (2021). A Comprehensive Security Framework Proposal to Contribute to Sustainability. Sustainability, 13(12), 6901. https://doi.org/10.3390/su13126901*

- *Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. Procedia Computer Science, 181, 59–66. https://doi.org/10.1016/j.procs.2021.01.103*
- *Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet. Group Decision And Negotiation, 13(2), 149–172. https://doi.org/10.1023/b:grup.0000021839.04093.5d*
- *Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. Computers & Security, 66, 52–65. https://doi.org/10.1016/j.cose.2016.12.016*
- *Heartfield, R., & Loukas, G. (2015). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Computing Surveys, 48(3), 1–39. https://doi.org/10.1145/2835375*
- *He, H., & Yan, J. (2016). Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-physical Systems, 1(1), 13–27. https://doi.org/10.1049/iet-cps.2016.0019*
- *Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007*
- *International Organization for Standardization [ISO]. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements. In International Organization For Standardization. International Organization for Standardization. https://www.iso.org/standard/27001*
- *Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal, 33(4), 377–409. https://doi.org/10.1108/maj-07-2017-1595*
- *Kaloudi, N., & Li, J. (2020). The AI-Based cyber threat landscape. ACM Computing Surveys, 53(1), 1–34. https://doi.org/10.1145/3372823*
- *Kanter, G. P., Kufahl, J., & Cohen, I. G. (2021). Beyond Security Patches—Fundamental incentive problems in health care Cybersecurity. JAMA Health Forum, 2(10), e212969. https://doi.org/10.1001/jamahealthforum.2021.2969*
- *Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804*
- *Khansa, L., Kuem, J., Siponen, M. T., & Kim, S. S. (2017). To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls. Journal Of Management Information Systems, 34(1), 141–176. https://doi.org/10.1080/07421222.2017.1297173*
- *Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors Related to Cyber Security Behavior. IEEE Access, 8, 125140–125148. https://doi.org/10.1109/access.2020.3007867*
- *Kreutzer, M., Cardinal, L. B., Walter, J., & Lechner, C. (2016). Formal and Informal Control as Complement or Substitute? The Role of the Task Environment. Strategy Science (Print), 1(4), 235–255. https://doi.org/10.1287/stsc.2016.0019*
- *Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal Of Information Security And Applications, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005*
- *Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. Journal Of Computing Sciences, 26(2), 80–87. https://doi.org/10.5555/1858583.1858595*

- *Kwak, D., Lee, S., Ma, X., Lee, J., Khansa, L., & Brandyberry, A. A. (2021). Announcement of formal controls as phase-shifting perceptions: their determinants and moderating role in the context of mobile loafing. Internet Research, 31(5), 1874–1898. https://doi.org/10.1108/intr-10-2020-0581*
- *Leach, J. (2003). Improving user security behaviour. Computers & Security, 22(8), 685–692. https://doi.org/10.1016/s0167-4048(03)00007-5*
- *Lee, C., & Lee, K. (2021). Factors affecting corporate Security policy effectiveness in telecommuting. Security And Communication Networks, 2021, 1–13. https://doi.org/10.1155/2021/2634817*
- *Li, L., He, W., Da Xu, L., Ash, I. K., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal Of Information Management, 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017*
- *Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security/Information And Computer Security, 30(2), 255–279. https://doi.org/10.1108/ics-06-2021-0091*
- *McCrohan, K. F., Engel, K. L., & Harvey, J. (2010). Influence of Awareness and Training on Cyber Security. Journal Of Internet Commerce, 9(1), 23–41. https://doi.org/10.1080/15332861.2010.487415*
- *Min, Z., Yang, G., Sangaiah, A. K., Bai, S., & Liu, G. (2019). A privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems. EURASIP Journal On Wireless Communications And Networking, 2019(1). https://doi.org/10.1186/s13638-018-1317-9*
- *Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. Management Information Systems Quarterly, 42(1), 285–311. https://doi.org/10.25300/misq/2018/13853*
- *Monteiro, J. J., Lunkes, R. J., & Da Rosa, F. S. (2022). Influence of formal and informal controls on trust and individual creativity. Journal Of Accounting & Organizational Change, 19(5), 689–705. https://doi.org/10.1108/jaoc-08-2021-0122*
- *Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. International Journal Of Information Management, 40, 54–66. https://doi.org/10.1016/j.ijinfomgt.2018.01.001*
- *Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal Of Information Systems, 18(2), 126–139. https://doi.org/10.1057/ejis.2009.10*
- *Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal Of Information Systems, 29(3), 306–321. https://doi.org/10.1080/0960085x.2020.1771222*
- *Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010*
- *Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Computing Surveys, 54(11s), 1–37. https://doi.org/10.1145/3514229*
- *Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack Detection and Identification in Cyber-Physical Systems. IEEE Transactions On Automatic Control, 58(11), 2715–2729. https://doi.org/10.1109/tac.2013.2266831*

