TOWARDS A RESILIENT WORKFORCE

A DEMOGRAPHIC APPROACH TO TARGETED CYBERSECURITY TRAINING

Haji, N - 5915856

Master Science and Business Management

Utrecht University

EY Utrecht

Primary supervisor: **Marten de Bruin**

Academic supervisor: **Bart Verkade**

Internship period: September 4th, 2023 – January 31st, 2024

Table of contents

Management Summary

Ernst & Young Global Limited (EY), an industry giant in professional services since its inception in 1903, has transformed and expanded over the years, solidifying its position as a key player in assurance, tax, transaction, and advisory services. The firm rebranded as 'EY' in 2013 to underscore its global presence and the comprehensive array of services it offers (1). Under the leadership of Global Chairman and CEO Carmine di Sibio, who assumed the role on July 1st, 2019, and Chief Financial Officer Jamie Miller, appointed in 2023, EY continues to thrive and innovate in a dynamic market.

Global Presence and Organizational Structure

As one of the 'big four' firms globally, EY, alongside Deloitte, KPMG, and PwC, plays a critical role in delivering financial and advisory support to a diverse clientele. The firm operates in over 150 countries, organized into three key regions: Americas, EMEIA (Europe, Middle East, India, and Africa), and Asia Pacific (1). The extensive EY network comprises 312,250 employees spread across more than 700 offices globally.

Awards and Recognitions

EY's commitment to excellence is reflected in numerous accolades, including being listed on 'Fortune's 100 Best Companies to Work For®' and the 'LinkedIN Top Companies List' (2). These accolades underscore EY's dedication to fostering a positive workplace environment and providing outstanding service to its clients. For a comprehensive list of EY's achievements and awards, you can refer to the 'Accomplishments and Accolades' page on their official website (3).

Core Services

EY's services are diverse, covering assurance, tax, transaction, and advisory functions. The company's primary focus on audit and assurance involves a meticulous examination of financial statements, internal controls, and financial reporting processes. This ensures compliance with accounting standards, providing stakeholders, including investors and shareholders, with confidence in the accuracy of financial information.

In the realm of IT audit and assurance, EY plays a crucial role in safeguarding businesses against the escalating threats of the digital age. The IT Assurance service analyzes, evaluates, tests, and secures IT systems, mitigating risks associated with unauthorized access, data breaches, and other malicious activities.

IT Audit and Risk Assurance at EY

In the dynamic realm of digital business, Ernst & Young Global Limited (EY) stands as a key player in providing comprehensive IT Audit and Risk Assurance services. EY's strategic approach to IT security and data integrity is instrumental in navigating the complex challenges posed by cybersecurity threats and ensuring the robustness of information technology systems.

Cybersecurity and IT Assurance

EY's IT Assurance service is at the forefront of safeguarding organizations against the escalating threats of unauthorized access, data breaches, and cyber-attacks. The service entails a thorough analysis, evaluation, and testing of IT systems to fortify them against emerging risks. Through penetration testing and vulnerability assessments, EY's experts collaborate with clients to develop tailored strategies that align with business objectives, ensuring not only security but resilience in the face of evolving cyber threats.

IT Audit Services

EY's IT Audit services provide a meticulous review of annual accounts, data security measures, and the seamless migration of operating systems. Annual accounts undergo detailed scrutiny to ensure accuracy, compliance with industry standards, and identification of potential financial risks associated with IT systems. EY's experts evaluate and enhance data security protocols, incorporating the latest advancements in cybersecurity to mitigate risks associated with data breaches.

Operating System Migration

EY's IT Audit experts play a crucial role in guiding businesses through the intricate process of operating system migration. Their meticulous planning and execution minimize the risk of data corruption or loss during transitions and upgrades. This focused attention ensures a smooth and secure migration, critical for businesses contemplating changes to their operating systems.

Continuous Improvement and Adaptability

Recognizing the dynamic nature of the IT landscape, EY emphasizes a culture of continuous improvement. The company stays abreast of emerging technologies, industry best practices, and evolving regulatory requirements. This adaptive approach ensures that EY's clients benefit from IT frameworks that remain resilient and capable of withstanding the challenges posed by the ever-changing digital environment.

Corporate Responsibility and Sustainability Initiatives

In 2023, corporate responsibility has become a defining aspect of a company's identity. EY acknowledges this imperative and has embraced the United Nations Global Compact (UNGC) principles, guiding its commitment to advancing the Sustainable Development Goals (SDGs) through the EY Ripples program (4). This initiative encourages EY members and staff to dedicate their time and expertise to projects aligned with the SDGs, with the ambitious goal of positively impacting one billion lives by 2030.

EY is not only committed to meeting UNGC principles but also strives for excellence in corporate responsibility, inclusiveness, and sustainability. This commitment encompasses global initiatives focusing on human rights and working towards a net-zero future. Collaborating with clients and similar organizations, EY leverages its distinctive skills, knowledge, and experience to drive positive change in three main areas: supporting the next generation workforce, working with impact entrepreneurs, and accelerating environmental sustainability.

EY's unwavering commitment to excellence, global impact, and corporate responsibility positions it as a formidable force in the professional services industry, with a vision for a sustainable and inclusive future. The company's rich history, global footprint, leadership, and diverse service offerings contribute to its continued success and influence in *shaping a better working world*.

1. Introduction

In an era characterized by an ever-increasing reliance on information technology (IT), organizations globally are finding themselves in the crosshairs of malicious individuals or groups. These adversaries execute sophisticated cyber-attacks that not only lead to financial losses but also inflict severe damage on an organization's reputation and overall well-being (5). As IT seamlessly integrates into daily operations worldwide, the associated risks have grown exponentially. Despite organizations' concerted efforts to fortify their IT environments, a considerable number fall victim to cyber threats. A study by Von Solms emphasizes that many organizations grapple with limited control over their IT infrastructure, rendering them susceptible to exploitation (5).

1.1 Inadequacies in Security Measures

One of the primary challenges organizations face stems from the insufficient implementation of robust security safeguards. The vulnerability of IT systems and networks becomes apparent when proper security measures are lacking, making these entities easy targets for cyber-attacks (5). Often, organizations are equipped just sufficient enough with proper cybersecurity measures, but many vulnerabilities are present without the knowledge of the organization themselves. They often notice the weakness in their security when it's already exploited and are left fighting off the attackers with a disadvantage from the start. These attacks are referred to as ***zero-day*** attacks (6).

1.2 Escalation of cyber-attacks

The menace of cyber-attacks has witnessed a marked increase in recent years, as evidenced by a study conducted among rural area citizens, shedding light on cyber security awareness and its related factors (7). In addition, the European Union Agency for Cybersecurity (ENISA) reported an increase in different types of cyber-attacks (8). These range from a ‘simple virus’ up to complex, multi-layered supply-chain attacks. The sophistication of hackers and the evolution of third-party threats have reached a point where entire organizations can be infiltrated remotely, leaving them vulnerable to a myriad of potential damages. In this context, it becomes imperative for organizations to not only acknowledge the escalating cyber threats but also to fortify their cybersecurity posture. The subsequent sections of this research will delve into the intricacies of information security awareness and the factors influencing safe behaviour, which entails adopting a range of actions and practices to minimize the risk of falling victim to cyber threats, aiming to propose an effective strategy to mitigate the evolving risks associated with the burgeoning IT landscape.

1.3 Current information security landscape

ENISA recently reported on the current state of the cybersecurity threat landscape. The report mainly identifies prime threats and major trends, with respect to the threat actors and their techniques (9). Some of the top threats are mentioned and described below:

- **Ransomware:** a type of malware (= malicious software) that locks a victim's data and/or device and keeps it locked, until the victim pays a ransom to the attacking party, often in monetary form (10). An example of such an attack is the clop ransomware attack on Maastricht University. An operational employee unsuspiciously opened a phishing mail, which resulted in a complete lock-out of their files. In under 30 minutes, the attacking party managed to lock down data of 267 servers at the university, including critical systems (11). In addition, the same ransomware attack was performed at Utrecht University, but because of the safeguards (anti-ransomware software) they implemented 2 years earlier, they were sufficiently protected against this threat (12).

- **Social Engineering:** These attacks are focused on manipulating individuals into divulging information they shouldn't share, downloading unauthorized software, or visiting websites they should avoid. Attackers employ psychological manipulation with the aim of exploiting human errors and weaknesses, rather than targeting technical vulnerabilities. This may also involve providing unauthorized access, where a victim unintentionally grants access that would not otherwise be given (13).

- **Threats against availability:** through this way, attackers try to disrupt organizational systems and their availability by destruction of their IT infrastructure, complete outages and/or rerouting of internet traffic. This is often done through **DDoS** (distributed denial of service) attacks, which causes a large influx and pressure on the servers of an organization, resulting in outages or downtime of their servers, which could be critical to their business (14).

- **Supply chain targeting:** this entails an attack on a business' supply chain. The hard part is that for these types of targeting, there is no 'one cure'. Supply chain security is challenging since it's a multi-disciplinary problem which requires accurate collaboration between multiple teams within an organization, in addition to constant moderation. All in all, it's a disruption of the "plan, make and deliver" theory which supply chains rely on (15).

These are just examples of a few modus operandi of cyber-attacks or data breaches that are out there. In practice, a lot of different types of cyber-attacks and data breaches occur on a daily basis, often in a set of combinations (16). For example, sending out a phishing mail is a type of social engineering. Upon opening the bad URL in the phishing mail, some sort of ransomware can be used to inflict damages. Often, the purpose of these cyber-attacks is financial gain for the attacking party, while the attacked party undergoes financial and reputational damage. In some cases, cyber-attacks have military or political purposes (17,18).

Over the past years, cyber-attacks and data breaches have been increasing significantly, as confirmed by several researchers (19–21). Because cyberwarfare entails a multitude of different types and styles, each with different purposes, we will categorize and define the two main types: ‘Cyber attacks’ and ‘Data breaches’. These definitions are given by CISCO, a prominent digital communications technology conglomerate corporation.

- **Cyber-attack**: “A malicious and deliberate attempt by an individual or organization to breach the information system or another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network.” (22).

- **Data breach**: “A security violation or incident that leads to the theft of sensitive or critical data or its exposure to an unauthorized party. These incidents can be intentional, such as a database hack, or accidental, such as an employee emailing confidential files to the wrong recipient.’ (23).

Despite both definitions having a lot of overlap, it is important to note that there is a significant difference in both. A data breach is nearly always a result of some form of a cyber-attack, but cyber-attacks do not always end up being data breaches. For example, the ransomware attack mentioned earlier in this thesis does not always have to conclude in a data breach, since ‘locking out’ an organization's system can be enough to cause severe damage to their business, without actually stealing any of their data.

1.4 The importance of cybersecurity and data breaches

To create an understanding of the importance of cyber-attacks and data breaches, a few examples of such attacks in the past will be explained with their concurrent risks and damages. In 2013, the hacktivist collective Anonymous launched a series of successful cyberattacks upon the Singapore government, as a response to web censorship regulations within the country. From governmental websites to airport networks, the country's infrastructure was under big threat, with potentially billions in damage to be done. An example of a big data breach can be seen at MasterCard. The globally known payment-processing corporation had one of its payment processors hacked in 2005, resulting in an announcement of the company stating that up to 40 million cardholders may have had their information stolen. In 2013, the American retail corporation Target was attacked and approximately 110 million Target customers were compromised. These examples show the devastating impact it can have on people financially, but also in their confidence in the organization's integrity. As a consequence, the reputational damage done to these organizations could cause for a lot of customers to end their business with the corporations, again resulting in even more financial loss. In order for organizations to properly protect their cyber landscape, proper safeguards have to be put in place. To know which safeguards are needed, we need to zoom in to the underlying properties of cyber-attacks and data breaches. A dominating definition regarding information security found in a lot of literature is the ‘CIA’ definition (24). It is based upon the following properties:

- **Confidentiality**: ‘Property that information is not made available or disclosed to unauthorized individuals, entities or processes.'

