The Elicitation of Cybersecurity Narratives: Bricoleur Story Completion, Decision making & Security design

Part 2.

Prof Julie Gore, Dr Jonathan Foster,
Dr Efpraxia Zamani , Dr David Gamblin,
Dr Sally Sanger, & Billie Dale

August 2023

discribe
IMAGINING SECURE DIGITAL FUTURES

The Discribe Hub+ is funded by UKRI through ESRC
Grant no: ES/V003666/1
For more information about the Hub+ please visit
www.discribehub.org

(C) 2021 Discribe Hub+ Creative Commons 4.0 BY-NC-SA Licence.
www.discribehub.org/copyright

Acknowledgements

We would like to thank the Digital Security by Design Social Science (Discribe) Hub+ and in particular: Professor Adam Joinson, Professor Genevieve Liveley and Nicola Llyod for their constant support throughout the project. Sincere thanks to our participants who took the time to engage with our story stems and critical decision interviews.

We also wish to warmly thank our early career team members whose enthusiam and curiosity for this area remains infectious: to Dr Wei Huang (Post Doctoral Research Assitant) who contributed to the initial scoping of the project and piloting of our story stems; Billie Dale (Research Assistant) who operationalised our story stem surveys and Critical Decision Method (CDM) interviews and analysis, and to Dr Sally Sanger (Post Doctoral Research Assistant) who was lead author for Part one of the project providing a rapid evidence review of security technology adoption.

Contents

Executive Summary

This report (part two) presents part of the work and findings of a 15-month investigative project examining security adoption decision making. It forms part of a wider portfolio of work funded by the ESRC-funded Digital Security by Design Social Science Hub+ (Discribe).

The project ran from May 2022 to August 2023 and was conducted in collaboration with a multidisciplinary team of academics at Birkbeck, University of London and the University of Sheffield. In the latter stages of the project one member of team joined the University of Durham.

- Part One: Understanding the security technology adoption process: a rapid evidence review

  The evidence from the Rapid Evidence Review points to the need for a holistic approach to adopting new security technologies which, firstly, should pervade all activities connected with this including e.g., risk management, dealing with unexpected consequences and decision-making. Secondly, no one risk factor should be focused on to the exclusion of others: technological risks and decisions are not more important that organisational, human or environmental ones. Finally, it is clear that adoption is not a process that can stop at the installation of the technology but must continue through the product's lifecycle.

- Part Two: Story completion and Critical Decision expert interviews

  The research completed here offers researchers a useful story stem survey methodology which provides cognitive insights into the challenges of cyber security adoption decision making in large organisations. We have much to learn from how experts and non-experts respond to challenging scenarios which may provide useful contextualisation to further explore decision making under uncertainty. We contend that a more detailed examination of risk, emotions, accountability, cynicism/negativity and a positive psychological approach to the design of cyber security interventions, policy and practice may effectively support behavioural and cognitive change.

List of Abbreviations

CDM – Critical Decision Method

CTA – Cognitive Task Analysis

HEE – Higher Education England

MFA – Multi-factor authentication

TAM – Technology Acceptance Model

1. Introduction

1.1 Project aim and objectives

Aim: To understand the process of security technology adoption within organisations.

Goals:

- Identify the perceived benefits and risks, organisational conditions and consequences of adopting new security technologies. (Part 1 & 2)
- Understand and review academic literature examining complexities in individual cognitive and organizational decision making processes associated with adoption/non-adoption. (Part one)
- Understand the role of regulatory governance and other incentives in institutionalising the adoption of new security technologies . (Part 1 & 2)
- Use a case story completion survey method and critical decision method (CDM) as innovative qualitative research approaches for eliciting and documenting the bases for analysing the benefits and risks, organizational conditions and consequences, and incentives related to the adoption of new security technologies. (Part 2)

1.2 Report coverage and structure

This report presents findings from Part 2 of the project and documents a creative methodological story stem survey tool to explore the perceptions, cognitions and behaviour of people working as IT experts and non experts in large organisations. Over 450 stories were completed via the online survey platform, Prolific in two waves with a general working population and an expert population working in IT related roles in large organisations. This is followed by the presentation of findings from an in-depth Critical Decision Method (CDM), cognitive task analysis interview study which primarily focussed upon IT security related experts working in large financial and Higher Education organisations.

2. Story Completion

2.1 Introduction

Cyber security has become a critical risk factor for organisations due to a number of high-profile security breaches which have been publicised in recent years (Securities and Exchange Commission, 2018). A security breach is when information is accessed by unauthorised and often malicious parties, including phishing, information leaks, and ransomware attacks. Organisations mitigate the exposure to these risks by adopting cyber security technologies. Previous studies have examined cyber security using a technical approach (Assante & Tobey, 2011; Jang-Jaccard & Nepal, 2014; Torres et al., 2019). Nevertheless, less is known regarding how decisions to adopt new cyber security technologies are made, the cognitive processes involved, as well as the perceived risks and benefits associated (Herath et al., 2020; Wang et al., 2021). Understanding more about the process of cyber security adoption at the organisational group and individual level rather than exclusively using a technological approach to analysis we suggest here, could have benefits in various ways. Firstly, it could identify common issues or problems that arise in an attempt for future decision-makers, technology developers, security technology designers etc. to avoid and/or support similar issues happening in the future. Furthermore, the clients or organisations and citizens/society warrant more of an understanding how organisations protect their information.

The purpose of this research is to identify how employees with varying knowledge perceive the process of adopting cyber security technology within an organisation. This includes the perceived risks and benefits, the organisation structure/culture in terms of cyber security, and the cognitive process of the decision-makers when discussing the potential adoption of secure technologies. Furthermore, this report will discuss the benefits of using the story completion methodology to gain valuable qualitative data. First, we will discuss background research into the cyber security adoption process. Following this, we outline our approach and methodology, as well as a themes based analysis that were identified from the 450 plus stories which were analysed. We conclude by reflecting on the accuracy of the story completion methodology as well as how this research has provided further knowledge on the perceptions of cyber security adoption and inferring the decision-making cognitions within these discussions. Lastly, we discuss areas for future research to develop these findings and how the story completion method shows promise for being advantages in future research.

2.1.1 Background

The DSbD programme has been established in response to a significant market need for increased cyber security (Johnson, 2022). This need has arisen because of the increased risk posed by digital vulnerabilities within a connected digital ecosystem. The effective implementation and use of new cyber security will be dependent not only on the objective features of the technology but also on organisational actors' subjective interpretations of and interactions with it (Orlikowski, 1993). This is known as the duality of technology, where its objective features meet with subjective interpretations via ongoing interaction (Orlikowski, 1993). These interactions and actions taken by decision-makers and users can have intended and sometimes unintended effects and consequences that lead to non-adoption. Thus, understanding the adoption process requires understanding the role of actors when interpreting the technology within their organisational conditions, and how that security technology is re-designed and used in practice via actors' interactions with it. This has been a long-standing topic of interest within information systems and information management (Brous et al., 2020; Davis, 1989; Orlikowski, 1992). Nevertheless, there is little research into the cognitive decision-making processes of these actors involved in its initial development and adoption along with the users' interactions with and perceptions of it.

Similarly, the majority of data breaches within organisations are reported as being due to human error (Dykstra, 2016; Kelly, 2017; Metalidou et al., 2014; Soltanmohammadi et al., 2013), thus it is also important to understand the perceptions and beliefs of employees and non-IT staff related to cyber security decision making. Without the staff, cyber security technology would be ineffective, and thus we argue, understanding their behaviour and cognitions are most important to combat data breaches. Despite the security policies made by IT experts, non-IT staff often report that they do not know or understand these policies or the procedures in place to protect their data and the organisation (Burke, 2020). Hence, although the risk to security is a major risk factor for the whole organisation, non-IT staff may be less aware of this risk and therefore less compliant. If we are to better understand how non-IT staff believe these decision-makers act, think, and feel, this could lead to a wealth of information regarding the culture and experiences of cyber security within large organisations.

2.1.2 Story completion methodology

Using the story completion method, we collected and analysed in total 454 stories about fictional situations regarding cyber security adoption within the workplace. This method involves participants writing short stories in response to prompts (story stems). This methodology was first used as a qualitative method in the field of feminist psychology in the early 1970s, and there has been increasing interest in the story completion method in other social science disciplines in the last few years (Moller et al., 2021; Clark, et al 2019). Recently, the method has been adopted within social psychology, and completed stories are primarily analysed thematically (Gerhold et al., 2019; Watson & Lupton, 2022). There are limited studies using storytelling to understand security issues, Gerhold et al. (2019) used a foresight approach based on sociotechnical imaginaries to investigate the coevolution of security technologies and societal development in Germany. They also used storytelling in scenarios to capture potential future developments and make them accessible in a broader negotiation process about the pros and cons of implementing new security technologies. Furthermore, Watson and Lupton (2022) in Australia used story completion methodology to identify people's perceptions and ideas surrounding the protection and privacy of their personal digital data. Thus, we chose this method because it encourages participants to be creative and consider different aspects of cyber security adoption in a safe research context.

2.1.3 Study aims

In this study, there were four story stems developed by the research team in consultation with different stakeholders associated with Discribe along with professional doctoral candidates working in a range of large organisation. To encourage creativity further, participants were given the prompt:

"What is most likely to happen? Please use your imagination to complete the story."

It is assumed that the narratives written in response to the story stems draw on the writers' own perspectives and feelings, without involving direct questioning which can encourage more rigid responses.

The aims of this study are threefold, to:

- understand the perceived benefits and risks of users of security technology.
- identify the organizational conditions and consequences of adopting new security technologies.
- determine the cognitive decision making processes which are utilised and shared by individuals involved in adoption discussions, policy or process.

2.2 Methodology

2.2.1 Participants

The project involved two separate study publications of our story stem questionnaire via the Prolific (www.prolific.co) online platform. To recruit the first sample of non-cyber experts, the following characteristics were set: lived in the UK, fluent in English, 18+ years old, not a student, worked in an organisation with 1000+ employees and had partaken in at least 10 previous studies with an approval rate of 90-100%. We wanted to ensure the participants' narratives was coming from experience of working in a large organisation. The demographic information was taken from a self-report questionnaire when individuals signed-up to Prolific. Firstly, a pilot study was published on Prolific with a target of eight participants to determine if the story stems were clear and comprehendible by non-IT experts. Following the pilot's success, the questionnaire was published again to recruit a further 60 participants. Of these 68 participants, four were removed as their responses were shorter than 10 words, or provided no extra information (i.e., reworded the story stem). This left a sample of 64 participants.

Of our 64 participants, 38 identified as male (59.4%), with the rest identifying as female. The sample ranged in age from 25-72 years, with a mean age of 41.09 (*SD* = 9.51). The majority of participants were White (87.5%), 4 identified as Asian, 2 as Mixed, 1 as Black, and 1 as other. At the end of our questionnaire, we asked participants to state their job title. Using the UK Standard Industrial Classification (SIC) Tool (Office for National Statistics, n.d.), these jobs were classified into sectors. Table 1 shows the number of participants who are classified into certain professions, with the most common profession being Section M: Professional, scientific and technical activities.