- *Rahim, N. H. A., Hamid, S. B. B. O. A., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), 606–622. https://doi.org/10.1108/k-12-2014-0283*
- *Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-Security Incidents and Audit Quality. European Accounting Review, 31(3), 701–728. https://doi.org/10.1080/09638180.2020.1856162*
- *Roy, S., Sharmin, N., Acosta, J. C., Kiekintveld, C., & Lászka, Á. (2022). Survey and taxonomy of adversarial reconnaissance techniques. ACM Computing Surveys, 55(6), 1–38. https://doi.org/10.1145/3538704*
- *Rubio-Hernan, J., Sahay, R., De Cicco, L., & Garcia-Alfaro, J. (2018). Cyber-physical architecture assisted by programmable networking. Internet Technology Letters, 1(4). https://doi.org/10.1002/itl2.44*
- *Sas, M., Reniers, G., Ponnet, K., & Hardyns, W. (2021). The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. Safety Science, 144, 105447. https://doi.org/10.1016/j.ssci.2021.105447*
- *Senkyire, I. B., & Kester, Q. (2021). Social Engineering Cybercrime Evidence Analysis Using Formal Concept Analysis. IEEE. https://doi.org/10.1109/icsiot55070.2021.00014*
- *Satvat, K., Hosseini, M., & Shirvanian, M. (2018). Camouflaged with Size: A Case Study of Espionage using Acquirable Single-Board Computers. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1809.04112*
- *Smith, S., & Jamieson, R. (2006). Determining key factors in E-Government information system security. Information Systems Management, 23(2), 23–32. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92671.4*
- *Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, 33(4), 410–424. https://doi.org/10.1108/maj-07-2017-1596*
- *Stake, R. E. (1994). Case Study: Composition and Performance. Bulletin of the Council for Research in Music Education, 122, 31–44. http://www.jstor.org/stable/40318653*
- *Stibbe, M. (2005). E-government security. Infosecurity Today, 2(3), 8–10. https://doi.org/10.1016/s1742-6847(05)70272-x*
- *Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology, 29(3), 233–244. https://doi.org/10.1080/01449290903121386*
- *Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191–198. https://doi.org/10.1016/j.cose.2004.01.012*
- *Wang, M., Huang, K., Wang, Y., Wu, Z., & Du, Z. (2019). A novel side-channel analysis for physical-domain security in cyber-physical systems. International Journal Of Distributed Sensor Networks, 15(8), 155014771986786. https://doi.org/10.1177/1550147719867866b*
- *Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. IEEE Access, 8, 85094–85115. https://doi.org/10.1109/access.2020.2992807*
- *Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access, 9, 11895–11910. https://doi.org/10.1109/access.2021*
- *Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A Survey on Metaverse: Fundamentals, Security, and Privacy. IEEE Communications Surveys And Tutorials/IEEE Communications Surveys And Tutorials, 25(1), 319–352. https://doi.org/10.1109/comst.2022.3202047*