- **Integrity:** 'Property of accuracy and completeness.’

- **Availability:** ‘Property of being accessible and usable upon demand by an authorized entity.’

If any of these properties are not sufficiently safeguarded through appropriate information security measures, it would be considered as unsecure and available to expose. It is therefore important to implement the proper safeguards to abide by those three properties. But, in order to effectively mitigate the risks to these three information security properties, we need to know where the exposure lies and where the main causes of cyber-attacks and data breaches actually come from.

1.5 The root cause of cyber-attacks and data breaches

For a long period of time, information security was a concept that should be achieved solely through technical measures. However, this approach of information security omits the critical role human behaviour plays in keeping information safe. In up to 88% of the time human behaviour plays an important role in the exploitation of an organization's IT infrastructure (25). In addition, the EY Global Information Security Survey in 2018-2019 reported that 34% of organizations think that careless/unaware employees are the biggest cause of cybersecurity incidents (26). Cyber-attacks and data breaches are thus often a result of human mistakes, albeit accidental or intentional (27).
While human errors indeed contribute significantly to cybersecurity challenges, it's crucial to acknowledge that technical vulnerabilities within an organization's IT infrastructure also play a

pivotal role. For instance, the risk of ransomware can be directly linked to existing technical vulnerabilities. In this context, it's essential to emphasize that even measures traditionally viewed as purely technical, such as patching, have a human component. Administrators, for example, must demonstrate safe behaviour by consistently implementing patching protocols to mitigate vulnerabilities effectively. Consequently, a comprehensive approach to cybersecurity necessitates considering both the technical maturity of the organization and the human aspects involved in maintaining a secure IT environment.

In this section, we will look into and discuss the most important different types of human-led root causes resulting in cyber-attacks and/or data breaches (28):

- **Phishing attacks** aim to deceive users through sophisticated means. These deceptive tactics involve fraudulent emails, text messages, phone calls, or counterfeit websites meticulously crafted to closely resemble genuine, authentic counterparts. While most email hosting providers offer built-in phishing and spam filters, successful phishing attacks can result in serious consequences, including identity theft, credit card fraud, ransomware attacks, data breaches, and substantial financial losses for both individuals and organizations (29). Phishing, as a form of social engineering, heavily relies on human error. The earlier-discussed Maastricht University breach serves as a notable example, illustrating how a simple human error can inflict significant damage.

- **Malware** attacks rely on human error as well but can also be packaged in legitimate software, which is almost impossible to detect without proper anti-virus software or firewall settings. Malware attacks often contain keyloggers or a similar form of spyware, which records sensitive credentials and data such as login usernames and password, which are accessible to the attacking party. However, malware can also be packaged into a phishing email where an organization's employee or an individual is tricked into clicking a malicious link, instantly installing malware onto the device or network.

- **Hacking**, as one of the oldest modus operandi for cyberattacks, poses a significant threat. Individuals who neglect regular password updates, fail to meet password criteria, or bypass two-factor authentication become susceptible to hacking attacks. These attacks, often driven by financial motives, may employ brute force techniques to breach employee credentials and access sensitive data. With the vast computing power available today, hackers can simultaneously attempt thousands of password combinations, rendering seemingly simplistic passwords like "ABCDEFG," "1234567," or "0000000" susceptible to cracking within seconds. Beyond unauthorized access, hackers can remotely install additional malware by exploiting compromised credentials, thereby escalating their control over an organization's IT infrastructure. On a positive note, ethical hackers, either individuals or groups, actively search for vulnerabilities within an organization's IT framework. Their role involves identifying weaknesses and promptly addressing them to minimize the risk of exposure. Conversely, 'hacktivist' groups such as Anonymous represent another category of hackers, often motivated by social and political causes.

- **Botnet attacks** involve the utilization of devices that come pre-installed with complex malicious programs, such as malware, viruses, and worms. These programs execute destructive actions covertly, operating without the user's awareness (30). Typically, these devices are programmed to execute activities like phishing scams, DDoS attacks, and other disruptive manoeuvres. The primary objective is to overwhelm IT network servers, ultimately leading to the incapacitation of an organization's operational capabilities.

- **Business email compromise (BEC)** threats are one the most damaging types of cybercrime in terms of financial damage (31,32). Others than the actual attack methods mentioned above, BEC are more a result of extortion/abuse of unauthorized access. Nevertheless, it is worth mentioning this type of abuse, since the rate of financial crimes via this method has been increasing recently (33–36). An example of a BEC fraud mentioned by Alawida et al. is an instance where hackers posing as officials from the World Health Organization (WHO) sent out emails and messages about the COVID-19 pandemic explaining that the attachment supplied in the e-mail gave tips on how to stop the disease from spreading. In reality, the attachment contained no relevant information but instead infected the devices of the organization with malware, specifically a keylogger, which allowed the attackers to track their victims’ online activities.

These abovementioned instances, merely skimming the surface of the vast landscape of today's cybercrime potential, underscore the substantial damage that can result from either unintentional or deliberate human errors. This realization prompts a critical question into how we can effectively mitigate the pervasive risks that exist. Subsequently, we will delve into addressing the existing research gap and propose strategies to enhance safe behaviour among individuals in the realms of information security and information handling.

1.6 The current knowledge

Information security is a fairly hot topic. Many researchers try to tackle and review issues regarding information security from many different perspectives. A lot of complex, technical safeguards are in place, which can be updated by better and more secure code, but these technical safeguards have a limit when it comes to effectiveness. The biggest part lies in the hands of human behaviour – employees who are either aware or unaware of the risks they take in their daily work. Thus, we have noticed a shift from attacking IT infrastructures to attacks aimed on exploiting human vulnerabilities (37). Although technical solutions can be of aid in reducing the risk and consequences of cyber-attacks, it has been found that focusing on the human aspect of information security plays an important role in cybersecurity, in particular research into factors that influence an individuals' safe behaviour in information security (38). Furthermore, it is stated that there is a need in researching human, organisational and training factors if the problem of security breaches is to be managed effectively (39).

In recent years, research into human behaviour has been increasing. A lot of literature is arising researching all kinds of human demographic factors, from age to gender, and how it correlates to safe behaviour in information handling. However, a lot of research has been done into the *intentional behaviour* of a human being into showing safe behaviour, rather than studying actual safe behaviour and correlations between the different factors. This is fairly hard to measure, since the intention to comply, or in general intention is very hard to measure. It is safe to state that there is limited research performed into safe behaviour of individuals, as is noted by several researchers (40,41).

1.7 The current research gap and goal of this thesis

As highlighted earlier, ongoing research delves into understanding how human behaviour shapes an organization's IT framework and the associated security risks. The complexity of human behaviour in the context of workplace safety adds a layer of intricacy to this investigation. Metalidou et al.'s research underscores the pivotal role of information security awareness in mitigating security threats arising from human errors (42). They emphasize the need for organizations to foster a culture where positive security behaviours are valued, instilling the understanding that security is a responsibility shared by every individual within their infrastructure, business, and services (42).

While researchers increasingly agree on the efficacy of educational campaigns and training sessions to enhance security awareness and keep employees abreast of the latest threats, a notable portion of the existing research focuses on challenging-to-measure constructs like attitude, intention, norms, and beliefs concerning safe behaviour (38,40,43).

Expanding on this, it becomes apparent that the current body of research is compartmentalized into distinct areas such as security training and education, security awareness, intentional behaviour, and actual behaviour. Each of these areas represents a consecutive step, akin to a 'conversion rate,' in the journey towards achieving safe behaviour. However, numerous studies tend to focus on isolated elements within these categories, despite their interconnected nature. Additionally, a significant challenge lies in the use of variables that are inherently hard to measure, as previously mentioned.

To bridge this research gap, it is imperative to delve deeper into the unexplored territories within safe behaviour. This includes a more comprehensive examination of security training and education, security awareness, intentional behaviour, and ultimately, actual (safe) behaviour. Emphasizing that these four components are interconnected and represent successive stages with their respective "conversion rates" can further contextualize the significance of this research. A visualization of the components and their relation in terms of conversion rates is depicted in **Figure A.**

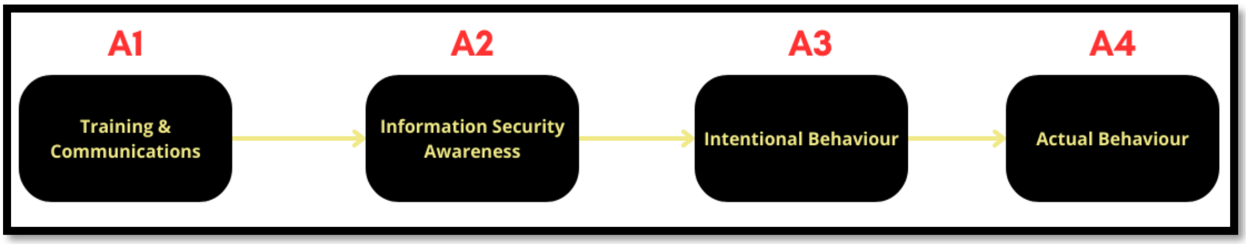


Figure A: Visualization of the interconnected components and their relation in terms of conversion rates.

In light of these considerations, the current thesis aims to explore measurable demographic factors and their correlation with safe behaviour in information handling. By synthesizing existing literature on demographic factors and safe behaviour, the intention is to develop a matrix of employee profiles, which will be built upon two parameters (X- and Y-axis). This matrix will categorize individuals within an organization into different 'profiles,' each with distinct focuses and needs. Consequently, this segmentation will enable the customization of training programs, making them more effective in promoting safe behaviour. The employee profile matrix is used as a useful framework to increase the conversion rate from component A1 to A2, from component A2 to A3 and from component A3 to A4. This is because in reality, there is a certain loss in every componential conversion. For example, the conversion from training and communications to information security awareness is not 100%, and from information security awareness to intentional behaviour has a certain loss in conversion as well, and so on. Hence, we would like to increase the input at the 'start' of this conversion, hoping that the loss in conversion decreases at every component, which would ultimately translate into safer actual behaviour.