In the second publish of our questionnaire, we specifically aimed to recruit cyber security experts. To find a specific sample, we firstly created a pre-screen questionnaire on Prolific (www.prolific.co). The requirements set for the 200 people recruited for the pre-screen survey were: characteristics were set: lived in the UK, fluent in English, 18+ years old, not a student, worked in an organisation with 1000+ employees and had partaken in at least 10 previous studies with an approval rate of 90-100%. The questions asked and the answers the participants could choose from are shown in Table 2. From the 200 responses, 36 worked in IT with a company with 750+ employees and responded that they make security adoption decisions 'Very often', or 'Often'. Since we wanted a larger sample, we also included the 21 participants who had been in sector for 10+ years and responded making adoption decisions 'Somewhat often'. This left us with 57 participants who were invited to complete the main survey on Qualtrics, of which 53 of them completed it. One participant was excluded as their responses were too long for the time they spent on the survey, indicating possibly that they used AI-generated text. It was considered in the best interest of the study to remove their data.

Table 1 *Job sector of participants classified using the UK Standard Industrial Classification (SIC) Tool (Office for National Statistics, n.d.).*

Profession	Number of participants
Section M: Professional, scientific and technical activities	22
Section N: Administrative and support service activities	17
Section Q: Human health and social work activities	7
Section J: Information and communication	7
Section K: Financial and insurance activities	4
Section P: Education	5
Section S: Other service activities	2
Section G: Wholesale and retail trade	2
Section O: Public administration and defence	2
TOTAL	64

Table 2 *The pre-screening questionnaire.*

Questions	**Answers**
How many employees does the company you work for have?	▪ 250-500 ▪ 500-750 ▪ 750-1000 ▪ 1000+
Do you work in the IT and/or cyber-information security sector?	▪ Yes ▪ No
If yes, how long have you been in this sector?	▪ 1-5 years ▪ 6-10 years ▪ 11-15 years ▪ 15+ years ▪ Not Applicable
In your role, how often do you make security adoption decisions?	▪ Very often ▪ Often ▪ Somewhat often ▪ Not often ▪ Never

Of the 52 participants, 43 identified as male (82.7%), with the rest identifying as female. The sample ranged in age from 22-63 years, with the mean age being 38.62 (*SD* = 9.28). The majority of participants were White (75.5%), 7 identified as Asian, 1 as Mixed, 3 as Black, and 1 as other.

2.2.2 Materials and Procedure

Once recruited, participants were redirected to Qualtrics (www.qualtrics.com), an online survey platform, and were guided to respond to four story stems (below). Both sets of participants completed the same story completion survey on the online platform. The complete questionnaire can be found on Appendix A. The story stems were developed to elicit narratives around the adoption of new cyber technology within a workplace. As stated previously the story stems were: piloted with advisors of the DSbD network who were cyber security experts to ensure the scenarios were realistic; they were also piloted with PhD students to check for ease of use, and were redrafted until they closely aligned with real-life situations. Asking participants to write about 'What is most likely to happen?', prompted participants to discuss the actions and emotions from each character in the story stem. Being asked to 'use your imagination' encouraged participants to be creative and ensured the task were cognitively demanding. The story stem prompts can be seen below:

1. It's 2024. A new hardware has recently been proven to reduce cyber vulnerability by 70% without interrupting users' usual activities. A and B – who are senior/strategic managers in organisation X – are having a meeting to discuss whether organisation X should become one of the first organisations in the world to adopt this new hardware.

   What is most likely to happen? Please use your imagination to complete the story.

2. C who works in organisation Y received an email from the IT department two weeks ago, requesting all employees to complete a software update within one month, which was related to a new hardware adopted across organisation Y to increase cyber security. C came to work this morning, only to find his/her work computer locked by a ransomware attack.

   What is most likely to happen? Please use your imagination to complete the story.

3. After a six-months transition period, organisation Z has implemented the new hardware to increase cyber security across all departments. Head of IT department D has just sent out an organisation-wide email announcing this milestone, before he / she gets an urgent call from

E, the head of another department, reporting a severe data leak which requires an immediate solution.

What is most likely to happen? Please use your imagination to complete the story.

4. It has been 5 years since F, the principle legal advisor of organisation W, called for the first meeting of senior management level regarding the adoption of the new hardware to increase cyber security. These meetings have been more and more frequent over these years, and today is the 17th meeting where proposals for incentives are being discussed.

What is most likely to happen? Please use your imagination to complete the story.

Participants were asked to write a story that was at least four sentences and were asked to spend at least 5/10 minutes responding to each story. Instructions noted that,

> "There is no right or wrong way to complete the story, and you can be as creative as you like. The stories are based upon fictional events. We are interested in the many different stories that people can write. Please don't spend too long thinking about what might happen next — just write about whatever first comes to mind."

After participants completed the stories, they were asked 3 likert questions, and one open-ended question. The first likert scale question asked: "How comfortable / uncomfortable were you by being asked to respond to the stories?" They were then given four answer statements to choose from: "very comfortable", "quite comfortable", "quite uncomfortable", and "very uncomfortable". The second likert question asked: "How familiar were the stories to you?" The four answer statements to choose from were: "very familiar", "quite familiar", "quite unfamiliar", and "very unfamiliar". The third and final likert question asked the participants: "How do your responses to the stories compare to what you would do in practice if similar events arose?" The four answer statements to choose from were: "very familiar", "quite familiar", "quite unfamiliar", "very unfamiliar". The goal of these questions was to determine whether the individuals taking part were IT experts or non-IT persons, and also to determine whether putting themselves in the shoes of the decision-makers made people feel uncomfortable in any way. The last question asked participants to disclose their job role if they were comfortable. This was an optional question however all participants provided an answer. Participants took around 25 minutes to respond and were reimbursed £3.34 (equating to £8/hour) for their time.

2.2.3 Data analysis

Of the 272 stories from the first sample of non-experts, 22 were removed for being less than 10 words long or containing no new information (i.e., they simply reworded the story stem), leaving 250 stories for analysis. Stories 1-63 were answers to Story Stem (SS) 1, stories 64-126 answered SS2, stories 127-189 answered SS3, and lastly stories 190-250 answered SS4. The length of these stories ranged from 10-339 words, with the average being 72.8 words (*SD* = 53.85).

Of the 208 stories received from the second sample of experts, four were removed for the same reasons as above. This left a total number of 204 stories. (Stories 1-52 were answering SS1, stories 53-104 for SS2, stories 105-156 for SS3, and stories 157-208 for SS4). The length of stories from the expert sample included an anomaly. One of the experts wrote considerably more than the others. Participant 49 wrote over 500 words for each of the story stems. Since he or she took over an hour to complete the survey, it was determined that he/she could have written the responses, and it was not automatically considered to be the work of an AI word generator. However, with his/her data included, the length of the stories ranged from 10-632 words (M = 62.405, SD = 78.57). With his/her data excluded, the length of the stories ranged from 10-224 (M = 52.26, SD, 32.71). Thus, his/her responses did skew the average and was deemed an anomaly.

Our analytic approach was based on previous story completion papers (Watson & Lupton 2022). Deductive thematic analysis was completed as we had no pre-determined coding scheme to analyse the data. Firstly, the main coder familiarized themselves with the data, and identified potential codes. These codes were then grouped into larger themes by the initial coder. These themes were then discussed by a team of three researchers/authors of this report to ensure they held true (Nowell, Norris, & White, 2017), and the team came together to name and define these themes through a process of iterative discussions.

2.3 Results

We identified four themes related to cyber security cognition and behaviour across the stories:

- Accountability,
- Emotion,
- Cynicism and Negativity, and
- Reputational Benefits and Risks.

2.3.1 Accountability

2.3.1.1 Non-experts

In this sense, we defined accountability as “the state of being accountable, liable, or answerable” (Dictionary.com, n.d., definition of accountability). This mainly came in the form of trying to eliminate blame on themselves or assign blame onto an individual/group. Blame is defined as “the act of attributing fault” (Dictionary.com, n.d., definition of blame).

This theme was found largely in response to SS2 with 17.4% of the narratives from this question being coded for accountability. SS2 involved character C finding out their computer was compromised by a security breach following them receiving an email 2-weeks prior to request the completion a software update within 4 weeks. The story did not identify whether C had completed the software update or not, and many participants derived/perceived C to have not done the update, and would therefore be to blame.

They feel responsible that they did not action the software update quicker (story 107)

They decide that C is to blame (story 114)

They tell C that it's his/her fault for not completing the software update and report him to senior management (story 114)

C will expect to be blamed for the ransomware attack (story 117)

On the other hand, a handful of participants assumed the software update was completed by C, and thus the IT department was to blame.

C contacted the IT department to demand why an attack had been allowed to happen despite the update (story 76)

The organisation will beat fault for giving employees a month to update (story 77)

Comparatively, a few stories focused on C attempting to shift blame way from himself.

C was cleared of all blame (story 110)

C quickly decides that they haven't actually done anything wrong (story 105)

Similarly, blame and accountability was also coded in stories following SS3, where the head of IT, D, had just implemented a new security technology, and moments after sending the success email to staff, he gained knowledge of a security breach. Some participants described D attempting to reduce their accountability.

> *D is prepared to throw members of their team under the bus to protect their position and this is what follows, with blame being delegated once the cover up inevitably fails to work (story 161)*

> *D is expecting for their department to be blamed for this failure (story 180)*

2.3.1.2 Experts

A similar pattern was found with the narratives produced by the expert cyber technologists' responses. Blame was a common theme, being coded for 44% of the SS2 narratives. Similar to the non-experts, many of the expert narratives blamed C.

> *C might loose his job if it was discovered he did not update his software as instructed (story 66)*

> *C is likely to have a disciplinary meeting and further training around cyber attacks (story 74)*

> *C would be first questioned about why the new mandatory update was not applied on the machine (story 89)*

However, more commonly seen in these narratives than those from the non-experts, C was not blamed, instead blame was placed on the IT department. Some of the experts wrote that the IT department should not have given C the responsibility to do the update himself, and having such a large time-frame for an update leaves too much vulnerability.

> *Updates should be enforced within a week - or even the same day, not left to the individual employees (story 64)*

> *It's not really C's fault as two weeks was within the prescribed timeframe to apply the update. It's most likely that the IT department will be under scrutiny as to why the policy was so lax that a critical update was to be applied within 30 days (story 79)*

> *As it has only been two weeks, there will be no repercussions on C that this has occurred due to not completing the software upgrade (story 93)*

Lastly, a minority of the experts assumed C did the update and thus blamed the new software, assuming there were bugs/vulnerabilities in the software that allowed for this data breach.

> *The IT department will look into how the new adopted hardware and software updates have been compromised by ransomware (story 62)*

> *a group of cybercriminals exploited a vulnerability in the software update (story 63)*

> *the email sent contained malware which infected user Cs machine and may have infected other machines (story 71)*

Furthermore, blame was coded for 17% of the SS3 narratives. The most common code was that the experts blamed the hardware.

> *The new hardware cybe rsecurity system isn't working as expected and has revealed as a result, a severe data leak has ensued (story 113)*

> *The investigation concluded that the hardware is in fact the cause of the attack (story 124)*

> *The hardware they implemented wasn't tested thoroughly and introduces vulnerabilities into the company IT estate (story 149)*

Contrary to this, a group of experts assumed the data leak was unrelated to the new hardware.