- *Wen, S., Kianpour, M., & Kowalski, S. (2019). An empirical study of security culture in open source software communities. IEEE. https://doi.org/10.1145/3341161.3343520*
- *Wiener, M., Mähring, M., Remus, U., & Saunders, C. (2016). Control Configuration and Control Enactment in Information Systems Projects: Review and Expanded Theoretical Framework. Management Information Systems Quarterly, 40(3), 741–774. https://doi.org/10.25300/misq/2016/40.3.11*
- *Wirtz, B. W., & Weyerer, J. C. (2016). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. International Journal of Public Administration, 40(13), 1085–1100. https://doi.org/10.1080/01900692.2016.1242614*
- *Yang, J., Liu, X., & Bose, S. (2015). Preventing Cyber-induced Irreversible Physical Damage to Cyber-Physical Systems. ACM Transactions On Information Systems Information Systems. https://doi.org/10.1145/2746266.2746274*
- *Zheng, B., Deng, P., Anguluri, R., Zhu, Q., & Pasqualetti, F. (2016). Cross-Layer Codesign for Secure Cyber-Physical Systems. IEEE Transactions On Computer-aided Design Of Integrated Circuits And Systems, 35(5), 699–711. https://doi.org/10.1109/tcad.2016.2523937*

8. Appendix

8.1 Appendix I, Company Information

	Company A	Company B	Company C
Company type	Municipalities (Noord-Brabant)	Municipalities (Noord-Brabant)	Medical group of general practitioners (Overijssel)
Number of employees	≈200	≈500	≈200
Interviewees	6	6	6
Most common data/information	Citizen data	Citizen data	Patient data
Mystery guest infiltration site	Main offices	Main offices	Main offices

8.2 Appendix II, Flyer Mystery Guest Visit

Mystery guest bezoek

De mystery guest

In opdracht van de CIO heeft een mystery guest….. bezocht. Doel: onderzoeken of hij ongeautoriseerd het pand kon binnenkomen en vertrouwelijke informatie kon vinden. Dat is gelukt. Op 9 april is de mystery guest langs geweest en heeft zich uitgebreid door het pand …….bewogen zonder verwijderd te worden. Daarnaast heeft hij diverse ruimtes kunnen betreden en lades en archieven met documentatie kunnen inzien of de mogelijkheid gehad om deze mee te nemen."

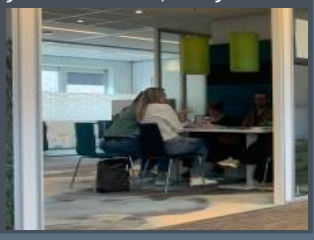
Adviezen

- Denk aan het drukken op Windsows+L bij het verlaten van je werkplek en het niet onbeheerd achterlaten van gevoelige informatie op je bureau.
- Spreek onbekenden aan om te achterhalen wat hun bij ….. brengt.
- Let op wie mee loopt bij binnentreden van het kantoor.
- Sluit alle lades en kasten.

Aanspreek cultuur

Bij de binnenkomst heeft de mystery guest zich niet hoeven te identificeren. Ook heeft hij vrij rond kunnen lopen op zoek naar informatie. Wel is de mystery guest twee keer aangesproken met de vraag wie hij is. Er is dus wel een aanzet tot een aanspreekcultuur bij ……., maar deze kan zich nog verder ontwikkelen.

Aanbeveling: Onbekenden aanspreken is lastig. Door dit toch te doen, door bijvoorbeeld te vragen wat iemand bij…… komt doen, kan je mee voorkomen dat onbekenden zich door het pand bewegen. Bij collega's navragen of zij iemand kennen kan hierbij ook helpen.



Toegankelijkheid

Door achter medewerkers aan te lopen en aan te bellen heeft de mystery guest toegang gekregen tot de kantoorruimtes en…. afdeling. Daarnaast heeft hij aan elke kast en laden gevoeld om te kijken of ze afgesloten waren.

Risico's

- Het kunnen vergaren van gevoelige (patiënt)informatie uit werkruimten
- Het kunnen verkrijgen van digitale toegang via aanwezige werkstations

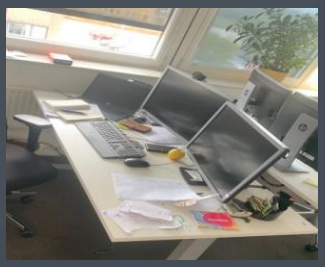
Aanbevelingen

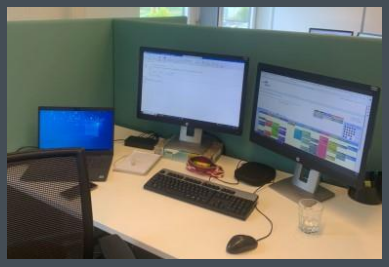
Let op wie mee loopt bij het binnentreden van het kantoor. Vergrendel alle laden en kasten en vergeet de sleutel niet van de kast/la te halen.