By focusing on these conversions, we hope to increase the conversion rate to actual safe behaviour, thereby mitigating cybersecurity damages as a result of human behaviour. A visualization of how the employee profile matrix influences the conversion from 'Training & Communication' to 'Actual Behaviour' can be seen in **Figure B.**

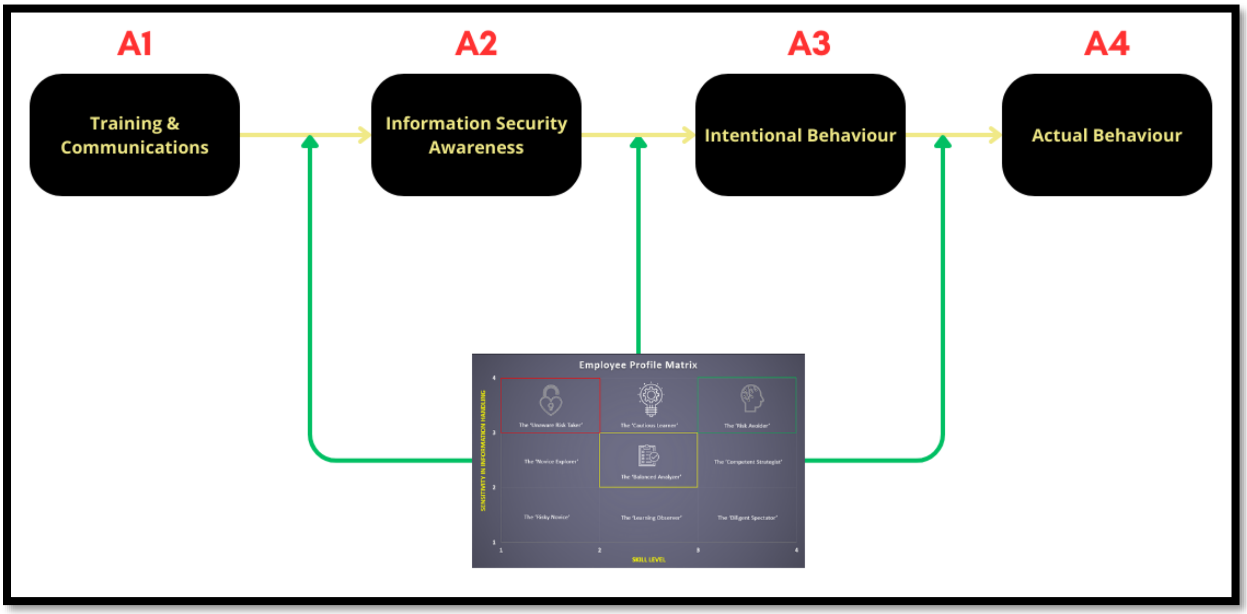


Figure B: Visualization of the interconnected components and their relation in terms of conversion rates and how the employee profile matrix influences these conversions.

In essence, the overarching goal of this thesis is to address the following research question**: "How can organizations implement tailored training, based on custom employee profiles, to enhance safe behaviour in information handling within their organization?"**

To answer this research question, we look at the following different sub questions:

- **Q1:** 'What is the role of training and education in improving safe behaviour in information handling for employees?'
- **Q2:** 'How can organizations better leverage training & communication to improve actual safe behaviour in information handling?'
- **Q3:** 'What are easy-to-measure variables that can be used for creating employee profiles which can be utilized to improve safe behaviour in information handling?'
- **Q4:** 'How can organizations utilize these profiles to provide tailored training to employees, thereby improving safe behaviour in information handling?'

2. Theoretical Framework

Safe behaviour regarding cybersecurity and information handling is often an end product of information security awareness (ISA) (44). The higher the awareness of an employee, the more likely they are to exert safe behaviour, or at least in a more frequent manner. It is therefore important to improve the effect of educational awareness training modules by customizing and tailoring these campaigns. Nowadays, new employees must complete a cybersecurity module during their onboarding. However, employees (from new to veteran) generally complete the same all-in-one basic modules with only little in-depth explanation on how the rapidly evolving IT cyberthreat landscape imposes great harm and danger to the individual and/or the organization. This creates the need for customized, tailored training programs. For example, a young, new employee starting their first ever job has a bigger need for basic training and gaining information and insight into how their cyber behaviour can be a risk for the organization. In contrast, an employee who has been working at an organization for 20+ years does not need such intense basic training but might need more focus on the updating cyberthreat landscape and how to be an example to other colleagues. In addition, the severity of damage depends on the data an employee is working with; a maintenance employee generally has less risky actions to complete in an organization's IT-landscape when compared to manager or executive personnel. Furthermore, in a healthy IT infrastructure, the user access, and their rights within the organization's IT-landscape of the maintenance employee should be significantly lower compared to manager or executive personnel. Hence, it would be excessive to train the maintenance employee with complex modules, but simple education on e.g. phishing links and how to recognize and report these would suffice. Thus, the tailored training programs would have a great effect in increasing employee's safe behaviour based on their skills and needs, rather than just dragging them through a basic training module (39, 45).

2.1 Employee profile matrix

To develop employee profiles effectively, we have to consider several factors. The employee profiles are based upon an individual's skill level (X-axis) and the sensitivity in information they handle, or in other words, the importance and impact of sensitivity of the data/information they work with (Y-axis). A worker's skill level is of paramount importance since it encompasses not only the technical skills of an employee, but also the level of experience and expertise an employee possesses. Therefore, we deemed this parameter important for the X-axis. Additionally, where the skill level defines the employee, it is important to look at the bigger picture when it comes to data handling: organizations have a stance in the IT-landscape per definition since their (for example) working industry may be of importance to the sensitivity of data they handle. In order to create efficient employee profiles, it is therefore important to consider both the individual/employee and the organization and its structure to narrow down on the key aspects where improvements could be made. Hence, we opted for the sensitivity in data handling as a parameter for the Y-axis.

For the skill level, we've focused on four key demographics (**2.2 Skill level**): 'Age,' 'Gender,' 'Education Level,' and 'ISA Policy Knowledge.' These specific demographic factors are chosen because they are well-researched and measurable, avoiding reliance on assumptions such as 'intention to comply' or 'intentional behaviour'.

For the Y-axis (**2.3 Sensitivity in information handling)**, we look at the probability per industry to be subject to a cyber-attack as per data from STATISTA. Additionally, we look at the IT/information sensitivity per department, the impact per job role and the IT dependency per working industry. In this section, we will delve into each of these factors and clarify their role in the theoretical framework and their significance for creating the employee profile matrix.

Each demographic factor has been assigned a weight based upon four different criteria: the amount of articles/research included in this specific framework, the disparity and discussion about the influence of the factor, the statistical and significant power found in research about the specific factor, and whether the focus is on safe behaviour (preferably) or ISA. The amount of research entails the amount of research papers that were found specifically for that demographic factor. The discussion about influence criterion focuses on the conclusions and implications given by literature and is based upon the degree of agreement (a higher degree of agreement results in little to no discussion; thus, more points are assigned). For statistical significance, we looked at the number of articles that performed statistically significant analysis upon their drawn conclusions. For the last criterion, we opted to prioritize research done directly into the relation between these demographic factors and safe behaviour. However, a substantial amount of literature focuses on ISA, which is a component in the conversion of training to actual behaviour (**Figure A, B)**. Each demographic factor could be assigned 1-3 points based on their outcome regarding these criteria, supported by the following:

Table 1*: Criteria for weighting of demographic factors.*

CRITERION	**1 point**	**2 points**	**3 points**
Amount of research	1-3 articles	4-7 articles	8+ articles
Discussion about influence	Low to no agreement	~ 50/50 agreement	Considerable agreement
Statistical significance	0-2 articles with statistical significance	3-5 articles with statistical significance	6+ articles with statistical significance
Focus on behaviour over ISA	ISA > behaviour	ISA = behaviour	Behaviour > ISA

2.2 Skill level

2.2.1 Age

Considerable research has delved into age as a demographic factor and its relationship to safe behaviour in information handling. Age not only directly influences safe behaviour but also provides insights into an individual's ISA. In the study by Branley-Bell et al., the researchers explored four specific aspects of safe behaviour—'Device Securement,' 'Password Generation,' 'Pro-active Checking,' and 'Password Updating'—revealing that younger individuals tend to be more susceptible to phishing and are more inclined to share passwords with their generational peers. On the other hand, older individuals exhibit greater security in these aspects, albeit with a potential shortfall in physical device securement. The overall consensus in the paper suggests that as individuals age, they tend to exhibit more safe behaviour, though the study primarily focuses on safe behaviour rather than ISA

(46). Pattinson et al. align with these findings, asserting that younger employees are more likely to engage in risky information security behaviour (47). In a similar vein, Mittal et al. emphasize the need to increase security awareness, especially among those aged 32 to 50, who demonstrated a tendency to leave important printouts on their desks (48). Darwish et al.'s research concurs, highlighting that the younger the individual, the more susceptible they are to phishing attacks, a conclusion supported by Kumaraguru et al. (49, 50). Whitty et al. and other studies on password sharing further affirm that younger individuals are more likely to engage in such behaviour (51–53). Unique perspectives emerge in Li et al.'s research, where the focus shifts to generation groups rather than age groups. Contrary to their hypothesis, they find that the younger generation (born after 1996) exhibits less safe behaviour compared to older generations, aligning with the broader research landscape (54).

While much research concentrates on age and safe behaviour, McCormac et al. and Chua et al. investigate how age influences ISA. Both studies conclude that older employees generally possess better ISA, theoretically translating to more safe behaviour in cybersecurity (55, 56). Out of the available literature for this demographic, 9 articles provided statistical significance for their research. In aggregate, the conclusion is that **'the older an employee or individual, the less susceptible they are to cyber-attacks'**.

Based upon this conclusion, we can classify and rank the following age groups:

Table 2*: Age groups and their respective scores for the employee profile matrix.*

Age	Importance	Points
< 18 – 29	Very unfavourable	1
30 - 49	Unfavourable	2
50 - 59	Favourable	3
60 +	Very favourable	4

In terms of a weight for the employee profile matrix, the following can be said about age as a factor:

- Amount of research: **3 points**
- Discussion about influence: **3 points**
- Statistical significance: **3 points**
- Focus on behaviour over ISA: **3 points**

Therefore, age as a factor scores **12 points** out of a total of **35**, with a total weight of **34%.**

2.2.2 Education level

Education level stands out as a significant demographic factor influencing safe behaviour, although assigning safe behaviour solely to a higher education level is challenging, considering the crucial role played by ISA. The theoretical framework suggests that a higher education level may correlate with elevated ISA and, consequently, more safe behaviour. This correlation between education level and ISA finds support among various researchers, as evidenced by studies such as those conducted by Chua et al. and Ojala Burman (52, 56).

The consensus across these studies aligns with expectations, indicating that a higher education level tends to correspond with better ISA. Some studies delve into the direct influence of education level on safe behaviour. For instance, Darwish et al. discovered that graduates from theoretical studies, like Humanitarian Studies, exhibit higher susceptibility to phishing and cyberattacks compared to (Computer) Science graduates (49). Similarly, Agarwal et al. found that a higher education level correlates with more safe behaviour (57). However, not all researchers found a clear correlation between an individual's education level and ISA or safe behaviour, as indicated by the work of Bulgurcu et al. (58). For this demographic factor, only two articles provided statistical significance. Despite these divergent findings, the available literature supports a general conclusion: '**A higher education level tends to correspond with higher ISA, suggesting a positive impact on an individual's cyber behaviour'.**

Based upon this conclusion, we can classify and rank the following education groups:

Table 3*: Education levels and their respective scores for the employee profile matrix.*

Education level	Importance	Points
No education	Very unfavourable	1
High school or equivalent	Unfavourable	2
BSc	Favourable	3
MSc +	Very favourable	4

In terms of a weight for the employee profile matrix, the following can be said about education level as a factor:

- Amount of research: **2 points**
- Discussion about influence: **2 points**
- Statistical significance: **1 point**
- Focus on behaviour over ISA: **1 point**

Therefore, age as a factor scores **6 points** out of a total of **35**, with a total weight of **17%.**

2.2.3 Gender

Gender represents a contentious demographic variable in cybersecurity research, predominantly focusing on the cyber behaviour of males and females while excluding additional gender categories in this thesis. Despite considerable debate regarding susceptibility to cyberattacks, numerous studies, including those by Branley-Bell and Chua et al., suggest that there is minimal disparity between genders (46, 52, 56). However, Darwish et al.'s study reveals that females exhibit higher susceptibility to phishing attacks and cybersecurity flaws, a conclusion supported by Sheng et al.'s findings (49, 51).