> *They identify the source of the breach, which was unrelated to the new hardware implementation. The leak resulted from an employee mishandling sensitive information (story 116)*

> *[They] trace the leak to Russian hackers. Organisation Z decides to blame this leak on the war and outside influence (story 138)*

2.3.2 Emotion

2.3.2.1 Non-experts

When coding the data, it was clear that many stories created great amounts of emotion expressed either through exclamations, profanity, or adjectives. A total of 47 stories (19%) contained a quote which was coded under the theme 'emotion'. Zero were from SS11, twenty-six (41.3%) from SS2, nine (14.3%) from SS3, and twelve (19.6%) from SS4. The main emotion that came across was fear or panic from individuals. This was particularly true in SS2 and SS3 where data breaches had occurred.

> *C panics at the spur of the moment (story 94)*

> *C would be alarmed (story 98)*

> *"Shit!" yelled Charles as he looked at his desktop PC (story 125)*

D is petrified at that point in time (story 157)

There was also various mentions of stress or anxiety.

[The] data leak was a difficult and stressful experience (story 147)

The experience has left C shaken and uncertain about the security of their work files (story 84)

D is anxious that their boss will be very unhappy about this leak (story 165)

Various participants identified a feeling of frustration for the characters in the story. This was very apparent in SS4, where F was partaking in the 17th meeting over 5 years discussing adopting cyber security technology.

F is at this point feeling incredibly frustrated that the new hardware has not yet been implemented (story 215)

F is almost ready to give up (story 235)

There is considerable disquiet among themselves and staff at (story 236)

F has become more and more frustrated with each meeting (story 242)

F sighed after finishing the presentation, thinking to themselves that presenting on this subject was like running face first into a brick wall (story 247)

[F] was getting impatient, bored, and concerned. Seventeen meetings! (story 248)

There was a small minority of expressions of positive emotion such as pride following the 17th meeting as described in SS4. Some of the participants wrote a positive ending to the story, rather than a frustrating and negative one as the majority seemed to conjure.

As F leaves the meeting, they feel a sense of pride (story 208)

F closed the presentation and sat. Satisfied in himself that he may have finally got through (story 241)

F is pleased with the outcome of the meeting (story 208)

2.3.2.2 Experts

This theme was identified within the experts' narratives, however this was to a lesser extent than the non-experts. A total of 21 stories (10%) were coded for 'emotion'. Four (7.7%) were from SS1, six (11.5%) from SS2, six (11.5%) from SS3, and four (7.7%) from SS4.

Similar to the narratives from the non-experts, there was a clear sub-theme of fear, panic, and anxiety within these stories, the majority being from SS2.

> *A and B are too scared to be one of the first companies to adopt the hardware (story 44)*
>
> *Panicked, C immediately contacts the IT department to report the ransomware attack (story 81)*
>
> *C is worried they will lose their job (story 100)*
>
> *D's heart sank as they received the urgent call from E (story 107)*

Again, there was also a trend of frustration throughout the stories. The idea that there is nothing the character can do, and/or that the culture of cyber security will never change.

> *The Head of Department D swears internally and threatens harm against E (story 135)*
>
> *F leaves frustrated and begins planning meeting 18 (story 161)*
>
> *There will be a lot of frustrated senior managers having had the same conversations over the last few years about the same hardware (story 183)*

However, an interesting difference between the experts and non-experts, was that the narratives from the experts contained more positivity and therefore, more positive emotions.

> *They are excited about the competitive advantage it could bring (story 10)*
>
> *A and B felt proud of their bold decision (story 28)*
>
> *They felt hopeful about the technology's potential impact (story 38)*
>
> *A and B might be excited about the new hardware's potential (story 49)*
>
> *F felt a mix of satisfaction and determination, knowing that their efforts were finally making a lasting impact on the organization's security culture (story 160)*

2.3.3 Cynicism/ negativity

2.3.3.1 Non-experts

Whilst coding data, it was clear many participants added lots of creativity into their stories. This also resulted in some cynical responses. The adjective cynical defines someone as being distrustful and/or pessimistic and showing contempt for honest and morally-correct actions (dictionary.com). Twenty-six stories (10.4%) were coded for this theme, with the majority (57.7%)

coming from SS4, where character F, the legal advisor, calls the 17th meeting regarding the adoption of new hardware to increase cyber security.

Many participants included various statements indicating that they viewed the senior management team and decision-makers as invincible and/or conceited.

> *The new hardware decision was ratified, installed without issue, nobody told them no, nobody dared. Yes, yes, yes, promotion - yes, yes, yes, promotion and the sequenced repeated for generations (story 50)*

> *The elite IT cavalry upstairs could fix it, but he couldn't involve them (story 112)*

> *D wants a promotion and cares mostly about the right people being sold the story of progress and success. D is prepared to throw members of their team under the boss to protect their position (story 161)*

> *The same people will make suggestions and speak proudly of themselves for any success (story 201)*

This therefore highlights that employees often have the views that the decision-makers involved in cyber security adoption are untouchable, and often put on a high pedestal. It is also clear that some participants do not believe they are deserving of this description and view them as incompetent and unprofessional.

> *The two men normally disagreed, blinded by their competition (story 50)*

> *B, on the other hand, is completely sick and tired of dealing with supposedly professional employees (story 53)*

> *C procrastinated and spent most of the month watching Llama videos on the internet and making memes about cheese (story 104)*

> *He poured whiskey into his coffee, grew some courage and confessed his incompetence to his superiors (story 112)*

> *He had rushed the upgrade, cut corners, assumed they wouldn't be targeted and left work early to go drinking (story 112)*

> *F leaves wondering how on earth he is still able to command a six figure salary despite having the same level of achievements of a snail trying to climb mount Everest walking backwards (story 213)*

> *The CEO and CFO nodded, absentmindedly. They were quite sick of this. They knew their employees could be trusted. "Maybe next year." they said in unison (story 238)*

This speaks to the perception of a negative organisational cyber security culture, which is defined as attitudes and behaviour of employees surrounding the cyber security process implemented in the workplace (Marotta & Pearlson, 2019; Martins & Eloff, 2002). The narratives added to this further by describing the cyber security technology adoption process as frustrating.

> *As frustrating as it is... it will probably happen again even with the new hardware in place (story 160)*

> *Why does it always have to happen like this, thought D. Just as we take one step forward, it's two steps back again (story 160)*

> *As in the previous 16 meetings, there is a lot of empty talk and no actual change, the intractable impasse continues (story 22)*

> *Most managers consider these meetings an utter waste of time as nothing is ever being decided. People no longer come to the meetings prepared or with energy to present new ideas (story 240)*

2.3.3.2 Experts

Contrary to the narratives produced by the non-experts, there was a lot less cynicism and negativity in the expert narratives. However, there was still some signs of cynicism, mainly from SS4. Of the 15 codes of cynicism in the expert sample of stories, 46.7% were from SS4.

> *Organisation W would probably look for cheaper solutions to what is being proposed and would either not implement a solution or would half-heartedly adopt a weak alternative which would inevitably lead to data loss (story 196)*

> *F is just back from an all-expenses paid holiday thanks to the company providing the hardware. The hardware is not working that well, but F doesn't really care (story 191)*

> *The senior management are likely to pat themselves on the back and reward the success of the project, even though major data breaches occurred (story 180)*

Unsurprisingly, the experts did show much more positivity and optimism in their stories regarding the security adoption.

> *With the successful integration of the new hardware, cyber incidents within the organization fall, boosting employee confidence (story 10)*

> *The implementation was a resounding success (story 28)*

> *The organization learns from the experience, strengthens its cyber security infrastructure, and remains committed to safeguarding its data and systems from any future threats (story 83)*

> *Though the ransomware attack was a significant setback, the organization emerges stronger and more resilient from the experience (story 103)*

> *D's actions and collaboration with the team lead to a successful resolution, earning praise from the organisation's leadership (story 108)*

This includes viewing the IT and security teams in a much more positive light, than the non-experts.

> *[The IT team] work tirelessly to recover and restore affected systems using the organization's data backups (story 103)*

> *They work tirelessly to contain the leak, reinforce security measures, and notify any affected parties (story 108)*

> *The experts work together to identify the vulnerabilities that have caused this issue. They also take measures so that the issue is contained and the damage to their systems are reduced (story 122)*

2.3.4 Reputational Benefits and Risks

2.3.4.1 Non-experts

Whilst discussing cyber security technology adoption, there is often a discussion of the benefits referring to the positive outcomes of the adoption for the organisation. Participants also highlighted these potential benefits, and many imagined an improvement of the organisations' reputation. The majority of narratives which were coded for this theme were seen in response to SS1 (50%) where A and B were discussing whether to become first-adopters for a new cyber security technology.

> *[Organisation X] is seen as an innovative and trendsetting company and pioneers for this new wave. They gain a reputation as a trustworthy group and gain new customers and increase profits each year (story 18)*

> *Organisation X hits the press as a pioneer in adopting this technology (story 32)*

> *The company would be viewed as keen on cyber security, which would lead to more people working with them as they would view the company as trustworthy (story 44)*

It will be good for the organisation to be seen as being on the forefront of cyber security (story 46)

However, participants also imagined damage to the reputation would follow a potential data breach. This was shown as 25% of the narratives from this theme were a result of SS3, which describes a data breach. This was viewed as a negative consequence or outcome.

This has led to a breach which could have catastrophic consequences including… their reputation would drop (story 81)

The ransomware attack… is reported in the media making the company look bad (story 91)

It is likely that this data leak will damage the company's reputation and cause a downturn in business (story 128)

Z was liquidated shortly after and after the incident was pinned on her, D had to change her name in order to find gainful employment again (story 178)

2.3.4.2 Experts

Findings in this theme were very similar to that from the non-experts, however once again as seen in the previous themes, the experts were much more positive.

They are excited about the competitive advantage it could bring… Organization X's bold decision pays off, setting a new standard for cyber security (story 10)

The news of organization X's pioneering approach gained them global recognition, leading to a surge in interest from potential clients and partners (story 28)

Gaining a competitive advantage and bolstering its reputation for robust cyber security measures (story 50)

F's unwavering dedication pays off, securing organization W's data and reputation in the long run (story 187)

Organization W becomes a benchmark for other companies in their industry, admired for their forward-thinking approach to cyber security (story 209)

Nevertheless, there was still some discussion about the negative affect of a data leak such as that from SS3 could have on the organisations' reputation.

Assessing the impact from the data leak to analyse what potential damage has been caused to the company's business and reputation (story 143)

Isolate affected server, investigate data leak, inform ICO, try to limit reputation damage (story 148)

2.4 Discussion

The story completion method is emerging as a creative method to produce narratives rich with emotion and cognitions and is more recently being used in different contexts from its original publications in mental health (Vaughan et al., 2022; Lloyd et al., 2022) feminist psychology (Kitzinger & Powell., 1995) and digital privacy dilemmas (Watson & Lupton, 2022). It also appears to provide participants with a protected/safe research environment which provides them the opportunity to voice often undiscussed ethically sensitive areas related to cyber security. This study investigated the perceptions of both non-IT experts and IT experts on cyber security technology adoption within large organisations. Using the story completion method was highly successful in allowing participants to use their imagination and creativity to produce their narratives which yielded high-quality qualitative data. Thus, a strength of this method is that it's a creative tool to engage participants in a hypothetical scenarios to reveal cognitive processes of social experience and perspectives. Therefore, this report supports the use of this methodology within wider contexts to gain different insights into hard to access areas of organisational behaviour.