Clean desk en clear screen

De mystery guest trof meerdere bureaus aan met open notitieblokken en gevoelige informatie die hij zo mee kon nemen. Daarnaast trof de mystery guest ook schermen aan die niet vergrendeld waren en waar hij zo toegang toe had kunnen krijgen.

Het risico is dat ongeautoriseerde gevoelige informatie kunnen vergaren, of bijvoorbeeld ransomware installeren.





VRAGEN? ……

8.3 Appendix III, Interview Guide

- Question 1(supervisor): What was the objective of the first mystery guest visit and how did it happen?
- Question 1(employees): Do you remember the first mystery guest visit?
    - Yes, what do you remember?
    - No, then I will give a quick recap of the visit
- Question 2: Can you describe the specific changes or initiatives your organization has implemented in response to the mystery guest audit recommendations?
- Question 3: Can you provide examples of how these changes have been integrated into your organization's daily operations or culture?
- Question 4: In addition to the immediate recommendations from the mystery guest audit, what additional cybersecurity initiatives has your organisation undertaken?
- Question 5: What motivated these additional initiatives?
- Questions 6: Have you noticed any changes in formal controls such as policies, procedures, training, etc? if so how did they affect you?
- Questions 7: Have you noticed changes in the area of informal controls such as culture and social control? if so how did they affect you?
- Questions 8: Have you noticed changes in the area of physical checks such as access passes? if so how did they affect you?
- Question 9: Which of the past changes had the most influence on your cyber awareness and why?

8.4 Appendix IV, Coded Interview Table

Quotation	Themes	Source
Good action to be more aware of awareness and to address each other and strangers.	Awareness refreshment	Interview 15
I try to check who it is, but I find it difficult to ask where the person comes from and whether he or she works here because that seems strange.	Awareness refreshment	Interview 10
Everyone has become more aware of it, but you do notice it. That some things. Yes, it can sometimes slip through.	Awareness refreshment	Interview 3
Awareness in general was also important. As a refresher then.	Awareness refreshment	Interview 3
And you notice that some people did not yet know about the recommendations because people often work from home and missed it, so the flyer helps some colleagues, but I already knew about them.	Awareness refreshment	Interview 6
Well, that mystery guest flyer report did help me refresh the closing screen	Awareness refreshment	Interview 7
Well, the clear screen and clean desk policy has simply been brought back for refreshment, so I have seen a change in that	Awareness refreshment	Interview 7
They certainly become more aware of it through the mystery guest visit	Awareness refreshment	Interview 8
Yes, you now see a lot more black screens when you walk around, that wasn't the case before	Change in awareness	Interview 10
Yes, certainly, as I just said, I also try to emphasize this to new employees, so to speak, because you feel kind of responsible.	Change in awareness	Interview 10
But I think you pay a little more attention now than you did before, But I would especially when I'm alone.	Change in awareness	Interview 11
Everyone has become more aware of it, but you do notice it. That some things. Yes, it can sometimes slip through.	Change in awareness	Interview 3
Awareness in general was also important. As a refresher then.	Change in awareness	Interview 3
And you notice that some people did not yet know about the recommendations because people often work from home, so that helps some colleagues, but I already knew about them.	Change in awareness	Interview 6