In contrast, McCormac et al. argue that female participants demonstrate significantly higher ISA scores compared to males, a perspective echoed by Cronan et al., who assert that men exhibit more unethical cybersecurity behaviour (55, 59). Additionally, Li et al. contend that the impact on security protection behaviour is stronger in the female group compared to the male group, aligning with their hypothesis that women possess a heightened awareness of cybersecurity severity when facing related issues (54). Out of the literature, only 6 articles provided statistical significance. In addition, other than the demographic factors mentioned besides 'Gender', we opted to assign 2 points for the male gender and 3 points for the female gender. This is because there is a lot of discussion about the differences in gender and safe behaviour or ISA exhibition, but most literature shows just a slight difference between the two genders.

Nevertheless, the discussion about which gender exerts more safe behaviour or has a higher ISA is an ongoing discussion, but based upon the available literature, it suffices to conclude the following: '**Females have a slightly higher ISA and therefore exert more safe behaviour regarding cybersecurity'.**

Based upon this conclusion, we can classify and rank the following two genders:

Table 4*: Genders and their respective scores for the employee profile matrix.*

Gender	**Importance**	**Points**
Male	Unfavourable	2
Female	Favourable	3

In terms of a weight for the employee profile matrix, the following can be said about gender as a factor:

- Amount of research:	**3 points**
- Discussion about influence:	**1 point**
- Statistical significance:	**2 points**
- Focus on behaviour over ISA:	**3 points**

Therefore, age as a factor scores **9 points** out of a total of **35**, with a total weight of **26%.**

2.2.4 ISA Policy Knowledge

A solid understanding of information security awareness (ISA) is considered crucial for fostering responsible behaviour in the digital world. One might assume that individuals possessing extensive knowledge of ISA policies would inherently be more vigilant about the cyber threats they face. However, Whitty et al. challenge this expectation through their study, revealing that "knowledge alone is insufficient to modify problematic cybersecurity behaviours." It is noteworthy that their investigation focused directly on behaviour rather than ISA itself, examining how pre-existing knowledge correlates with safer online practices (53). Despite this contradiction, the prevailing consensus in most studies aligns on the notion that heightened ISA policy knowledge contributes to increased ISA and, consequently, should manifest in safer online (58, 60–63). For this demographic factor, 4 articles provided statistical significance for their results. Thus, we can conclude the following: **'Greater familiarity with ISA policies is expected to result in more safe cybersecurity practices.'**.

Based upon this conclusion, we can classify and rank the following ISA policy knowledge levels:

Table 5: *ISA policy knowledge levels and their respective scores for the employee profile matrix.*

ISA Policy Knowledge	Importance	Points
No knowledge	Very unfavourable	1
Basic Knowledge	Unfavourable	2
Advanced Knowledge	Favourable	3
Expert	Very favourable	4

In terms of a weight for the employee profile matrix, the following can be said about ISA policy knowledge level as a factor:

Amount of research:	**2 points**
Discussion about influence:	**3 points**
Statistical significance:	**2 points**
Focus on behaviour over ISA:	**1 point**

Therefore, age as a factor scores **8 points** out of a total of **35**, with a total weight of **23%.**

2.3 Sensitivity in information handling

To establish the Y-axis parameters for the employee profile matrix, we conducted a survey among EY IT-experts with a prerequisite of **a minimum of 5 years of experience in the field of IT Risk Assurance within the organization**. This ensured that the survey responses were derived from substantial empirical expertise. The survey comprised three questions, each requiring responses on a 4-point Likert scale ranging from 'None' to 'Low,' 'Medium,' and 'High.' IT-experts were tasked with assigning scores for three variables. Additionally, it's noteworthy that the 'None' score was not utilized throughout the entire survey, and thus, it is omitted from the tables below. Furthermore, a fourth variable was included, focusing on the likelihood of an industry being susceptible to a cyberattack or data breach. This data is derived from the annual STATISTA report (64). Given that these variables are solely derived from the expertise of IT-experts without the same criterion as the 'Skill Level' section, each variable within this section holds an equal weight of 25%.

2.3.1 Working Industry

In evaluating the IT dependency of different industries, it is essential to establish a systematic ranking system based on the extent to which each industry relies on IT components such as hardware, software, and networks. The following brackets and criteria have been defined for this purpose:

Low (2 points): Industries categorized as "Low" have basic IT integration, but their dependency is restricted. Technology is used for basic, fundamental functions, with room for improvement in adopting advanced solutions. Considerations involve basic use of IT-systems for routine tasks, limited adoption of advanced technologies, and moderate reliance on manual processes. The impact of IT disruption is moderate, allowing basic functions to continue.

Medium (3 points): Industries in the "Medium" category exhibit a moderate level of IT dependency, with substantial integration of technology into various aspects of operations. The industry is proactive in developing new technologies but may not be at the cutting edge. Considerations include significant use of IT-systems for core processes, proactive adoption of common technologies, and moderate investment in cybersecurity and data protection. The impact of IT disruption is considerable, affecting core processes and technology-dependent functions.

High (4 points): Industries categorized as "High" are highly dependent on information technology, leveraging advanced solutions for enhanced efficiency, innovation, and competitiveness. Robust cybersecurity measures are in place. Considerations involve extensive integration of IT into all aspects of operations, embracing cutting-edge technologies for innovation, and a strong emphasis on cybersecurity and regulatory compliance. The impact of IT disruption is significant and high, potentially halting critical operations and innovation processes. Comprehensive disaster recovery and continuity plans are crucial in this scenario.

This systematic categorization allows for a comprehensive understanding of the varying degrees of IT dependency across industries. The results derived from an industry-specific assessment can be effectively presented in a table format, highlighting the respective IT dependency levels and the potential consequences of a cyber-attack or data breach within each industry. IT-experts were presented with 15 distinct industries and tasked with ranking and scoring them according to the level of IT dependency within each specific industry. The resulting classification is based on their responses:

Table 6*: Working industries' respective scores for the employee profile matrix based on level of IT - dependency.*

Working Industry	IT Dependency	Point range
-	None	1 – 1,49
Real Estate	Low	1,50 – 2,49
Accommodation Construction Education Entertainment News and Media Professional Services Public Administration Retail Transportation Other…	Medium	2,50 – 3,49
Finance Healthcare ICT/IT Services Manufacturing Water and Utilities	High	3,50 - 4

2.3.2 Department

In the context of assessing the information sensitivity of various departments within an organization, it becomes imperative to categorize and rank them based on the nature and criticality of the IT-related data they handle. The following scoring brackets and criteria have been established for this purpose:

Low (2 points): Departments categorized as "Low" handle some sensitive IT-data, but the impact of breaches is limited. Basic measures are in place to ensure basic confidentiality. Considerations include the handling of moderately sensitive information, resulting in limited operational disruption and reputational impact. The financial and legal consequences from potential data breaches remain minimal.

Medium (3 points): Departments in the "Medium" category handle moderately sensitive IT-related data, with measures in place for its protection. The impact of data breaches within this bracket could have moderate consequences. Considerations involve the handling of significant sensitive information, leading to significant operational disruption and reputational impact. There are potential financial and legal consequences associated with data breaches.

High (4 points): Departments categorized as "High" handle highly sensitive IT-related data, with robust measures in place to ensure its protection. The impact of data breaches within this category could have severe consequences. Considerations encompass the handling of critical and highly sensitive information, resulting in severe operational disruption and reputational impact. The financial and legal consequences of data breaches are expected to be severe, requiring strict compliance with legal and regulatory requirements for data handling.

This systematic categorization and ranking system enable a comprehensive understanding of the varying degrees of information sensitivity across departments. Such insights are crucial for identifying potential vulnerabilities and establishing targeted cybersecurity measures. The results from the survey are depicted below.

Table 7*: Departments' respective scores for the employee profile matrix based on level of information sensitivity.*

Department	Information Sensitivity	Point range
-	None	1 – 1,49
-	Low	1,50 – 2,49
Facilities & Maintenance Marketing & Public Relations Procurement Production & Operations Sales Other…	Medium	2,50 – 3,49
Finance & Accounting Human Resources Internal Audit IT Legal & Compliance Research & Development	High	3,50 - 4

2.3.3 Job Role

A third factor in determining the information sensitivity of an employee is their job function or job role. Based upon four different types of personnel, IT-experts were asked to rank these job roles. This question aims to investigate which types of jobs are associated with certain risks when, for example, information is mishandled or when they fall victim to a cyber-attack or data breach. It is important to consider various types of impacts here because each type of job can bring different kinds of risks. Therefore, it is important to classify the impact level per job type. In order to do so, we look at the different types of personnel below.

Operational Personnel (Frontline employees handling day-to-day tasks)

Operational personnel are primarily engaged in executing day-to-day tasks within the organization. Their responsibilities include routine operational activities, often with limited exposure to strategic decision-making. The potential impact of information mishandling, cyber-attacks, or data breaches may vary based on their level of interaction with IT systems and sensitive data.

Lower Management (Team leaders supervising operational personnel)

Lower management consists of team leaders responsible for supervising operational personnel. Their roles involve a combination of managerial oversight and operational involvement. The potential impact on information security is influenced by their responsibilities and their role in guiding frontline employees.

Higher Management (Departmental leaders responsible for strategic decisions)

Higher management comprises departmental leaders responsible for making strategic decisions. Their roles involve shaping the overall strategy and policies of their respective departments. The potential impact on information security is significant due to their strategic decision-making responsibilities and oversight functions.

Executive Personnel (C-level) (Top-level executives shaping overall organizational strategy)

Executive personnel, including C-level executives, hold the highest organizational positions and are responsible for shaping the overall strategy and direction of the entire organization. The potential impact on information security is profound, given the critical nature of their decisions and the organization-wide consequences.

When analysing the impact of different job roles within an organization, it is essential to categorize and prioritize them based on the nature and criticality of their responsibilities. The following impact brackets and criteria have been defined for this purpose:

Low (2 points): For job roles classified as "Low," the impact on information security is moderate. Individuals in these roles may have some managerial or operational responsibilities related to IT systems, but their exposure is not extensive. The potential consequences of information mishandling or cyber threats are moderate, allowing for basic functions to continue with room for improvement in adopting advanced solutions.

Medium (3 points): In job roles designated as "Medium," the impact on information security is considerable. Individuals in these roles have significant responsibilities and exposure to IT systems, potentially affecting core processes and technology-dependent functions. The consequences of information mishandling, cyber-attacks, or data breaches may range from moderate to high, reflecting the strategic nature of their decisions.

<u>High (4 points)</u>: For job roles categorized as "High," the impact on information security is significant. Individuals in these roles, often at the executive or top-level management, play a critical role in shaping the organization's overall strategy and direction. Their decisions and oversight responsibilities may result in profound consequences in the event of information mishandling, cyber-attacks, or data breaches. The potential impact is high, potentially halting critical operations and innovation processes, requiring comprehensive disaster recovery and continuity plans.
This systematic categorization provides a nuanced understanding of the varying degrees of impact associated with job roles concerning information security risks within an organization. It serves as a framework for the IT-experts participating in the survey, allowing them to evaluate and rank the relative significance of each job role in mitigating the consequences of information-related incidents. The results from the survey are depicted below.