The report focused on four themes: accountability, emotion, cynicism/negativity, and reputation as a benefit and consequence. These themes correspond directly to Part 1 of this research project in which a rapid evidence review of the data on adoption of cyber security was conducted (Sanger et al., 2023). These themes will now be discussed in relation to the extant literature.

2.4.1 Accountability

This current study found a common theme within the narratives of allocating blame and accountability on characters in the story. Organisational blame has become of increasing interest within organisational psychology literature (Skarlicki et al 2017; Bhargava 2018; Lupton & Warren, 2018). A recent qualitative paper analysing 27 interviews with employees agreed with this instinctual reaction to "blame first and then think" (Lupton & Sharwar, 2021, p.15) with some participants believing someone needed to be blamed in order to "show that it matters" (Lupton & Sharwar, 2021, p.21). In addition, Qualitative research into cyber security also showcases individuals' focus on accountability, whether that be regarding personal data security (Dogruel & Joeckel, 2019; Haney et al., 2021) or the security of an organisation (Renaud et al., 2021). Thus, with something as serious as a data breach, it's logical that the narratives from this study would indicate who they believed was at fault.

Participants also found themselves attempting to put blame away from the actor within the story. This may be due to the participants identifying with the actors, and showed a natural instinct to shift blame from the self. Lupton and Sharwar's (2021) interviews identified that attributing blame onto others has a purpose to remove the responsibility from ourselves. Nevertheless, research indicates that human error results in a large proportion of data breaches (Dykstra, 2016; Kelly, 2017; Metalidou et al., 2014; Soltanmohammadi et al., 2013). Thus, organisations have placed responsibility put on the individual to protect themselves and their organisation of data breaches. This was even more essential due to the Covid-19 pandemic where the majority of employees were working from home. There does appear to be a push to deliver mandatory cyber-safety training to employees (Aldawood & Skinner, 2019), however, a report from Mimecast (2016) of 436 IT experts across the globe found that a quarter of companies did not implement cyber awareness training, and a quarter do so only once when employed. This is supported by a more recent paper by Burke (2020), findings that typically cyber-safety training is not routinely repeated after joining a company. Thus, a lot more is needed to be done to reduce human error within organisations. Organisations that actively promote compliance with their security policies see an overall increase in security (Tang & Zhang, 2016) and positive attitudes towards security policy (Parsons et al., 2014). Reports indicating the high rate of human error causing data breaches highlights how easy is it for an organisation to put the blame on one employee. Thus, it is logical as to why an individual would want to shift the blame off of themselves. Evidently, one could argue this still falls on the organisation's responsibility to ensure all employees receive the necessary training routinely. Nevertheless, this attitude could be what results in a negative organisational security culture, and in turn, cynical and negative attitudes of employees.

Despite the evidence that human error is to blame for a large majority of data breaches within organisations, employees fail to understand their role in cyber security. A review into cyber security landscape found that employees place too much trust in the IT security systems and thus feel less responsible for cyber security within their workplace (Benson et al., 2018). Again, this goes to show that employees do not feel that they are responsible and thus take cyber-safety less seriously than they arguably should. The narratives supported this by indicating that cyber-safety should only fall on the IT experts, not the employees. Thus, organisations need to do more to ensure they are highlighting the seriousness of cyber-safety. They should ensure this information is spread in a respectful and easy-to-understand manner to avoid any resentment or negative views of the IT experts. This could lead to a negative work culture and organsiational cynicism.

2.4.2 Emotion

Emotion makes up a fundamental part of our daily lives, including at work. People often suffer from work stress, the psychological and emotional response when a work environment does not match the worker's needs and capabilities (National Institute of Occupational Safety and Health, 1999). Thus it not surprising that the narratives produced in this paper clearly contained rich emotive expressions such as stress, fear, and panic. A case study of a global manufacturing company which experienced a cyber-attack produced interesting findings on the emotions resulting from a data breach (Stacey et al., 2021) which support the narratives found in this paper. Interviews with eight employees of different job roles found that the IT security team "oscillated between positive problem-focused coping and negative emotion-focused coping" (Stacey et al., 2021, p. 7). The non-IT staff reported feeling frustrated and annoyed by the security policy and stated that they did not understand the seriousness of not adhering to these policies. This in turn frustrated the IT staff, thus showing the negative cycle within the culture of organisational security. During the cyber-attack, the assistant IT security manager had to take the lead due to the manager's absence, this led to extreme feelings of stress, anxiety, and feeling overwhelmed. Nevertheless, senior management remained positive, and this led to the assistant IT manager's increase in self-efficacy and therefore result in more positive emotions. Thus, this indicates that the feelings of stress and panic that were reported in the narratives show a real-life and accurate response that IT individuals face during a data breach such as the case study described above. This does tell us that non-IT experts are aware of the stress and pressure that decision-makers are facing during these data breaches or when adopting cyber security. Nevertheless, the case study also shows that good communication and support, as well as remaining positive, can support the team and result in better affective outcomes. This could lead to the implementation of targeted wellbeing interventions for IT-experts.

Another emotion which was largely reported within the narratives was frustration. This has been found in other studies such as Gross et al. (2017) who found anger to be the dominant emotion following viewing a false news report of a severe cyber security incident. Thus, again, the reaction of anger and/or frustration is supported by previous research.

Both the experts and non-experts narratives were coded for emotion, however the experts showed less emotion within their narratives than the non-experts. Evidence has shown that individuals rely on their emotions when making decisions (Laborde et al., 2013; Panno et al., 2015; Slovic et al. 2002; Sunstein 2003). However, novelty can produce stronger emotions than familiar situations (Weierich et al., 2010), which may be why the experts showed less emotion in their narratives. The IT-experts are familiar with these scenarios having answered that they make security adoption decisions at least ‘Somewhat often’. Thus, they showed less emotion due to their familiarity with the scenarios. Alternatively, a key characteristic of naturalistic decision-making (NDM) is that experts rely on previous experience and rationality and instinct when making high-pressure decisions (Klein et al. 1991) such as following a potential data breach. Thus, the experts in this study may have used their rationality and instincts when writing their narratives compared to the non-experts who used the context and their emotions to guide their perceived response. Thus, this finding supports naturalistic decision-making theories, and supports our aim to determine the specific cognitive processes that are involved in expert decision-making in adopting cyber security.

2.4.3 Cynicism/ negativity

Investigating the organisational culture has long been an area of interest within organisational psychology. A positive organisational culture increases employee commitment and loyalty to the company (Martin et al., 2006). More specifically, a positive security culture has shown to promote employees to engage in and enforce cyber security practices (Parsons et al., 2015; Parsons et al., 2010; Renaud and Goucher, 2012). Nevertheless, there appears to be little research into whether workplaces have a negative or positive organisational security culture. This research found that many individuals hold negative and cynical ideologies regarding cyber security. As aforementioned above, this may be due to a lack of cyber security awareness and a nonchalant attitude towards cyber security (Ertan et al., 2019). Nevertheless, there is contradictory evidence into the relationship between awareness and culture as Chen et al., (2015) found that awareness contributed little to organisational security culture. This indicates that future research is necessary to establish this relationship further. Still, the evidence indicating that organisations need to increase cyber security awareness to encourage employees to actively uphold cyber security policies could have positive effects. Training and awareness are the next steps for many organisations to increase the overall attitudes and culture of security within their company.

Organisational cynicism has long been researched (Kanter and Mirvis, 1989; Reichers et al., 1997), however there is evidence that this has increased within the contemporary workplace (Arslan & Roudaki, 2019). Organisational cynicism refers to the negative attitudes of employees towards the organisation (Dean et al., 1998). Some scholars extend this definition and add that employees hold this opinion due to their belief that their employers lack honesty and are trying to ‘fool’ their employees (Nair & Kamalanabhan, 2010). The narratives produced from this study support the idea that employees often have a negative and cynical view of their senior management team, and the decision-makers involved in cyber security adoption. For example, story 161 in response to Story Stem 3 involves the disussion that the character D, the head of IT, would “*throw members of their* *team under the bus to protect their position*". This clearly shows organsiational cynicism and a clear distrust for the senior management team, the belief that they are dishonest with their employees and just out to make themselves look better. Organisational cynicism is linked to employee behaviour such as punctuality, work ethic and performance, job satisfaction, and intention to stay employed at the organisation (Dean et al., 1998; Sagie et al., 2002). This highlights the importance of senior management teams trying to reduce the organsiational cynicism surrounding cyber security, and encourage openness and clarity with their employees.

Reeves et al. (2021) model claims that employees may become cynical about cyber security due to fatigue. This can manifest from receiving confusing and complex advice regarding cyber security (advice-related source of fatigue) or the actions they must take to counter cyber security are equally complex and confusing (an action-related source of fatigue). This suggests again the idea that the organsiation themselves need to make cyber security policies easy to understand and implement by employees to encourage positive organsiational security culture and reduce organsiational cynicism.

2.4.4 Reputational Benefits and Risks

Reputation, being an intangible asset for companies, is seen to provide a competitive advantage (Gatzert, 2015; Gatzert & Schmit, 2016; Rindova & Fombrun, 1999) and make the company more attractive to stakeholders (Fombrun, 2012). Thus, it is understandable why many of the narratives in this paper focused on reputational benefits and risks when discussing adopting cyber security technologies or the result of data breaches. Self-report questionnaires and interviews with IT specialists support these findings that perceiving improved reputation as an expected benefit of adopting cyber security technologies is found for IT experts as well (Berlilana et al., 2021; Donalds & Barclay, 2022; Gangwar & Date, 2015; Herath et al., 2020). Furthermore, there is evidence that improved reputation was an actual benefit of adopting cyber security technologies, although this was at a lesser extent that expected (Berlilana et al., 2021; Donalds & Barclay, 2022). Thus, it is logical to factor reputational benefits and risks when considering cyber security technology adoption. Similarly, researchers have reported a loss of reputation as a perceived consequence of adopting cyber security technologies. Historically, AlAbdulkarim & Lukszo (2010) found that companies rated a damages to reputation as their number one concern when adopting cyber security technologies. This was a theme mentioned throughout the narratives following a data breach, however the given the reflections are also to an extent retrospective, further investigation of whether or not concerns about reputational damage prevail more than a decade later may be required. This also could have applications to the workplace with regards to using reputation as an incentive. For example, more recently, participants in the workplace report this factor to be significant as an incentive (both positive and negative) to facilitate cyber security technology adoption (Donalds & Barclay, 2022; Sivan-Sevilla, 2021).