No, I don't know anything about a mystery guest visit	Communication error	Interview 4
I think there is sufficient communication internally, but there is a lot of communication about many topics. So what sticks with you, huh?	Communication error	Interview 7
I was busy and didn't look at the intranet because it doesn't really contain the most important information and I certainly don't go through the entire intranet to see if I missed something.	Communication error	Interview 9
Of course I don't always succeed because I will undoubtedly have forgotten it, but I think about it much more often now	Difficult to adhere	Interview 10
it's always a little awkward to stop someone and ask who they are, especially when it seems like they're just there to do their job.	Difficult to adhere	Interview 10
Yes indeed, and so many people work here, I know many of them, but I certainly don't know them all, so that is difficult, yes, even though I keep an eye on my laggard every morning when I enter	Difficult to adhere	Interview 10
Yes I have that too. I have certainly become more aware of the physical checks within our company, but to be honest, I sometimes find it difficult to approach people about this.	Difficult to adhere	Interview 10
Well, I find that very difficult, because there are so many people walking around.	Difficult to adhere	Interview 13
Yes, that is quite difficult because there are sometimes some higher placed people walking around and I see people just hesitate to approach them.	Difficult to adhere	Interview 14
I try to check who it is, but I find it difficult to ask where the person comes from and whether he or she works here because that seems strange.	Difficult to adhere	Interview 9
After the mystery guest visit I never actually see anything un the bureau's when I leave. I'm usually one of the last, but there's no stuff lying around or papers or anything.	Formal controls	Interview 1
That is a difference from before because the mystery guest visited us. You now notice that everyone closes their screen as much as possible, even though this does not always happen, but it is of course not waterproof either.	Formal controls	Interview 1
Every time I leave my desk, I close everything and keep it clean and I try to pass that on to new employees	Formal controls	Interview 10
Keeping it clean. Can I indicate with my hand on my heart that I do that.	Formal controls	Interview 12
But I do believe that since then, well, really, because of the Mystery Guests, I have been a little quicker to enable my Windows lock and then walk away.	Formal controls	Interview 13
Well, lock the screen, yes, because as I just said, I have never done that before, so that is what I have become most aware of and also generally more aware.	Formal controls	Interview 2
In any case, those cards can also give a kind of signal when they are within a certain distance of the laptops, so that the laptop will also be automatically locked	Formal controls	Interview 4
Well, that flyer report did help me refresh the closing screen	Formal controls	Interview 7
Well, the clear screen and clean desk policy has simply been brought back for refreshment, so I have seen a change in that	Formal controls	Interview 7
I wasn't there when the first mystery guest arrived, so it was nice that (the name of the person) helped me with the rules and such.	Informal controls	Interview 10
it is true that (Name) did indeed help us with the culture of turning your screen black and keeping your desk clean if that is also seen as culture	Informal controls	Interview 10
Every time I leave my desk, I close everything and keep it clean and I try to pass that on to new employees	Informal controls	Interview 10
We sent an email on his behalf that he would be bringing cake the next day.	Informal controls	Interview 11
We have certainly had it all together in response to your message on Connect and discussed the recommendations	Informal controls	Interview 13

Yes, some people say, oh, I still have to lock my screen, or you just see that it becomes a kind of automatic.	Informal controls	Interview 2
And you notice that some people did not yet know about the recommendations because people often work from home, so that helps some colleagues, but I already knew about them.	Informal controls	Interview 6
If someone does not lock his screen, an email will be sent to everyone on the team there to ensure that the sausage roll must be collected.	Informal controls	Interview 8
a "vergeet me nietje" post it will be put on the screens if it was not locked	Informal controls	Interview 8
Within my department, if someone leaves a computer unlocked, they will always be spoken to if someone else sees it there or if key cards are visible somewhere, for example while they are in a meeting or go to the toilet, then this is also discussed afterwards.	Informal controls	Interview 8
I have the same thing because I am more aware of shutting down my computer, but that is more because of employees like you (pointing to his colleague) who tell me that I have to do it	Informal controls	Interview 9
the culture helps the most with being aware. I tell others to lock their screen and that makes him do it without me being present.	Informal controls	Interview 9
Probably because it's a fun thing to talk about. Such a mystery guest visit is something, how do you say unique, because it really comes close	Informal controls	Interview 9
Then I heard that someone came in and was addressed by… from ICT. He says, Gosh, who are you and why do you come here?	Physical control	Interview 15
It's just that you are even more aware of that when you just see people you don't know. That you just ask	Physical control	Interview 1
Yes, I do see that I and others are paying more attention to who we let in	Physical control	Interview 10
Yes I have that too. I have certainly become more aware of the physical checks within our company, but to be honest, I sometimes find it difficult to approach people about this.	Physical control	Interview 10
But I think you pay a little more attention now than you did before, But I would especially when I'm alone.	Physical control	Interview 11
Well, I honestly never thought about the fact that someone walks around like that, so I do plan to do something about it.	Physical control	Interview 12
Politeness is one thing, but if you have doubts about whether a colleague is a colleague, you can simply say so in a friendly way.	Physical control	Interview 3
It is true that the tips to look behind me do help me. When I walk in, do I look behind me?	Physical control	Interview 7
I don't let people tag along if I don't know them. Even though I don't know everyone here	Physical control	Interview 7
We have been working on a system so that people have to register. This allows you to better check who is who, which is also useful because I am a bhver	Recommendations	Interview 14
Well we figured it out, oh yes, it really was a really good training	Recommendations	Interview 2
In any case, those cards can also give a kind of signal when they are within a certain distance of the laptops, so that the laptop will also be automatically locked	Recommendations	Interview 4
We conducted an awareness training about Information Security and Privacy through the mystery guest and it actually explains what happened to the mystery guest. This is done by also showing the video with the recommendations in it.	Recommendations	Interview 5
Yes, we get good feedback on the training that it is at least a bit fresh and not long-winded	Recommendations	Interview 5
There is certainly an intranet message every month. Repeating things or connecting them to current events	Recommendations	Interview 6