Table 8*: Job Roles' respective scores for the employee profile matrix based on level of impact.*

Job Role	Impact Level	Point range
-	None	1 – 1,49
-	Low	1,50 – 2,49
Lower Management Operational Management Other...	Medium	2,50 – 3,49
Higher Management Executive Personnel	High	3,50 – 4

2.3.4 Probability

In this section, we will assess the likelihood of the aforementioned industries falling victim to a cyber-attack or data breach based on statistics obtained from STATISTA. STATISTA is a global data and business intelligence platform renowned for its extensive collections of statistics and reports (65). The reported data entails data breach incidents which span from November 2021 to October 2022, representing the most up-to-date dataset for cyber-attack and data breach reports (64). From these total numbers of cyber-attacks and data breaches, we filter out the cyber-attacks specifically performed by means of social engineering, since this form of cyberattacks correlates very closely with human behaviour. To offer a comprehensive understanding of the probability levels, we will categorize the probabilities as follows:

<u>Low Probability (1-50 reported breaches) (2 points)</u>: In this classification, industries falling within the low probability range have reported a relatively lower number of cyber-attacks or data breaches as a result of social engineering, ranging from 1 to 75 incidents. This suggests a comparatively lower risk level, indicating that these industries have experienced a modest number of security incidents during the specified timeframe.

<u>Medium Probability (51-100 reported breaches) (3 points)</u>: Industries classified under medium probability have reported a moderate number of cyber-attacks or data breaches as a result from social engineering, ranging from 76 to 150 incidents. This level of probability signifies a moderate risk level, indicating a notable but not exceptionally high frequency of security incidents within these industries.

<u>High Probability (100+ reported breaches) (4 points):</u> Industries falling within the high probability range have reported a substantial number of cyber-attacks or data breaches as a result from social engineering, exceeding 100 incidents. This classification suggests a heightened risk level, indicating that these industries have experienced a significant frequency of security incidents during the specified period, necessitating a heightened level of attention to cybersecurity measures.

This categorization aims to provide a clear overview of the probability levels associated with cyber-attacks and data breaches within different industries, specifically as a result from social engineering attacks, offering insights into the potential vulnerability and risk mitigation needs for each sector. Thus, the final ranking is depicted below:

***Table 9:** Working Industries' respective scores for the employee profile matrix based on level of probability of falling victim to a cyber-attack as a result of social engineering.*

Working Industry	Probability	Point
-	None	1
Accommodation Construction Education Entertainment ICT/IT Services Real Estate Transportation	Low	2
Healthcare Manufacturing News and Media Public Administration	Medium	3

Retail		
Finance Professional Services Water and Utilities	High	4

After defining every factor and ranking them with their respective scores for the employee profile matrix, we are able to propose a framework explaining how these factors play a role in safe behaviour. **Figure C** shows the final theoretical framework which will be used as a basis for creating the employee profiles.

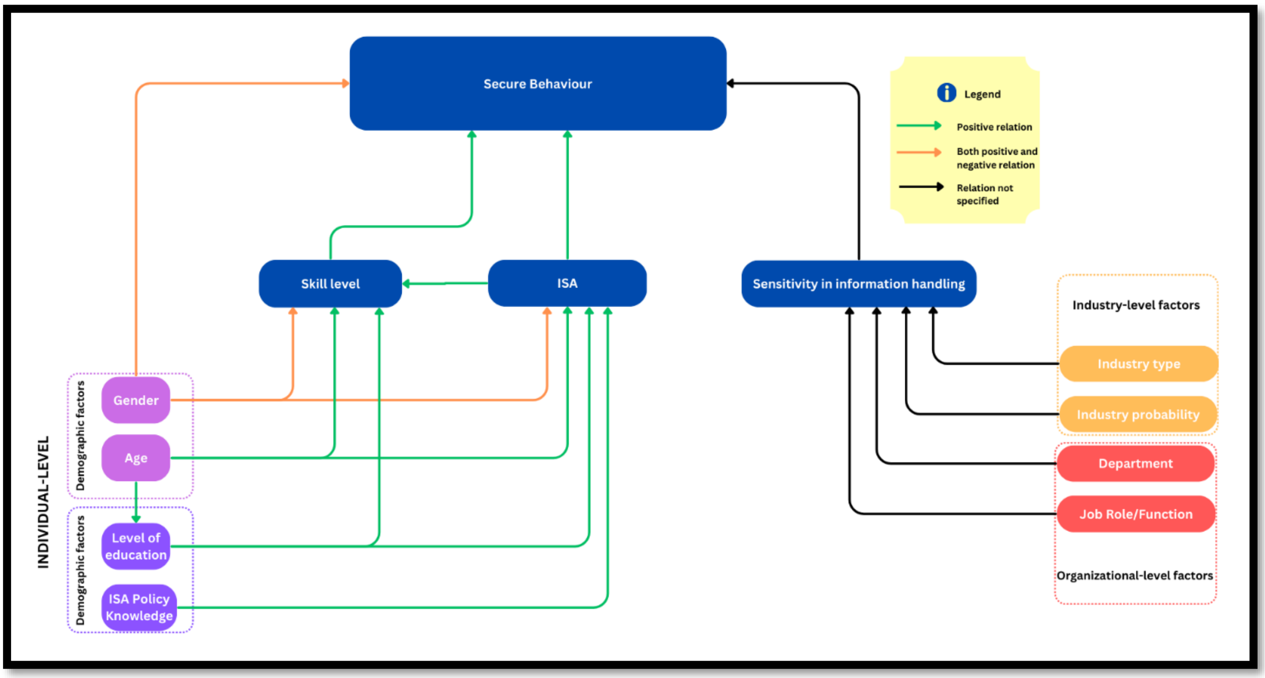


Figure C: Theoretical model for safe behaviour, ISA and the underlying factors.

3. The Employee Profile Matrix

The full employee profile matrix can be found here:

Employee Profile Matrix.xlsx

3.1 About the matrix

In the pursuit of a comprehensive understanding of an organization’s workforce, we created the Employee Profile Matrix, a strategic tool that encapsulates a wealth of information derived from a thorough exploration of various variables outlined and examined in a preceding section. This matrix serves as a dynamic representation of the diverse attributes, skills, and characteristics that collectively shape an organization’s workforce. Grounded in a meticulous analysis of variables such as job roles, impact levels, information sensitivity, and IT dependency, the Employee Profile Matrix delves into the intricacies of an organization’s workforce composition. By synthesizing these multifaceted elements, we aim to gain valuable insights into the unique qualities and contributions of each employee within the organization. This strategic tool not only facilitates a nuanced understanding of individual roles and their associated responsibilities but also provides a holistic view of the organization's overall (potential) resilience to challenges such as cyber threats and data breaches. As we navigate the complex landscape of modern workplaces, the Employee Profile Matrix emerges as an invaluable resource, empowering us to tailor our strategies, training programs, and risk mitigation efforts to align seamlessly with the diverse profiles and needs of our workforce. Through this matrix, we embark on a journey of fostering a resilient, adaptive, and empowered workforce poised to meet the evolving demands of our dynamic organizational landscape. As such, we present the Employee Profile Matrix in **Figure D.** Ideally, the ‘best’ employees would be classified in the profile with the green outlining (The Risk Avoider). Here, the employee has the highest sensitivity in information handling, but also the highest skill level to deal with such responsibilities. In contrast, employees classified into the profile with the red outlining (The Unaware Risk Taker) have a low skill level, but a high sensitivity in information handling. Here, the employee lacks sufficient skill to safely handle the level of sensitivity in information handling. The profile with the yellow outlining (The Balanced Analyzer) is a profile that meets the aforementioned profiles in the middle. Employees in this bracket have a medium-level sensitivity in information handling and skill level, which means they do possess some level of skill and responsibility, but would benefit from advanced training.

The matrix in the Excel-file is fairly easy to use. On the top left, one can pick the demographics that are applicable to their situation, which will be decisive for the placement on the matrix. A visualization of the matrix components can be found in the **Appendix**.

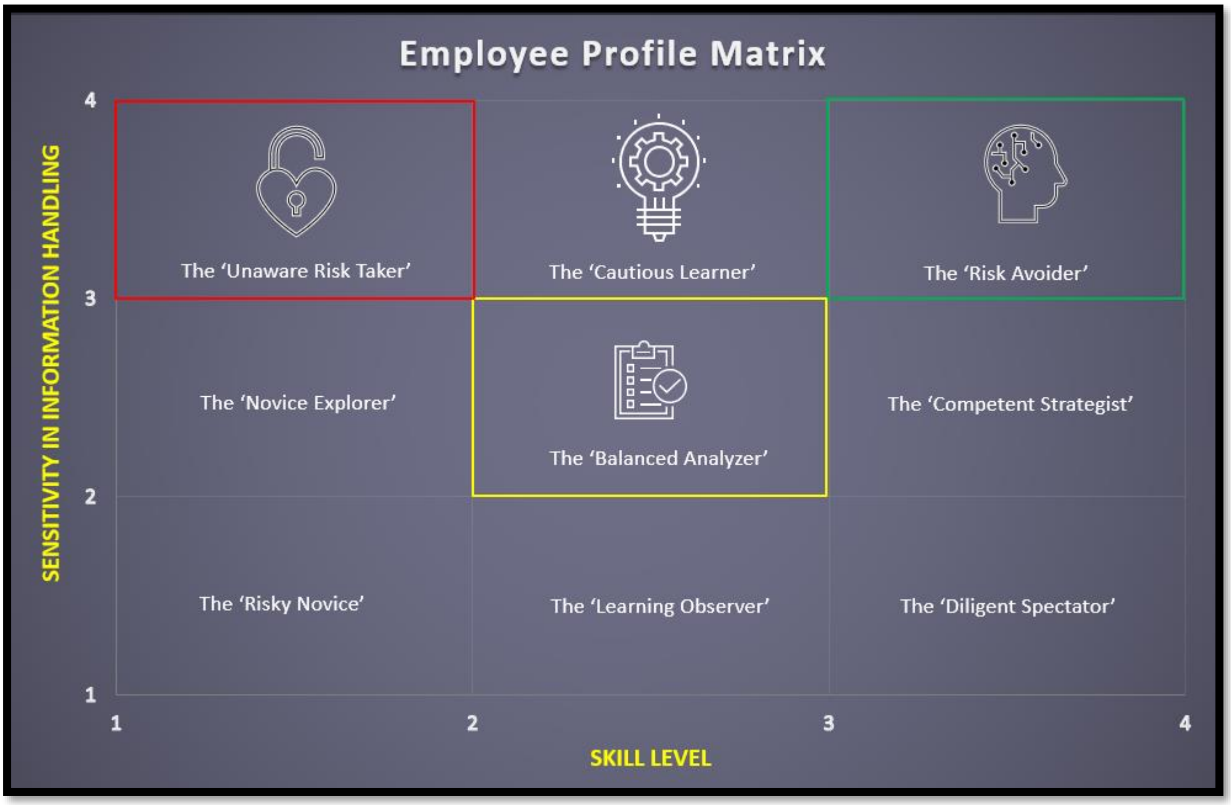


Figure D: The Employee Profile Matrix with nine different profiles.