2.4.5 Limitations and future work

On the one hand, using Prolific to recruit participants has some limitations; participants may only have been motivated to complete the story stems for financial gain. On the other hand, we were able to gain some insights into non-IT employees' opinions and attitudes towards cyber security adoption. Whilst we suggest that individuals who would be motivated and interested in our story stems would most likely be IT experts, it was still highly worthwhile to gain rich qualitative insights into the attitudes of individuals with little-to-no interest in cyber security.

In regard to future areas of research, this paper supports the use of the story completion method to determine perceptions and attitudes of the cyber security adoption process within the workplace. Thus, it would be interesting to analyse the narratives of IT experts and the security adoption decision-makers themselves in greater detail. The responses from both the non-IT individuals and the IT experts could then be compared to identify differences in decision-making cognitions between the two. Such work could be underpinned by theoretical considerations of naturalistic decision-making, which identifies how experts make decisions often under uncertainty.

2.5 Conclusion

Overall, the research completed here offers researchers a useful story stem methodology which provides cognitive insights into the challenges of cyber security adoption decision making in large organisations. We have much to learn from how experts and non-experts respond to challenging scenarios which may provide useful contextualisation to further explore decision making under uncertainty. We contend that a more detailed examination of risk, emotions, accountability, cynicism/negativity and a positive psychological approach to the design of cyber security interventions, policy and practice may effectively support behavioural and cognitive change.

3. Security adoption within Higher Education

This section provides a focus upon security adoption within education, specifically the Higher Education Environment as a background to a Cognitive Task Analysis (CTA), Critical Decision Making (CDM) study.

3.1 Background

Information security is a vital topic for the education sector as a whole as it “consistently falls within the top five sectors for the number of reported information security (IS) incidents.” (ICO 2018). Bongiovanni noted in 2019, in a well-conducted systematic literature review, that attacks in the sector were increasing. In the year preceding April 2023, GOV.UK (2023) found that UK educational institutions from primary schools to higher education were more likely than businesses to have identified cyber security breaches / attacks. This report also showed that higher education establishments (HEEs) were more vulnerable to attack than schools, more likely to experience a wider range of attacks and to be more severely affected. It found that 85% of the 52 HEEs surveyed (N = 44) had experienced attacks of the following types:

- Phishing (100%) (Ahmed & Al-Haddad, 2021, describe different types of this)
- Impersonation (86%)
- Virus, spyware, malware (64%)
- Unauthorised access by staff (43%)
- Any other breaches or attacks (43%)
- Denial of service attacks (30%)
- Unauthorised access by students (20%)
- Takeover of user accounts (16%)
- Unauthorised access by outsiders (16%)
- Ransomware (9%)
- Unauthorised listening to video conferences or IMs (7%)
- Hacking of bank accounts (7%)

Sixty percent stated that, as a consequence, they had experienced a serious outcome such as loss of money or data, or having their accounts used for illicit purposes. Fraud was a more likely outcome for HEEs than either schools or businesses. Other less severe harm was caused to many:

> "Three-quarters (75%) of higher education institutions say they were negatively impacted regardless of whether there was a material outcome or not. Most commonly, they report needing additional staff time to deal with the breach or attack, or to inform customers or stakeholders (70%) and new measures being needed to prevent or protect against future breaches or attacks (48%)." (GOV.UK, 2023)

These figures are similar to the preceding year (apart from a decline in unauthorised listening, which is posited as due to the return to in-person meetings/conferences). The frequency of attacks was also alarming, as fifty percent stated they experienced these weekly. GOV.UK (2023) also noted that HEEs were more likely to have to consider external and/or overseas threats due to their research partnerships.

Bongiovanni summarises why HEEs are an area at risk of cyber-attack:

> "Universities sit at one of the most crowded intersections of the digital economy: these open-by-design (Borgman, 2018; Chapman, 2019), decentralised, multi-stakeholder, transient platforms are traditionally associated with technology, research and innovation. Students, academics, staff and visitors regularly access universities' IT infrastructures to consume and produce data, in a multi-modal fashion: from personal mobile phones and smart-watches (bring-your-own-device…), through corporate laptops and tablets, to laboratory sensors and swipe access card systems, the data exchange among universities as organisations and their different categories of end-users is continuous... From an attacker's viewpoint, times when universities seemed not to own any attractive asset are long gone: from computational power (used, for example, to launch distributed-denial-of-service attacks or, more recently, to "mine" cryptocurrencies) through personal data (for example, students' social security numbers in the US), to intellectual property and some research data, universities are rapidly climbing hackers' interest lists (Roman, 2014)" (2019, p351)

In 2021-22 the higher education sector consisted of approximately 285 organisations (those who returned data to the Higher Education Statistics Agency). The sector benefitted from 2.2m UK students and 233,930 members of staff, 43% of which were academic staff (Higher education in numbers (universitiesuk.ac.uk) See also Higher Education Staff Statistics: UK, 2021/22 | HESA).

3.2 Existing literature

There is a strong literature on educational technologies and their adoption generally. For example, Granic (2022) reviewed technology adoption theories used to explain factors affecting successful adoptions. Her systematic literature review identified 47 studies from between 2003-21. Granic observed that most studies used the Technology Acceptance Model (TAM) and focused on e-learning, m-learning, Learning Management Systems (such as Blackboard or Moodle), and social media use. Most studies were of the higher education sector and a majority concentrated on students (however, this contrasts with Ifenthaler's 2020 study where it was stated that most models of adoption looked at school settings). Granic grouped factors affecting adoption into three categories (user, social and task & technology aspects) finding the following to be:

> "self-efficacy, subjective norm, (perceived) enjoyment, facilitating conditions, (computer) anxiety, system accessibility, and (technological) complexity were the most frequent predictive factors (i.e. antecedents) affecting educational technology adoption" (Granic, 2021, p9725)

It is plausible that such factors may also affect technology adoption in HE in terms of cyber security.

However, the latter area in relation to HEEs is less well researched with most articles published since 2014 (Bongiovanni, 2019). Bongiovanni's systematic literature review identified 40 relevant papers covering:

- risk management frameworks / standards used for information security management
- information security policies
- socio-technical, holistic studies (e.g., "IT security as the product of organisational negotiations; human factors" p353)
- technical solutions e.g., security threats, security controls
- cyber-behaviours e.g., understanding student cyber behaviour
- culture and awareness in the organisation
- governance

The largest body of papers concerned university-wide studies e.g., on the effectiveness of specific system adoptions, followed by papers on students and cyber security. The review concluded "major gaps exist in literature on information security management in HE" p355.

3.3 Attitudes to cyber security

GOV.UK (2023) found that staff in HEEs had varying attitudes towards information security. For example, all interviewees appreciated it when they found high level engagement at senior management (board) level:

> "They felt it gave cyber security a voice at a senior level, showed wider staff that cyber security was a priority, and helped to embed cyber security within broader risk management processes" (GOV.UK, 2023)

However, some stated that their boards lacked interest or adequate time for cyber security and needed to be prompted into action by government requirements. This highlights the importance of regulation, and suggests a sometimes-superficial engagement:

> "There were also several concerns raised in interviews about the superficiality of current board engagement in cyber security, where the policies and structures in place did not necessarily match actions. In some cases, interviewees felt their boards considered cyber risks to be below other major institutional risks… One higher education institution interviewee noted that their board had a manual for how to deal with major physical incidents like fires, floods, bomb threats and pandemics, but this did not cover cyber incidents. Another interviewee from a higher education institution described how the advice of their long-established cyber incident response team tended not to be acted on by the board." (GOV.UK, 2023)

(See also Pupion, 2010's discussion of HE reliance on crisis management to effect adoption) Shropshire et al., 2010, looked at the impact of negative and positive framing of messages on intention to adopt security technology among US university students. They found that negative framing was significantly more effective in leading to the uptake of detection technologies (here specifically an email filter) than preventative technologies (a biometric keyboard). Perceived ease of use and perceived usefulness were important influences on adoption, which Granic (2022) later also confirmed.

3.4 Cyber security activity in HEEs

Less than half of the HEEs had a specific cyber security strategy in place, which compared negatively with the business sector. However, generally the evidence was very positive. HEEs were more likely than businesses to have technical controls in place conforming to the requirements of the government-endorsed ‘Cyber Essentials’ scheme, e.g., firewalls, secure configurations, user access controls, malware protection and software patch management. They were more likely to seek out advice when needed and GOV.UK (2023) noted that the culture of HEEs facilitated security:

> “higher education institutions in particular highlighted a culture of sharing information and learning with each other, with networks like the JISC cyber security community group facilitating this sort of support and guidance. This sort of culture was less present in private sector businesses”

They were also more likely to take action to identify cyber security risks than business, including through “vulnerability audits and penetration testing, and…investing in threat intelligence”, although the latter was down from the previous year (GOV.UK, 2023). The sector had a good record on password management, monitoring user activity and using VPNs. There was more common usage of two-factor authentication than in schools. HEEs were also likely to have measures in place to address incidents, e.g., guidance on roles and responsibilities (92% of 44), guidance on external reporting (71%), and written guidance on who to notify of an incident (79%).

An area identified for more action in this sector was that of cyber security in relation to the full supply chain. Half of the HEEs surveyed had not taken action in this area other than reviewing immediate suppliers. Additional problems were caused by allowing access via devices not owned by the HEE, and there appeared to be a deterioration occurring in the following areas:

> “higher education institutions are now less likely than in 2022 to have separate Wi-Fi networks for staff and visitors (77%, vs. 92% in 2022) and to use ways other than the cloud to back up their data (73%, vs. 89% in 2022).” (GOV.UK 2023)

They were the least likely type of educational body to inform directors or the board of trustees of incidents or to inform a regulator. In terms of the National Cyber Security Centre’s ‘10 steps to Cyber Security’ guidance, HEEs were strong in most areas, only weaker as regards asset management (having a list of critical assets), vulnerability management (applying software updates within 14 days), and as noted, supply chain security (monitoring risks from this).

3.5 Specific security technologies

A wide range of specific security-related technologies have had some uptake in Western higher education. Examples include cloud computing, two-factor authentication, blockchain, antivirus and anti-malware software, RFID for laptop security (see e.g., Wyld 2010), and use of smart technologies to create a smart campus (see e.g., Zhang et al., 2020, Majeed & Ali 2018). Three will be touched on here: two-factor authentication (2FA), blockchain and cloud computing.

In 2018 Colnago et al., stated that adoption of 2FA remained generally low, with research attention chiefly focused on use in financial institutions. He looked at the partially mandatory adoption of 2FA in a university, specifically focusing on user views, decisions about adoption and behaviours as well as usage patterns. Results indicated that:

> "people who adopted 2FA at CMU found it annoying, but fairly easy to use, and believed it made their accounts more secure. A user's [previous] experience [of the system deployed] often led to positive perceptions of [it], which sometimes translated into 2FA adoption for other accounts. The likelihood that a user would subsequently adopt 2FA for other accounts was related to their opinions about 2FA ease-of-use and perceived value. While we found some evidence that people who were required to adopt 2FA had more negative perceptions than those who adopted voluntarily, the differences were smaller than expected" (p2)

Their recommendations included working through common use cases in advance of adoption to minimise unexpected outcomes, incremental deployment, making adoption mandatory and communicating well with users to dispel unfounded fears and negative assumptions. Gonzalez Arrieta et al. (2021) offered two methods for the adoption of two-factor authentication (2FA) in a university giving the pros and cons of each.