What's funny is the clear screen and desk policy is on your screen when you close your screen, so you remember it better.	Recommendations	Interview 7
That pub quiz helped bring information security and privacy. it was really fun.	Recommendations	Interview 8

8.5 Appendix V, mystery guest visits

Mystery guest audit company A

These recommendations are tested two years later with the arrival of the second mystery guest. Similar to the first visit the mystery guest is able to enter the building and offices of company A by tailgating employees. This gives an indication that the recommendations of tackling the speak up culture and accessibility have not fully worked. Although the mystery guest was once again able to infiltrate the company it was significantly harder to manoeuvre through the building as the company installed more doors with keypads which made it harder for unauthorized personnel to wander around. Even though there were extra doors with keypads installed within the offices the office of the mayor and management was unlocked. This made it easy for the mystery guest to enter their offices and find a document sent from the ministry about subsidies. In the four hours that the mystery guest was undercover, he was only approached once. The employee introduced herself and was curious about who the mystery guest was because she had not seen him before. Here the mystery guest used his fabricated identity to trick the curious employee into thinking he was doing some cyber-related checks.

Contrary to the first audit, the compliance towards the clean desk and clear screen policy is much better. During the five hours of being undercover, the researcher has only found one person not locking their screen when leaving their workstation, even though this person locked their screen multiple times that day.

Mystery guest audit company B

During the second mystery guest audit, the mystery guest successfully gained entry into the building by tailgating an employee. The employee, upon noticing an unfamiliar face, looked back disapprovingly but did not confront the mystery guest. Feeling apprehensive about being caught, the mystery guest chose not to follow this person further to avoid a potential confrontation. After waiting inside for a period, the guest proceeded to follow another individual through a locked door and an access-controlled elevator to reach the office area of the building. Here the mystery guest was once again not confronted by the employee.

Throughout the visit, the mystery guest was approached only once for occupying a reserved space. However, he was able to move freely around the premises, inspecting cabinets containing critical information regarding various banking details and tax documents. Ultimately, it was observed that the clean desk and clear screen policies were generally well enforced, with only one instance of an unlocked screen noted.

Mystery guest audit company C

During the second mystery guest audit at company C the mystery guest once again the mystery guest was able to enter the premises by tailgating employees. When entering the offices the mystery

guest was able to access an unattended workstation and plug his laptop into the workstation and access their local Wi-Fi. During the whole stay, the mystery guest was only approached ones by a curious employee who had not seen the face of the mystery guest. The mystery guest was able to deflect the conversation after he gave a fake name and the employee went her way after not asking what his business was at the company. During their time at the company, the mystery guest was able to walk freely throughout the offices and even left the building to go to the toilet and gain access by tailgating again. The toilet was outside of the office's physical security measure (door with keypad). During the visit, the mystery guest was able to see one screen left unlocked which is a significant change in contrast to the first mystery guest audit. After being 4 hours at the company the mystery guest left without being discovered.