In the era of rapid digital advancement and innovation, it appears increasingly uncommon for individuals to have absolutely no grasp of digital knowledge. Most people, especially the younger generation, possess basic skills such as handling a phone or setting up a password. Consequently, classifying individuals into profiles with the minimum skill level and sensitivity in information handling seems nearly impossible, due to organizations being more reliant on IT. In present day, there are almost no organizations that are fully IT-independent. Therefore, we assert that, despite the existence of profiles like 'The Risky Novice' and 'The Learning Observer,' this employee profile matrix will not categorize individuals into these 'lower' profiles. Nevertheless, by incorporating additional factors into the base of this matrix and considering influences on the sensitivity in information handling, a more accurate placement of individuals can be achieved. This approach enhances the likelihood of employees being categorized into the aforementioned 'lower' profiles, offering a more nuanced and precise assessment of their skills and information handling capabilities. Suggestions are made in every profile, yet these could be open to interpretation and should be viewed as a conceptual suggestion for future research, as for the names of these profiles, which could be modified to a better fit.

3.2 The Profiles

As **Figure B** shows, there are nine different profiles in this framework, each based upon their skill level and their level of sensitivity in information handling. In this section, we will propose several employee profiles as a concept, which can be used as building blocks for future research.

The Risky Novice

Foundational cybersecurity training for The Risky Novice should concentrate on generic topics such as password management, safe browsing practices, and understanding governance principles. These modules will establish a strong foundation, promoting basic security hygiene. Interactive sessions on recognizing common cyber threats, such as malware and social engineering, will contribute to their overall awareness.

The Novice Explorer

Building on foundational knowledge, The Novice Explorer can benefit from interactive cybersecurity training covering a variety of topics. Increasing the skill level of The Novice Explorer is important, to create an awareness of the sensitivity of the information they are handling. Basic principles on password management, safe browsing and recognizing threats will contribute to their evolving understanding of cybersecurity.

The Unaware Risk Taker

Fundamental cybersecurity training for The Unaware Risk Taker should cover a range of topics. Interactive modules on secure communication practices, recognizing and reporting incidents, and understanding the importance of data classification will contribute to their overall awareness. Regular reinforcement through simulated scenarios and practical exercises will reinforce the significance of security in their role.

The Learning Observer

Progressive cybersecurity training for The Learning Observer can involve modules on incident response, security awareness campaigns, and secure data handling practices. Advanced phishing simulations, coupled with interactive sessions on recognizing insider threats and safe collaboration practices, will align with their observational learning style.

The Balanced Analyzer

Tailored training for The Balanced Analyzer should extend beyond phishing to cover more nuanced aspects of cybersecurity. Advanced threat intelligence training, and incident response exercises will complement their analytical skills. Furthermore, training modules on governance can prove to be beneficial.

The Cautious Learner

With higher skill levels, The Cautious Learner can benefit from specialized training in areas such as penetration testing, secure network architecture, and advanced threat detection. Modules on regulatory compliance and privacy considerations will align with their cautious approach. Encouraging their participation in red teaming exercises and collaborative threat intelligence activities can leverage their expertise.

The Diligent Spectator

Advanced cybersecurity training for The Diligent Spectator should encompass threat hunting, advanced threat detection techniques, and cybersecurity leadership. Modules on secure cloud practices, incident response planning, and collaborative cybersecurity initiatives will align with their advanced skill set. Encouraging their active involvement in red teaming exercises can leverage their expertise for organizational benefit.

The Competent Strategist

Tailored training for The Competent Strategist should focus on strategic cybersecurity aspects. In addition to phishing awareness, modules on policy development, security governance, and leadership skills will contribute to their strategic expertise. Encouraging them to lead security initiatives, develop security policies, and mentor others can maximize their impact.

The Risk Avoider

Highly specialized cybersecurity training for The Risk Avoider should cover advanced topics such as threat modelling, risk management, and regulatory compliance. Advanced threat simulations, hands-on exercises in incident response planning, and strategic cybersecurity leadership training will contribute to their advanced skill set. Encouraging them to play a leadership role in fostering a security-aware culture throughout the organization is crucial.

4. Discussion & Conclusion

4.1 The 'Skill Level' factors

This study utilized four key individual-level demographics—age, gender, education level, and ISA policy knowledge—to construct employee profiles. The research, conducted over six months, drew from a somewhat limited body of literature for scoring purposes. It's crucial to acknowledge that there is additional literature available that could enhance the value of this research. Consequently, this study and its derived products should be regarded as foundational for future research endeavours aimed at better addressing and mitigating cyber threats and associated damages.

When developing customized employee training modules based on individual profiles, it is crucial to consider additional factors which may not be on the level of the individual, such as the national culture of a country (66). While the employee profile matrix from our research categorizes employees into distinct profiles, it is essential to incorporate Hofstede's cultural dimensions, which encompass broader, nationwide factors that are equally significant. One such dimension is **'uncertainty avoidance**', indicating the extent to which a country's culture seeks to minimize uncertainty. High uncertainty avoidance countries tend to establish numerous rules to clarify any potential ambiguities, while low uncertainty avoidance cultures may prioritize adherence to existing rules without an emphasis on written documentation.

For countries with high uncertainty avoidance, it becomes imperative to articulate specific rules for employees. Conversely, in countries with lower levels of uncertainty avoidance, a different, less rule-centric approach may be more effective. In addition to Hofstede's uncertainty avoidance dimension, various other dimensions have been explored, and it is highly advisable to consider these dimensions when building upon the research presented in this thesis (67, 68).

For future research, the inclusion of different factors is recommended, ensuring consistency in criteria across all factors to achieve a more precise placement of individuals in the employee profile matrix. It's worth noting that the scores assigned to demographic factors in this research are subject to interpretation, allowing for potential variations in the final scores. However, these variations may not significantly impact the overall outcomes.

4.1.1 Age

Among the four individual-level demographic factors examined, age emerged with the highest weight in this study. The literature review conducted in this thesis underscored the significant role of age in shaping individuals' behaviour in handling information. The findings suggest that, generally, older individuals exhibit safer workplace behaviour. However, a real-world discrepancy becomes evident with age, particularly in terms of technological proficiency. Seniors in particular may not be as tech-savvy as younger adults who tend to stay more in line with rapid digital innovations. Therefore, it is advisable to delve further into research exploring how safe behaviour may decline with increasing age, focusing on specific aspects like phishing training, device security or password management (69).

4.1.2 Education Level

In addition to age, there is a clear consensus when it comes to how an individual's education level translates to safe behaviour. Most research concluded that the higher the education level of an individual, the higher the ISA of this individual and therefore the safer the behaviour this person is expected to exert on the workplace. According to the study of Sheng et al. educated people have a higher level of thinking about consequences and are thus behaving more carefully (50–52). Therefore, considering an individual's education level when creating training programmes is highly recommended since this factor can be a strong indicator of a person's ISA and the capabilities to potentially enhance their ISA. However, available literature mostly looks at the relationship between the education level and a person's ISA, which is not the direct aim for the research conducted in this thesis. Additional research into how education level directly influences actual behaviour on the workplace would be of additional value to the framework proposed in this thesis.

4.1.3 Gender

Gender is the most controversial demographic factor included in the model. Researchers often disagree on which gender exerts more safe behaviour. For example, McCormac et al. found that females have a higher ISA than men, which would translate into safer behaviour (55). In contrast, Sheng et al. found the opposite (51). Furthermore, most research focuses on the direct relationship between gender and behaviour, but there is quite some literature available arguing that gender correlates with a person's ISA directly before translating into safe behaviour. This is also the reason that this demographic factor only scores one point for 'discussion about influence', because it seems that a lot of researchers do not (fully) agree with each other. Moreover, there is no literature available that considers additional genders, which has been an increasing point of attention over the last years. Because of this lack of research, people that identify outside the binary male/female genders could consider picking their biological gender, since the vast majority of academic literature research includes only these two genders.

4.1.4 ISA Policy Knowledge

Arguably one of the most important factors is an individual's ISA policy knowledge. As expected, most researchers agree on that the higher an individual's ISA policy knowledge is, the safer behaviour they exert. However, ISA policy knowledge does, naturally, include an individual's ISA without looking at safe behaviour directly. As **Figures A and B** show, ISA comes second in the conversion from training to actual behaviour, which means that regardless of the increased ISA, it would be most beneficial to translate ISA to actual safe behaviour as much as possible. On that note it seems that the framework proposed in this thesis can be of extra additional value, since an increase in ISA is mostly based on proper and interesting training modules, with a goal of increasing the conversion rate to actual behaviour significantly. ISA is mostly dependent on correct and proper training that poke an individual's interest, which makes the individual store more information from those training modules, thereby increasing the conversion rate from training to ISA and ultimately actual safe behaviour. Nevertheless, ISA policy knowledge is somewhat harder to measure compared to the other three variables defining the skill level in this framework, since it's incorporated into an individual rather than a given fact such as age, gender, and education level. A recommendation to somewhat measure the ISA policy knowledge of an individual could be a minor quiz/questionnaire involving basic to advanced questions. This could serve as a useful tool to measure an individual's ISA policy knowledge. Otherwise, if the situation includes an existing employee rather than a new employee, the organization could consider checking within the department or team how they would perceive the individual's ISA policy knowledge and use that as a reference to classify said employee in the employee profile matrix. Furthermore, it is important for organizations to not only let their employees know these policies exist but encourage them to actively comply with these policies (52, 70). Incentives like bonuses or other forms of rewards could be very valuable in the pursuit of ISA policy compliance.

Moreover, the employee profile matrix generated in this study could be enriched by incorporating additional individual-level demographics. While our selection of easily measurable demographics was intentional for this research, there is potential value in exploring demographics that are somewhat more challenging to quantify. For instance, factors like an individual's **prior experience with security incidents** (51, 60, 71) and **impulsivity** (72) could provide valuable insights. Additionally, other challenging-to-measure factors might prove beneficial.

As previously discussed, extensive research has delved into the role of safe behaviour and individuals' intentions to comply with information security policies. Egelman et al. explored people's intentions as a precursor to planned behaviour using the Security Behaviour Intentions Scale (SeBIS) (73). Furthermore, studies on the psychology of compliance with security policies exist (74–76). Given appropriate measurements and methodologies, incorporating factors related to individuals' intentions to behave or comply with IS(A) policies could enhance the proposed matrix in this thesis.

4.2 The factors for sensitivity in information handling

In contrast to the demographic factors as a result from literature research, four different factors – not on an individual level – have been incorporated in the employee profile matrix. Because not only do the demographic factors regarding an individual influence safe behaviour, but it is equally important to consider different factors regarding the working industry, the department, the job role/function, and an industry's probability to fall victim to cyberattacks as a result from existing data from STATISTA. Here, in addition to data from STATISTA, we rely on the expertise of IT Risk Assurance experts who have been working at EY for over 5 years. Their insights and experience from years of working with cybersecurity issues are a fundamental provision to this employee profile matrix. Nevertheless, due to time constraints there were just eight responses on the survey sent to over 50 people. For future purposes, it may be useful to include more responses for a refined scoring of the different factors that make up the sensitivity in information handling.

Additionally, the original scores as a result from the survey were rounded up or down for simplicity. However, we noticed during the testing of our model that there was not much discrepancy in employee profile placement. Therefore, we used exact scores as a result from the survey in the factors 'Working Industry', 'Department' and 'Job Role'. As mentioned before, it would be very beneficial for researchers using this framework for further research to include more responses to have a more significant discrepancy between the different factors and how they score.

4.2.1 Working Industry

The results from the survey show that the working industry with the highest IT dependency is IT/ICT services. The industry 'Real Estate' scores the lowest when it comes to IT dependency. Scores have been appointed to the respective working industry as a result from the survey. The scores represent the correlation between the IT dependency in that specific working industry according to the IT experts. These scores are open to interpretation and personal experience from IT experts outside this sample size could add valuable insights that would be useful in defining the scores.