Alhumayzi et al. (2023) noted that despite having many potential applications in HEEs, blockchain uptake is low in the sector, perhaps as a result of insufficient attention to employee acceptance. Alshahrani et al. (2022) discussing blockchain's potential for better academic smart certification, noted that there was no existing guidance on this. They also explored attitudes and acceptance by potential users.

Ali et al., (2018) offered a systematic review of cloud computing adoption in HEEs, its benefits and challenges and factors affecting adoption. They found 20 papers showing a high level of successful adoption together with a high level of interest. A second paper (Ali, 2019) drawing on the same data noted specifically “a lack of cloud adoption studies in the HEI domain from multiple perspectives, particularly in relation to the wider socio-technical concerns related to cloud adoption” (p89)

3.6 Technology as disruption and transformation in HEEs

Finally, it is important to acknowledge that HEEs are undergoing digital transformations in every aspect from the automation of campuses to the ways in which education, teaching and research are carried out.

> “An emerging “threat” that is garnering increasing levels of concern is that of disruptive automation in the higher education sphere, not only in ancillary functions such as learning management systems, information processing and provision of student support services, but also going to the root of the academic function—the education experience. This development will have fundamental implications for higher education” (Wells, 2019, p21)

The cyber security challenges brought about by this are not yet fully known, but what is clear is that the need for attention to cyber security in the higher education sector is greater than ever.

4. Cognitive Task Analysis: The Critical Decision Method

4.1 Introduction

Digital vulnerabilities can pose significant corporate risks, such as interruptions to business and financial losses (Sheehan et al. 2019). Examples of these vulnerabilities are phishing attacks and ransomware attacks. Security technologies such as hardware can protect a company from data breaches by minimising risk and highlighting vulnerabilities. The number of cyber incidents has risen…thus indicating the need for further investigation to prevent attacks. The European Council announced in April 2021 that a centre of excellence for cyber security will be established to fund research and technology development to increase security and critical network and information systems (European Council, 2021). This further highlights the importance of cyber security as an area of research.

Despite the increasing need for a stronger understanding of cyber risks, the availability of such data is limited. A systematic review of cyber risks by Cremer et al. (2022) concluded that the lack of available data regarding cyber risk and prevention can lead to profound problems for organisations. This may be due to the fact that the cyber security and threat landscape is an evolving area, and thus data sources do not remain relevant for long (Biener et al., 2015). Similarly, cyber security and particularly data breaches within organisations are often kept secret and not disclosed (Eling & Schnell, 2016). Hence, there is limited real-life case studies to research and learn from; if these organisations were open about their mistakes and vulnerabilities, policies and practices could be developed in other organisations faster to avoid more data being lost or private data being released (Falco et al., 2019). More specifically, there is limited data on the effective adoption of security technologies.

One way to inform best cyber security practice is to investigate the adoption of new security technologies. These findings could directly impact organisations and be useful to key decision-makers and stakeholders. Our rapid evidence review (Part 1 of this Discribe funded research project) which systematically investigated current findings in this area, found that there is limited research which takes a holistic approach to investigate the adoption of security technologies (Sanger et al., 2023). Often the research focuses is on one type of hardware or one type of data breach. Organisations cannot predict what data breach will come up, and often use multiple hardware and software to protect their data. Thus, there is a clear gap in knowledge.

This study aims to investigate the decision-making process of adopting security technologies in large organisations. To do this, we draw on the Naturalistic Decision-Making (NDM) framework to collect information from cyber security experts on their own personal experiences with adopting cyber security. This report will discuss background research into the adoption of cyber security technology, provide details of the Critical Decision Making (CDM), cognitive task analysis methodology, and then finally discuss our qualitative data findings and their implications for real-world practice.

4.1.1 Cyber security background

The DSbD programme has been established in response to a significant market need for increased cyber security (Johnson, 2022). This need has arisen because of the increased risk posed by digital vulnerabilities within a connected digital ecosystem. The effective implementation and use of new cyber security will be dependent not only on the objective features of the technology but also on organisational actors' subjective interpretations of and interactions with it (Orlikowski, 1993). This is known as the duality of technology, where its objective features meet with subjective interpretations via ongoing interaction (Orlikowski, 1992). These interactions and actions taken by decision-makers and users can have intended and sometimes unintended effects and consequences that lead to non-adoption. Thus, understanding the adoption process requires understanding the role of actors when interpreting the technology within their organisational conditions, and how that security technology is re-designed and used in practice via actors' interactions with it. This has been a long-standing topic of interest within information systems and information management (Brous et al., 2020; Davis, 1989; Orlikowski, 1992). Nevertheless, there is little research into the cognitive decision-making processes of these actors involved in its initial development and adoption along with the users' interactions with and perceptions of it.

4.1.2 Naturalistic Decision Making

Naturalistic decision making (NDM) is the study of how decisions are made in complex real-world settings (Klein, 2018). These often include scenarios which are dynamic, uncertain, and continually changing in which urgent and high-pressure decisions are required in real time with significant consequences (Klein, 2018). Cognitive Task Analysis (CTA) was developed with in the NDM community to specifically investigate expertise and decision-making (Militello et al., 1997). Rather than identifying what decision was made, the CTA approach attempts to observe how and why that specific decision was made in that specific scenario. Understanding experts' mental models, ability to identify subtle cues, and strategies used to make decisions can provide valuable application to practitioners and their day-to-day work (Gore et al., 2018; 2015; Brown et al, 2023).

CTA methodology has been used in a variety of professional settings, for example healthcare (Clark, 2014; Militello et al., 2014), military (Phillips et al., 1998), and first-responders (Battaglia et al., 2002; Prasanna et al., 2009). Mahoney et al. (2010) conducted a CTA study within cyber security; however, this was to aid in the development of better security training within the workforce. As far as we are aware there is currently no other research which utilises CTA methodology to investigate the decision-making process of cyber security technology adoption in organisations. Thus, this report attempts to begin to bridge this gap.

4.1.3 Study aims

In this study, eight experts in cyber security were interviewed using the Critical Decision method (CDM), cognitive task analysis interview methodology. They each discussed a scenario in which they personally had to make a decision regarding adopting security technology/policy. The interview transcripts were then analysed using thematic analysis. The aims of this study are, to:

- understand the perceived benefits and risks of users of security technology.
- identify the organizational conditions and consequences of adopting new security technologies.
- determine the cognitive decision making processes which are utilised and shared by individuals involved in adoption discussions, policy or process.

4.2 Methodology

4.2.1 Participants

Once ethical approval was obtained, cyber security experts working in UK organisations were contacted to participate. These individuals were discovered through the DSbD network as well as by researching the information security teams of higher education institutions across the UK and contacting individuals' whose information could be found online. Snowball sampling then commenced from these first few participants. We aimed to recruit 8-10 participants who had recent experience of making decisions regarding adopting security within a large organisation.

We recruited eight participants for the study (25% female). Of these eight, participants 1 and 2 worked in Cyber security in large financial organisations, and the participants 3-8 worked in higher education institutions (HEI). Please see Table 1 for each participant's job title, and the number of years of experience making cyber security adoption decisions.

Table 1

Participants' job titles and years of experience making cyber security adoption decisions.

Participant	Job Title	Years of experience making cyber security adoption decisions
Participant 1	Director of Technical Risk Assessment	5 years
Participant 2	Cyber Risk Manager	5 years
Participant 3	Technical Director	12 years
Participant 4	Information Security Manager	20 years
Participant 5	Head of Information Security	24 years
Participant 6	Head of Information Security	5 years
Participant 7	Chief Information Security Officer	15 years
Participant 8	Director of Information Security	11 years

4.2.2 Materials and procedure

Eight participants were interviewed using the Critical Decision Method (CDM) a cognitive task analysis. See Table 2 a summary of the Interview Protocol, with the complete Interview Protocol being found in Appendix B. Developed within the Naturalistic Decision-Making community, this approach uses a narrative-based, semi-structured interviewing technique to elicit the decision-making processes that underpin expertise in complex work environments (Militello et al., 1997). During the interview, participants retrospectively discuss a cognitively demanding decision they had to make. By going through this scenario in depth, and probing to gather more information, we can uncover the cognitions which aided this decision. Interviews were completed by two or three of the research team via MS Teams. CTA and CDM interviews typically involve at least two interviewers to ensure sound observations and in-depth questioning of detailed tasks.

Using the existing recommendations for conducting CDM, the interview had four sweeps (Stanton et al, 2013) - see Appendix A for the full interview guide with examples of the probes used. In sweep one, the researchers work with the participant to identify an event relevant to our research aims, namely cognitively demanding decision when adopting cyber security within their workplace. We were interested in challenging cases as they are often easiest to recall and feature complex cognitions. The key requirement for a scenario/decision task was that the participant was the decision-maker themselves and had a direct effect on the outcome. Once a scenario/decision task has been agreed upon by the participant and researchers, the participant is asked to provide a narrative of the decision from start to finish. The researchers refrained from interrupting but did gently probe if the participant drifted off topic. During this time, the researcher is attempting to draw a timeline of the experience, this leads to sweep two: timeline verification. This sweep involves the researcher retelling the incident to the participant and the expert is encouraged to establish any errors or add extra details. Any ‘critical turning points’ are identified and circled within the timeline.

Table 2

Protocol for Critical Decision Method interview, adapted from Stanton et al (2013)

Interview Sweep	**Probe Examples**
Sweep 1: Incident Identification	Think about the security adoption decisions that you have made. Tell me about a time that really stands out as a challenging case. It may have been challenging because of how the decision was presented to you or your team or due to a particular individual or tech challenge
Sweep 2: Timeline Verification	Can you provide a 2-minute overview of the decision? How many minutes/hours/days from being asked to adopt the security measure to implementing it, did this take? Were there any challenging points in the early management of the process? Did any decisions alter your train of thought?
Sweep 3: Deepening	Where were you when you learned of need for the security measure? What were you doing? Where were your team? What was the time of year/time of day? What was your role at the time? Who told you about security requirement? What information did you initially have? What more did you want to know? Was the history/info reliable? Was anything confusing/ contradictory? Who else was taking care of the security adoption decision? What were their impressions? Did you seek advice/input from others? Describe the operational requirements needed to complete your task.
Sweep 4: ‘What if?’ Queries	Describe your differential. Why were you considering different options? Did your prior experience with security influence how you completed the task? How did this experience change how you think about security adoption? What would you have done differently? What if the requirement had been seen by a provider at a different level of the organisation/internal/external? Did your team challenge your understanding of the security adoption measure? What were the learning points that you took away from this experience? How comfortable do you feel in managing security adoption decisions?

Once the timeline has been verified, sweep three commences. Here, the researchers will focus attention onto the critical points highlighted during timeline verification and ask the expert to talk through it again whilst using cognitive probes to gain further details. These cognitive probes are developed with the research questions in mind some examples are: “Who else was taking care of the security adoption decision and what were their impressions?”, “Describe the operational requirements needed to complete this task.”. Not all probes were used in every interview, the researcher has the freedom to decide which probes are appropriate and also to create additional ones guided by their curiosity at the time of the interview (Crandall, et al., 2006). The fourth and final sweep contains ‘what if?’ probes. This is to shift the expert’s focus away from the incident and orient them towards hypothetical scenarios to develop a more analytical perspective from the expert (Crandall et al., 2006). Each interview took around 1 hour in total and were conducted remotely via Microsoft Teams. Verbal consent was granted from the participants to record and transcribe the interview.