4.2.2 Department

The department factor correlates with the information sensitivity handled within that specific department. It seems that the Facilities & Management department scores the lowest and Legal & Compliance scores the highest, which is in line with expectations. Regardless, the Maastricht University ransomware attack was caused by a Facilities & Maintenance employee who opened a phishing link. Therefore, organization should consider employees in 'the lowest ranks' as much as a potential weak link as they would consider someone from the higher ranks within their organization. Additionally, departments not included in this thesis could be included with their respective score, given that this scoring is a result from proper research or empirical evidence.

4.2.3 Job Role

For job role we chose four different main roles. It seems that higher management roles have the highest impact when fallen victim to a cyberattack, but there is not much difference with executive personnel. Operational personnel have the lowest impact out of these four, with lower management having a similar impact according to the results. Important to note is that job roles can be sub-classified into different specific jo roles. It would be equally important to base the scores given on any job role not included in this thesis upon proper research or empirical evidence.

4.2.4 Probability

Other than the previous factors, the scoring for a working's industry probability to fall victim to a cyber-attack is based upon reported data from STATISTA. Working industries have been categorized based upon the amount of social engineering-based cyber-attacks. This may cause an exclusion of other important cyber-attacks such as system intrusions or privilege misuse, which could be considered a result of human error too. Nevertheless, for future research purposes it may be beneficial to include more types of cybersecurity issues as a result from human behaviour, thereby categorizing the probability of a working industry to fall victim to cyber-attacks in a more accurate manner, which contributes to a more accurate placement on the employee profile matrix.

4.4 Methods of training

Using tailored training programs can be very beneficial for organizations to mitigate their risk of falling victim to cybercrimes. In this thesis, we have mainly focused on how to differentiate between employees. Regardless, a point of attention which should not be ignored is the available and preferred methods of training. By educating their employees on the threats, risks and overall information security awareness policies, organizations can reduce losses (as a result of cyber-attacks) significantly (77, 78). However, as there is no 'one size fits all' approach for these training modules, the way in which these training modules are presented or given to employees may just be as important. It is imaginable that a PowerPoint presentation about a certain subject regarding cybersecurity may be very exciting to one person, but unappealing to another person within the same employee profile. It is therefore recommended for developers of these training modules to consider the different types of training which could be appealable to employees. Examples are case studies, eLearning modules, 1-on-1 coaching, instructor-led training, interactive training or training by means of gamification (79). Research from Pattinson et al. found that 'the extent to which the training an individual received matched their learning preferences was positively associated with their ISA level' (80). However, they state that the frequency in which the training was given did not directly predict ISA levels. It is therefore safe to state that an increased frequency of training could and would be beneficial, but an excess in training would probably receive the opposite result. Thus, it is recommended for organizations to consider the possible methods of training for their employees.

We have employed a comprehensive approach to construct employee profiles by examining individual-level demographics, sensitivity factors, and incorporating insights from both literature and experts. Our research acknowledges the limitations of the available literature and emphasizes its foundational nature for future endeavours in addressing and mitigating cyber threats. The analysis of individual demographics, such as age, education level, gender, and ISA policy knowledge, has provided valuable insights into their influence on safe behaviour. Furthermore, the inclusion of sensitivity factors, considering working industry, department, job role, and industry probability, contributes to a holistic understanding of information security. As we recommend the inclusion of additional demographic factors and explores methods of training, it highlights the dynamic nature of the employee profile matrix and its potential evolution in future research and practical applications. The incorporation of Hofstede's cultural dimensions and diverse training methods further emphasizes the need for tailored approaches in enhancing information security awareness and behaviour among employees. Ultimately, this research serves as a starting point for a more nuanced understanding of factors shaping employee profiles and offers a foundation for the development of targeted and effective training programs in the realm of cybersecurity.

5. Self-reflection

When initially looking for an internship, I did not expect to end up in the world of IT Auditing. Especially with the background in biomedical sciences, I figured I would probably end up at a company that specializes in health-related matters. However, as I have always had a weakness for IT and IT-related projects/matters, I saw this internship period as the perfect opportunity to delve into the business side of IT. Hence, I applied for the internship at EY and fortunately was allowed to perform my research within their walls. At first, I did not know what to expect from the internship, as it seemed that I was ‘from another planet’ when it came to the technical knowledge about the world of IT risk assurance. However, I was set to learn as much as possible since I really like working in this field. I wanted to learn how these IT audit meetings were performed, how they were processed and what the final effect was of such an audit. Additionally, I wanted to learn more about cybersecurity and how organizations can improve their cybersecurity, since there has been a lot of news in the media about big multinational companies or governmental institutions that fell victim to cyberattacks, often to a great extent. Something about all this just intrigued me more and more, which made me come up with the scope of my research, being individual employees that can be a weak link in the fight against cybercrime. Hence, I figured that improving their skills and knowledge about cybersecurity (policies) could contribute to a better IT-infrastructure for organizations to mitigate these malicious cyberattacks.

A big challenge though was to understand the daily work of my colleagues. It seemed that people were working on different projects, from IT general control audits to dissecting project timelines for big companies to see where they dropped the ball and how they could improve. Furthermore, some colleagues were working on cloud-related services and others were busy with privacy-related projects. At first, I felt lost because of all this various work, but I soon realized that it is an opportunity for me to see which area I would like to work in the most and which areas I liked less. Additionally, I must say that the FBE courses did not really prepare me for the world of IT audits, but something that I learned in these courses proved quite handy on the job. It seemed that an understanding of the hierarchy within an organization such as EY is very important, as it shows the route you can traverse from intern on. During the courses we were often told that an organizations hierarchy is of utmost importance. It was also an eye-opener for me, as I have never really worked in such a professional setting, I must say that I underestimated the importance of etiquette on the work floor. In my last internship in the lab, it was fairly an informal setting with music on the work floor and people just walking around doing their own thing, which had a significantly different atmosphere. At EY, I noticed that the business world requires a way more formal approach to your peers and the people around you in general: it is something that I expected, but still underestimated to a certain extent. Therefore, this internship proved quite useful for me to adapt to the etiquette a company as EY requires.

Subsequently, I noticed that my lack of experience in the world of IT (specifically IT auditing) was somewhat a weakness in order to set up my research. The start was very slow, and I did not really know which aspects intrigued me the most, up until I realized that I could combine my analytic skills, which I consider as a major strength, in order to tackle a real-life problem which organizations such as EY could benefit from. Therefore, I think when I finally had my goal in sight, I worked tirelessly to come up with a decent and useful research. Furthermore, I’d like to state that a bigger focus on IT could be beneficial for the FBE courses, but I am glad that it is not absent completely.

The whole process started when partners from Dell came over to the Utrecht University campus and gave a workshop on how Web3 and blockchain are evolving. This planted a seed in my mind which made me realize that I’d love to work in an IT-related field. After some research I found the EY internship job position. With my sister working at EY (Financial Audit) for over 5 years, she recommended me to take up this offer as EY was a very good place to start my career. Lastly, I really enjoyed my time at EY Utrecht and I am happy to say that I got offered a contract by EY to start my career with them after I graduate from the SBM master.

6. References

1. EY Legal Statement 2023.

2. EY Awards & Recognitions 2023.

3. EY Accomplishments & Accolades 2023.

4. EY Ripples Program.

5. von Solms R. Information security management: why standards are important. Information Management & Computer Security. 1999 Mar;7(1):50–8.

6. IBM: What is a zero-day exploit?

7. Nallainathan S. Study among Rural area citizen regard to Cyber Security awareness & Factors relating to it. 2021 Jan;9:322–6.

8. ENISA - Cyber threats.

9. ENISA - Threat Landscape.

10. IBM - What is Ransomware?

11. What Maastricht University learned from the ransomware attack (part 1) | SURF.nl.

12. A cyber-attack like in Maastricht: small chance, but the impact is enormous | DUB (uu.nl).

13. [What is Social Engineering? | IBM.

14. What is a DDoS Attack? | IBM.

15. What is supply chain security? - IBM Blog.

16. Abbiati G, Ranise S, Schizzerotto A, Siena A. Merging Datasets of CyberSecurity Incidents for Fun and Insight. Front Big Data. 2021 Jan 26;3.

17. Manshu Xu, Chuanying LU. China–U.S. cyber-crisis management. Springer Nature - PMC COVID-19 Collection. 2021 Jun 28;3(1):97–114.

18. Benjamin Edwards, Alexander Furnas, Stephanie Forrest, Robert Axelrod. Strategic aspects of cyberattack, attribution, and blame. Proc Natl Acad Sci U S A. 2017 Feb 27;114(11):2825–30.

19. Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Comput Secur. 2021 Jul;106:102267.

20. Ignatovski M. Healthcare Breaches During COVID-19: The Effect of the Healthcare Entity Type on the Number of Impacted Individuals. Perspect Health Inf Manag. 2022;19(4):1c.

21. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022 Jul 17;47(3):698–736.

22. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

23. https://www.cisco.com/c/en/us/products/security/what-is-data-breach.html#:~:text=A%20data%20breach%20is%20a,files%20to%20the%20wrong%20recipient.

24. Lundgren B, Möller N. Defining Information Security. Sci Eng Ethics. 2019 Apr 15;25(2):419–41.

25. [https://www.verdict.co.uk/uk-data-breaches-human-error/.

26. Hong Y, Furnell S. Understanding cybersecurity behavioral habits: Insights from situational support. Journal of Information Security and Applications. 2021 Mar;57:102710.

27. White G, Ekin T, Visinescu L. Analysis of Protective Behavior and Security Incidents for Home Computers. Journal of Computer Information Systems. 2017 Oct 2;57(4):353–63.

28. https://www.ibm.com/topics/cyber-attack.

29. https://www.ibm.com/topics/phishing.

30. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences. 2022 Nov;34(10):8176–206.

31. Greathorn Business Email Compromise Report.pdf.

32. Cross C, Gillett R. Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud. J Financ Crime. 2020 Apr 22;27(3):871–84.

33. Abiodun O. An Enhanced Practical Difficulty of One-Time Pad Algorithm Resolving the Key Management and Distribution Problem. 2018.

34. Achim MV, Văidean VL, Borlea SN, Florescu DR. The Impact of the Development of Society on Economic and Financial Crime. Case Study for European Union Member States. Risks. 2021 May 18;9(5):97.

35. Ünvan YA. Financial Crime: A Review of Literature. In 2020. p. 265–72.

36. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity.

37. Sokratis Nifakos, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, et al. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors (Basel). 2021 Jul 28;21(15):5119.

38. Ng BY, Kankanhalli A, Xu Y (Calvin). Studying users' computer security behavior: A health belief perspective. Decis Support Syst. 2009 Mar;46(4):815–25.

39. Waly N, Tassabehji R, Kamala M. Improving Organisational Information Security Management: The Impact of Training and Awareness. In: 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems. IEEE; 2012. p. 1270–5.

40. Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. Correlating human traits and cyber security behavior intentions. Comput Secur. 2018 Mar;73:345–58.

41. Bauer S, Bernroider EWN, Chudzikowski K. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Comput Secur. 2017 Jul;68:145–59.

42. Metalidou E, Marinagi C, Trivellas P, Eberhagen N, Skourlas C, Giannakopoulos G. The Human Factor of Information Security: Unintentional Damage Perspective. Procedia Soc Behav Sci. 2014 Aug;147:424–8.