4.2.2 Data analysis

Interviews were recorded and transcribed via Microsoft Teams and analysed using thematic analysis using the six-phase approach (Clarke & Braun, 2015). The interviews were initially read by the first coder through once whilst listening to the recording to ensure the transcription was accurate and to become familiar with the data. The first coder then read the transcripts again to draw initial codes and then group these codes into themes. Five themes were identified, which were defined with the research team. These themes are discussed below.

4.3 Results and Discussion

During the eight interviews, we discussed various security applications, please see Table 3 for a list of which security adoption implementations were discussed in each interview. Qualitative analysis drew out a number of interesting codes and themes including: Organisation structure, benefits of security adoption, mitigating risks, culture change. However, in this report, we will focus on the five themes: executive function, socio-technological skills, adaptive cognition, hierarchical factors, and negative bias. Throughout this section, we discuss these themes in more detail.

4.3.1 Executive Function

To answer our research questions ‘What cognitive decision-making processes are utilised and shared by individuals involved in adoption discussions, policy or process?’ and ‘How do decision-makers and users make sense of the security adoption process? What models of the process, its components, and relationships are implicit in these stories?’, we coded for decision-making cognitions. Decision-making can be conceptualised as a goal-directed cognitive process (Colautti et al., 2022). Several studies found that decision-making processes – particularly in risky and high-pressured situations – may be related to executive functions (EF; Brand et al., 2006; Del Missier et al., 2010; Skagerlund et al., 2021; Toplak et al., 2010). Thus, we define this theme as: exhibitions of decision-making cognitive processes.

4.3.1.1 Fear and stress/worry

Some of the experts did discuss how decision and implementation, if went wrong, could have significantly negative effects on the organisation as a whole. For example, P8 mentioned,

> *“Because this was a project that had a drop-dead date and we ended up running out of time. We ended up agreeing that we would go as we have to keep/kept pushing the end date to the last possible moment, which is what also brought in a quite a lot of stress and pressure… There was a dawning realisation across quite a large swathe of the university that this was really big, really scary and if it went wrong cause they would have to go back to paper for quite a significant period.”*

Furthermore, P3 discussed the urgency of the situation they identified,

> *“It was a broad part of a broader threat… in previous examples where the NCA had been in contact, they have seen activity off the back of it. So it wasn't, you might have a problem if you don't do anything, it's, people who have had this happen to them definitely had problems going forward. So it made it a much more pressing and concrete threat as opposed to a hypothetical.”*

Thus, the scenarios the experts discussed clearly involved an element of urgency and criticality within the decision-making process.

Table 3

The security adoption discussed by each of the participants during all eight interviews.

Participant	Security Adoption	Description
P1	Multi-Factor Authentication	Adding an extra step to the sign-in process (i.e., authenticating the sign up via a text/phone call or an app)
P2	Secure Browser	Acts as a barrier between the user and the website such that they cannot click on any links or download any files. This assumes everything on the internet is dangerous. Once a malware check is completed, then they can use the website.
P3	Multi-Factor Authentication	Adding an extra step to the sign-in process (i.e., authenticating the sign up via a text/phone call or an app)
P4	Multi-Factor Authentication	Adding an extra step to the sign-in process (i.e., authenticating the sign up via a text/phone call or an app)
P5	Compliance Training Service	A compliance/ training scheme. Monthly training courses to complete as well as phishing simulations such that users are sent fake phishing emails, if they click the link they are sent to an internet page designed by the provider where they are informed that they would have downloaded malware onto their computer if the phishing email was real, and they are given extra training to complete.
P6	24/hour security protection	They decided to buy two services: a well-respected company to provide high-scale protection to a small aspect of their internal systems (the most important data), and a small business to virtually triage incoming cyber events which are raised to the internal team to deal with if deemed necessary.
P7	Policy change	New scheme whereby staff remove their university accounts from external and personal websites (i.e., social media, life insurance, online shopping). This was under the knowledge that more external emails would lead to an increased likelihood of staff members to click on a phishing link.
P8	Uploading all student data from on-site to on the cloud	Uploading student data to the cloud.

4.3.1.2 Competing priorities

Notably, throughout the interviews, experts discussed having to deal with competing priorities. For example, P1 mentioned,

> *"It's competing priorities. Whether that be from sheer volume of work because of the regulatory commitments that are needed around change… the potential that you're gonna have to postpone some client agreed change to take time out to implement this... you have to look at is this a particular priority? Is that a legal or regulatory requirement? Because that's going to come first."*

Furthermore, when asked how they decide where to begin with the process P3 clearly displayed that there were multiple tasks with competing priorities, stating,

> *"We needed to do stuff in parallel… At the time we had these priority groups that we needed to make work… [migrating VPN across to MFA] was tested within the IT team over the weekend to ensure could do all their work remotely… we got assurance that it was stable to the level needed, then bringing finance people on at that stage so they could do their work… initially it would only be available to staff. So that we could make sure it could cope with the load"*

4.2.1.3 Analysis

The experts discussed having to decide between multiple options, and they reported analysing the information to support their decision-making. P8 discussed having to decide between two different approaches, and assessing what each approach could mean for the organisation,

> *"We had two options essentially to migrate it into the cloud or to rebuild it on premises. We did a proof of concept and a kind of an assessment about whether on premises would have been easier, cheaper but would give us no platform or off which to pivot for the future. So, that was my first big decision, I had a paper put in front of me and I made the decision to go to the cloud."*

Furthermore, when deciding on a technology to adopt, P5 discussed doing a market survey,

> *"There was discussion around what exactly we wanted out of it… The three companies were all providing slightly different products, but they were broadly the same sort of thing. So I had to pick out the bits that I thought were important and one was the ease of making the changes to the content."*

P6 also had to go through a similar process of analysis to decide what technology to adopt,

> *"[you] start talking to the suppliers and immediately there their eyes light up in terms of how much we should be investing in their tooling… That changed the scope of the project to that point, cause at that point we're not looking for if we were to go down the route that they*

> *were suggesting rather than just looking for [what we wanted]. It's looking at the whole toolset and we didn't have budget for that, we had no appetite for that, and it isn't what we had originally envisaged as the scope." … "[The] internal stress was getting all of that aligned in my head in terms of what are they offering and how does that align to what we want to do"*

Thus, there is a clear element of analysis and information gathering. However, this is not always possible in every situation. P3 had very little information to analyse, so had to go with the safest choice with the least amount of acceptable risk,

> *"We knew that our credentials have been released, but we didn't know how the attacker had got hold of them. If it had been through a phishing attack, that might be a one off and changing passwords might be enough to defeat them short term. But equally it could be a remote access trojan…if [a student's] laptop was infected, even if they changed their password, the attackers would get hold of it again and we wouldn't be in in a bit of face off. So, there were considerations made on the business impact around this" … "So that that amount known, you have to go to a place where you could have some sort of assurance, and multi factor authentication was seen as that solution"*

Furthermore, P5 indicated that they used their own previous experience with different technologies to aid their decision,

> *"It was the good experience with (the training provider) and the fact that we've got in some departments in my previous place 100% completion."*

This indicates that they may have subconsciously already made their decision with which technology to adopt before the market survey began.

4.3.2 Socio-technological skills

Often, there is a socio-technical gap seen in organisations, which is the misalignment between social and technical factors (Whitworth & de Moor, 2009). Malatji et al. (2019) discuss the importance of reducing this gap within cyber security systems, to do this they developed the socio-technical systems theory. This theory highlights the importance of using an approach to optimise the alignment between social and technical dimensions of a system (Malatji et al., 2019). Thus, socio-technical systems take into account complex social and technical systems to meet the needs of society (Baxter & Sommerville, 2011). To do this, one must take a holistic approach to integrate both social and technical systems (Whitworth & de Moor, 2009) and harness the best possible practices for both systems (Carayon et al., 2015; Walker et al., 2007).

This approach is even more necessary within cyber security since the majority of cyber-attacks are caused by human error, but the hardware in place can often reduce the impact of these attacks. Thus, taking a holistic approach to ensure both factors are using the best approach could promote better cyber security practice. Within the interviews, the experts discussed the importance of considering the social aspects of security adoption when making decisions. Thus, this for this paper, this theme is defined as discussions on the importance of social skills and relying less on the technological explanations to get people on board.

4.3.2.1 Experience

Not taking a holistic approach and considering the importance of the social factors appears to be one experience which the experts regret. In one case, P1 discussed how they wish they had considered the social factors earlier in their process,

> *"[I] should have been better in communicating to key stakeholders that this was coming along rather than, 'this is really important, you're gonna do it… To be fair, maybe we hadn't explained it properly in the first place, the, the, benefits… Did we just assume people would know what we are talking about?"*

This idea is supported further by P3,

> *"[we] needed to warm up the audience more because they didn't have that familiarity and doing that, I don't want to say wasted time, because it was necessary at the time, but to have we done more to warm up the keep them aware in advance of some of these things."*

These interviews demonstrate not taking on that holistic socio-technological approach can lead to more problems and difficulties during the launch.

Further, both P1 and P3 discussed that this was something they learned throughout their career and with their experience, and that their younger self would make the mistake of not considering the social factors. P1 stated,

> *"Someone taking over my role tomorrow, the thing they'd find most challenging is the size and complexity of our organisation. Because I've built up a big network… and I understand how everything works and ticks… I know most of the key people… a lot of it's all up in my head about who's the best person to ask for."*

Furthermore, P3 confirmed this by saying,

> *"if I was doing it early in my career, I'd come from a much more technology-based want. The human impact of the decisions I was making didn't really come into my considerations at that stage."*

Thus, they are aware that considering the social factors is something they are continuingly challenging within their work, and are trying to not keep making the same mistakes. This was supported further by P7 who said,

> *"I think one of the things for me is we often call them soft skills or whether it's human skills… computers are easy to do what you tell them… Dealing with organisations dealing with groups of people that, that's the really tricky stuff. That's where you really earn your money. So if I was talking to someone who was new to security, I'd probably be saying don't worry too much about the technology. Go and develop your people's skills and I don't just mean in terms of selling stuff, but actually your own confidence… having that confidence to make difficult decisions to say the things that needed to be said to the people that needed to hear it."*

Thus, these interviews clearly display that a characteristic of cyber security expertise is having those social skills and taking on that holistic approach to also consider the social factors.