43. Talib S, Clarke NL, Furnell SM. An Analysis of Information Security Awareness within Home and Work Environments. In: 2010 International Conference on Availability, Reliability and Security. IEEE; 2010. p. 196–203.

44. Ahlan AR, Lubis M, Lubis AR. Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. Procedia Comput Sci. 2015;72:361–73.

45. Akter S, Uddin MR, Sajib S, Lee WJT, Michael K, Hossain MA. Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Ann Oper Res. 2022 Aug 2;

46. Branley-Bell D, Coventry L, Dixon M, Joinson A, Briggs P. Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. Hum Behav Emerg Technol. 2022 Oct 21;2022:1–10.

47. Pattinson M, Butavicius M, Parsons K, McCormac A, Calic D. Factors that Influence Information Security Behavior: An Australian Web-Based Study. In 2015. p. 231–41.

48. Mittal S, Ilavarasan PV. Demographic Factors in Cyber Security: An Empirical Study. In 2019. p. 667–76.

49. Darwish A, Zarka A El, Aloul F. Towards understanding phishing victims' profile. In: 2012 International Conference on Computer Systems and Industrial Informatics. IEEE; 2012. p. 1–5.

50. Kumaraguru P, Sheng S, Acquisti A, Cranor LF, Hong J. Teaching Johnny not to fall for phish. ACM Trans Internet Technol. 2010 May 10;10(2):1–31.

51. Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. Who falls for phish? In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM; 2010. p. 373–82.

52. Emma Ojala Burman. Impact of demographic factors on information security awareness: a study on professionals and students in Sweden . 2021;

53. Whitty M, Doodson J, Creese S, Hodges D. Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. Cyberpsychol Behav Soc Netw. 2015 Jan;18(1):3–7.

54. Li L, Xu L, He W. The effects of antecedents and mediating factors on cybersecurity protection behavior. Computers in Human Behavior Reports. 2022 Mar;5:100165.

55. McCormac A, Zwaans T, Parsons K, Calic D, Butavicius M, Pattinson M. Individual differences and Information Security Awareness. Comput Human Behav. 2017 Apr;69:151–6.

56. Chua HN, Wong SF, Low YC, Chang Y. Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics. 2018 Sep;35(6):1770–80.

57. Agarwal R, Prasad J. Are Individual Differences Germane to the Acceptance of New Information Technologies? Decision Sciences. 1999 Mar 7;30(2):361–91.

58. Bulgurcu, Cavusoglu, Benbasat. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. 2010;34(3):523.

59. Cronan TP, Leonard LNK, Kreie J. An Empirical Validation of Perceived Importance and Behavior Intention in IT Ethics. Journal of Business Ethics. 2005 Feb;56(3):231–8.

60. Kranz J, Haeussinger F. Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. Vol. 3, International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design. 2013.

61. Hanus B, Windsor JC, Wu Y. Definition and Multidimensionality of Security Awareness. ACM SIGMIS Database: the DATABASE for Advances in Information Systems. 2018 Apr 25;49(SI):103–33.

62. Jaeger L. Information Security Awareness: Literature Review and Integrative Framework. In 2018.

63. Ryan JE. A COMPARISON OF INFORMATION SECURITY TRENDS BETWEEN FORMAL AND INFORMAL ENVIRONMENTS. 2006 Aug 7;

64. STATISTA - Annual Report Data Breaches Worldwide By Industry.

65. STATISTA - About Us.

66. Govender S, Kritzinger E, Loock M. The influence of national culture on information security culture. In: 2016 IST-Africa Week Conference. IEEE; 2016. p. 1–9.

67. https://www.simplypsychology.org/hofstedes-cultural-dimensions-theory.html.

68. Hofstede - Model of National Culture.

69. Et. al. NHNZ. Synthesizing Cybersecurity Issues And Challenges For The Elderly. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021 Apr 10;12(5):1775–81.

70. Hadlington L, Parsons K. Can Cyberloafing and Internet Addiction Affect Organizational Information Security? Cyberpsychol Behav Soc Netw. 2017 Sep;20(9):567–71.

71. Hwang I, Wakefield R, Kim S, Kim T. Security Awareness: The First Step in Information Security Compliance Behavior. Journal of Computer Information Systems. 2021 Jul 4;61(4):345–56.

72. Whiteside SP, Lynam DR. The Five Factor Model and impulsivity: using a structural model of personality to understand impulsivity. Pers Individ Dif. 2001 Mar;30(4):669–89.

73. Egelman S, Peer E. Scaling the Security Wall. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. New York, NY, USA: ACM; 2015. p. 2873–82.

74. Anderson, Agarwal. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly. 2010;34(3):613.

75. Hazari S, Hargrave W, Clenney B. An Empirical Investigation of Factors Influencing Information Security Behavior. Journal of Information Privacy and Security. 2008 Oct 10;4(4):3–20.

76. Chan M, Woon I, Kankanhalli A. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security. 2005 Jul 10;1(3):18–41.

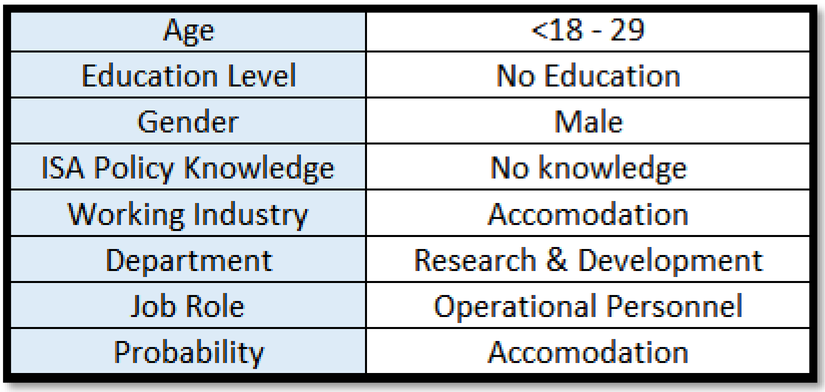
77. Return on investment (ROI) of cybersecurity training | Infosec (infosecinstitute.com).

78. Value of Security Awareness Training | Arctic Wolf, How effective is security awareness training? (usecure.io).

79. 7 Types of Training Methods (and How to Choose) | ELM Learning.

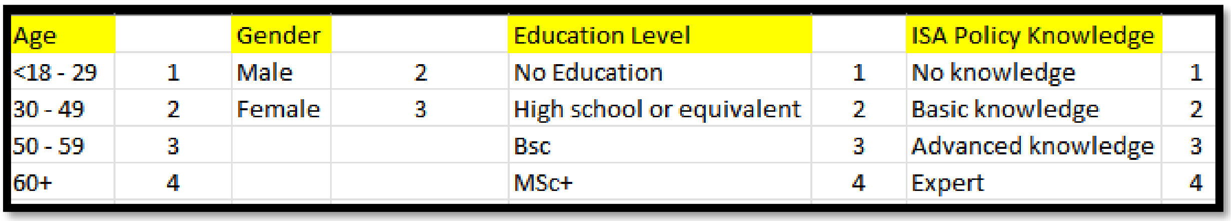
80. Pattinson M, Butavicius M, Lillie M, Ciccarello B, Parsons K, Calic D, et al. Matching training to individual learning styles improves information security awareness. Information & Computer Security. 2019 Nov 11;28(1):1–14.

Appendix



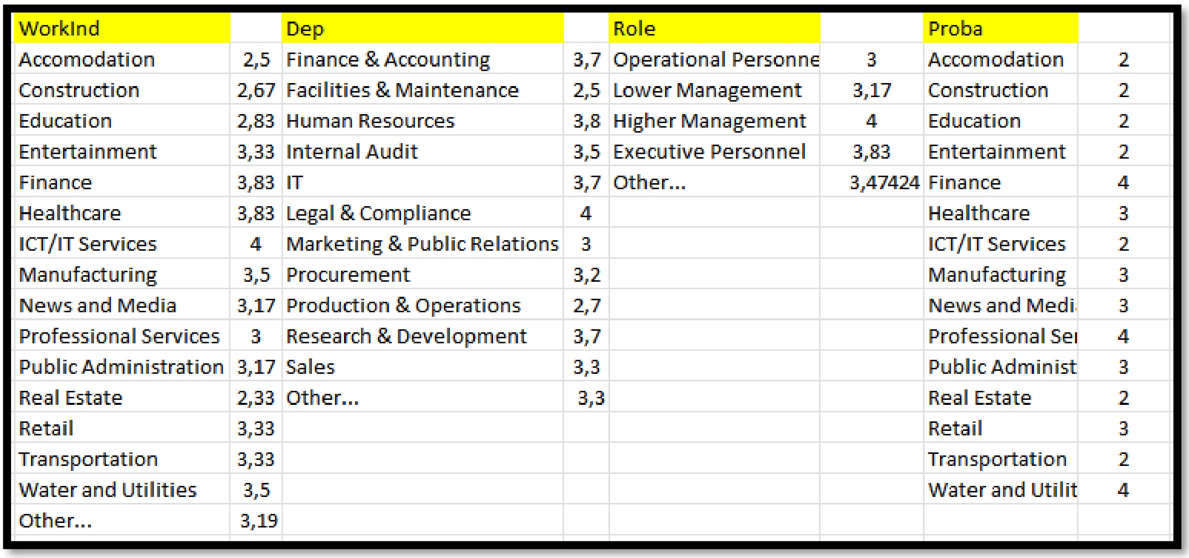
Age	<18 - 29
Education Level	No Education
Gender	Male
ISA Policy Knowledge	No knowledge
Working Industry	Accomodation
Department	Research & Development
Job Role	Operational Personnel
Probability	Accomodation

Figure E: Visualization of customizable input factors in the Employee Profile Matrix.



Age		Gender		Education Level		ISA Policy Knowledge	
<18 - 29	1	Male	2	No Education	1	No knowledge	1
30 - 49	2	Female	3	High school or equivalent	2	Basic knowledge	2
50 - 59	3			Bsc	3	Advanced knowledge	3
60+	4			MSc+	4	Expert	4

Figure F: The demographic factors for the ‘Skill level’ axis and their respective scores as used in the Employee Profile Matrix.



WorkInd		Dep		Role		Proba	
Accomodation	2,5	Finance & Accounting	3,7	Operational Personne	3	Accomodation	2
Construction	2,67	Facilities & Maintenance	2,5	Lower Management	3,17	Construction	2
Education	2,83	Human Resources	3,8	Higher Management	4	Education	2
Entertainment	3,33	Internal Audit	3,5	Executive Personnel	3,83	Entertainment	2
Finance	3,83	IT	3,7	Other...	3,47424	Finance	4
Healthcare	3,83	Legal & Compliance	4			Healthcare	3
ICT/IT Services	4	Marketing & Public Relations	3			ICT/IT Services	2
Manufacturing	3,5	Procurement	3,2			Manufacturing	3
News and Media	3,17	Production & Operations	2,7			News and Medi	3
Professional Services	3	Research & Development	3,7			Professional Se	4
Public Administration	3,17	Sales	3,3			Public Administ	3
Real Estate	2,33	Other...	3,3			Real Estate	2
Retail	3,33					Retail	3
Transportation	3,33					Transportation	2
Water and Utilities	3,5					Water and Utilit	4
Other...	3,19						

Figure G: The demographic factors for the ‘Sensitivity in information handling’ axis and their respective scores as used in the Employee Profile Matrix.