4.3.2.2 Communication and Persuasion

One social factor the experts discussed in depth was communicating and persuading people that this new security adoption was necessary. P7 discussed "socialising the change ahead of actually pressing the button and launching it to all staff" in length. One way he did this was through persuasion,

> *"How we articulated it, it was very much about setting out the story, doing it with the cold hard facts, backed up with that bit of narrative" … "Trying to persuade our data protection Officer, nice and straight forward, we used rules, regulations. Trying to persuade our Chief Financial Officer, it was about risk, it was about stats, it was about numbers. Trying to persuade some of the academic faculty, executive boards… we did use some of the more personal, funnier, silly stories where appropriate. One of the messages that we've used with all staff and it is one that we do believe is that this is actually better for staff because it adds a separation between work and between their personal lives."*

Thus, during the planning stage, the team not only began discussing the technology and policy changes, but also set up a plan for how to socialise this change to different individuals. This clearly shows that they take the social factors of these security adoption seriously, and put time and effort into preparing their staff/users.

Furthermore, P4 discussed that the most cognitively demanding aspect was communicating the change,

> *"It was all about persuading people that we needed to do it… how we're going to communicate this occupied a significant amount of the time during that that whole period … easily 60 or 70% of our cognitive load in in in these kind of projects goes to how to communicate to the customer."*

This idea was seen also from P2 when asked what the most cognitively challenging aspect of the adoption process is

> *"it's convincing other people… you can request something an idea and then to have to to other people to understand that idea… or to get to like a whole business structure on board especially something that is so wide it is quite difficult I guess a lot of time to actually explain why what you want and the reasons why you want that."*

Thus, taking on the social factors, although it is important, it appears to be the most challenging and cognitively demanding aspect of the process. This may be because, as seen by P1 and P3, this can often be something that they do not do well, and can cause more issues in the long-run.

Lastly, within this theme there was also a discussion around building relationships with individuals in order to support the implementation of security. P7 mentioned,

> *"Lots of playing on my own relationships with other members of senior management and various other bits and pieces" … "It is very much about relationships at my institution, if you want to get stuff done."*

Furthermore, P4 discussed using these relationships as a way to influence and persuade others,

> *"Who was the actually the most influential, influential person in each of the business units? Be the the person who, if you persuaded them that this was the right thing to do, would have the biggest. Carry the biggest weight in making that change."*

Thus, these experts also highlighted the importance of building a network of individuals in order to know who to approach and persuade first about potential changes, to allow them to persuade and convince others. Here, it is clear there is a tactical and calculated approach to getting staff on board.

4.3.3 Adaptive cognition

Naturalistic decision making (NDM) researchers recognise their focus on macrocognition, as they investigate expert actual cognitive processes, as opposed to anticipated, imagined or false scenarios created in a laboratory (Militello et al., 2017). Macrocognition is defined as adoption of cognition to complexity (Schraagen et al., 2017), and thus by extension, one could define expertise as cognitive adaption to complexity through their skills and knowledge. This is necessary as the work environment is difficult to predict due to its complex and ever-changing characteristics. This is even more true in the world of cyber security where the threat landscape and technological advances are constantly changing and adapting (Rahman et al., 2023). Thus, not only should experts process the skills and knowledge of procedural and routine aspects of their work, but also to be adaptive and flexible when dealing with unexpected and/or novel situations (Militello et al., 2017; Ward et al., 2018). Similarly, being able to metacognitively resolve goal-conflict, is necessary to ensure the desired goal and outcome is achieved (Gunn & Taylor, 2021). Thus, this theme is defined as showing flexibility and adaptability when dealing with unexpected/novel conflicts/situations during the security adoption process.

During the interviews, cyber security experts discussed adaptivity and flexibility when making these difficult security adoption decisions. Some showed their ability to adapt and be flexible, and others reflected on the fact that they lacked adaptability and should have been more flexible during the process. One way the experts displayed adaptability was discussing using a phase approach to the implementation, to allow for changes and adaptations. P2 used this approach,

> *"We had a two- or three-month period where we have like an two step phase… If there was actually a problem we could try to go to the project team and say 'can you fix this?', 'can you fix that?' That's reason we have that two-step period…They start trying [the new browser] and if something was not working, obviously the project team will work on that."*

Thus, slowly implementing the change allows for problems to come up which can be solved before the final launch, after which changes are more difficult. This approach also allows for the team to listen to the concerns and worries from the staff/users and adapt their approach to allow the least amount of interruption to individuals' work.

Furthermore, P7 showed adaptive cognition when receiving feedback in the early stages of the implementation process,

> *"We had a few 'ohh heck' moments we hadn't thought of when composing the FAQs, but that was really good because we got those relatively early in the process, so we could adapt as we*

> *went along. One of the things that we have adapted is it's not a binary thing, it's not work vs personal. There's a spectrum. So for things like your academia.edu profile, the research gave very little bits and pieces. You will have a work and a personal profile that overlaps. If you're a career academic, you will have a professional profile that you need to maintain, and you might use your ac.uk account to do that. And we recognise that same for staff and student discounts, we're quite happy with that."*

Hence, we can see how P7 was able to use the feedback from users to adapt their approach to the scheme to encourage further engagement with the new policy.

Furthermore, experts discussed remaining flexible for particular groups of individuals during the process. For example, P3 mentioned that,

> *"There were a certain set of students who were doing exams. That week and they were given two days extra to reset their passwords so it didn't interrupt with their exams… to allow them to finish their coursework."*

P4 confirmed the need to be flexible with the users by saying,

> *"We have a lot of international students, people are in other countries, people travel a lot. What happens when we switch it on if they haven't read the emails, haven't got the communications? How disruptive that will be for the people who haven't looked at the comms and stuff like that."*

Here, it is clear that during the development portion of the adoption process, it is vital to consider particular groups of users and remain flexible with the adoption process for them.

Moreover, it is important to not only be adaptive to users/ staff, but also to remain adaptive with security for the current and everchanging threat landscape. This is shown by P6 who discussed sometimes the need to move away from certain security services if they are no longer meeting the organisations' needs,

> *"We're not gonna continue onto into the third year with the small business that provided us with that virtual support… we've moved on, the threat landscape has moved on, and our technology landscapes moved on. And actually the smaller supplier hasn't moved at the pace that I'd have expected or wanted them to."*

Here, it is clear that adaptive cognition is necessary within the world of security as new threats are present all the time as technology advances. Thus, it is important to ensure the organisations' security is providing the best level of protection as these changes occur.

4.3.4 Negativity Bias

This theme follows on from cyber security experts exhibiting adaptive cognition, as the interviews displayed their tendency to show negativity bias. In this context, we define negativity bias as the tendency to expect and focus on negative aspects or outcomes.

Most of the experts highlighted that they often get negative responses and reactions from users/staff. As P2 mentioned, this may be because

> *"there's a lot of people that don't like change."*

This was repeated by P4 who said,

> *"We were having lots of conversations with the key business units, the stakeholders and at points, you're kind of you run up against a brick wall, which is we just don't want change… this idea that better security is better conceptually, but we just don't want any change for us."*

This may explain the negative responses of people when they are made aware of potential security implementation. P1 said,

> *"you sometimes get the resistance well. Why? What? What, why? Why do we need to do this and the way?" … "It was almost that gut reaction of 'But we don't need to do this work.'"*

Thus, the decision-makers made it clear that negative feedback was received often by them and their team due to the lack of flexibility and understanding from their users/staff.

Having this understanding means the experts often have to mitigate for and expect these negative responses from the users/staff. This takes place in the planning element of the decision-making process. For example, P7 highlighted that,

> *"I wasn't particularly looking forward to the trade unions meeting and was effectively in the staff meeting, waiting for the riots. But again, we put a lot of time into the argument, we checked it amongst ourselves and socialised it before."*

This shows how they anticipate the negative response and so do all they can to support and warm-up their users before launching the technology/policy change. P7 also discussed the success they had during the launch, and he was convinced this was due to them preparing the users and staff,

> *"the other sleepless night was when we did the all-staff e-mail and actually properly announced it… people were interacting with it and we put so much effort into our FAQs and*

> *the arguments we'd made and all the rest of it. People were able to get the why we were doing it… So it it kind of landed with a bit of a whimper."*

Thus, this decision-maker used their experience and expertise to predict a negative response from staff, and so prepared their FAQs and arguments before launching to limit these.

The reason these experts showed this negativity bias when discussing the response of the users/staff may be because that is often the only feedback they get. When asked what feedback they were getting following the implementation, P2 stated,

> *"most of them problems, because obviously people don't don't don't like change… So it's only problems. So they never come under around and say 'ohh very good this solution'. No, no. So always the feedback, any feedback are you getting is always wrong, it's always bad… If they don't say anything, that means it's good."*

Thus, they expect only negativity because that is what they are accustomed to receiving. Positive feedback is only assumed when individuals do not say anything negative.

4.3.5 Hierarchical Factors

Lastly, many of the experts discussed the importance of understanding the organisation structure; and this included being aware of the hierarchy. There were discussions around getting senior management approval, and the affect this can have on persuading other members in the organisation. Thus, this theme of 'Hierarchical Factors' includes discussion around how adopting is handled depending on senior approval/attention, and the ways this can be granted.

As discussed previously, decision-makers use different approaches to get different teams on board, and one of those teams is using support from the senior team. P2 discussed the method he used and why it is important,

> *"we try to rephrase it that way [discussing the affect of implementing on metrics and bonuses] so we get more attention especially on the senior side because they are the ones who, if you get on board, it's much easier to get the budget approved for the project."…"if more senior colleagues are on board with that, people are assuming that things are good for the business."*

This idea is supported further from P3,

> *"thanks to the backing of the Vice Chancellor… that was the key… He's called the actions that. Yeah, very persuasive. Not least on the staff side, I mean the students."*

Lastly, P7 also highlighted using relationships you have with the senior team in order to support your project and get people on board,

> *"It is very much about relationships at my institution, if you want to get stuff done… If the Chief operating officer of the Chief Financial Officer of the University Secretaries, who also a senior information risk owner and a couple of the vice presidents, have researched or interested in it, you're probably gonna get a pretty good outcome."*

Thus, as clearly established, when deciding how to go through the adoption process within cyber security, it is important to be aware of how you can get people on your side. A part of this, is to be aware of the affect the senior team can have on the whole process, and attempt to use that to your advantage.

Furthermore, it was discussed that if the senior management was for the implementation, it could happen regardless of the rest of the organisation. For example, P4 mentioned

> *"[The Dean] came back full of 'ohh, you know, bad stuff can happen. What can we do about it? This MFA thing, when can we roll that out?' and we went 'well we can switch it on, we can switch it on this afternoon if you want.' And then it was okay, we'll go ahead and do it."*

Thus, although previously, it has been discussed that often new policies or security measures are more effective when there is buy-in and backing from the users themselves, this is not always necessary. If the senior people agree to the change, it will be implemented. This is further supported by P2's statement,

> *"But there's sometimes not even a point in [explaining to people why this would be good for the organisation]. It's just a waste of time. Just try to tell them that, well, your boss has said this, and we have, we have all agreed to do this. It is what it is, sorry."*

This shows how having the support from senior management can change how the implementation is dealt with, thus indicating that it may be the first step when deciding whether to adopt.

Lastly, two of the experts discussed how talking to senior managers and anyone with authority can be difficult. Firstly, P6 discussed feeling nervous and apprehensive report problems to their senior managers,

> *"I was then thinking about how to articulate that to our stakeholders, to the IT director, and the CISO. So reporting back to them in a way that is our is is concise and not just seeming like I'm coming with excuses. And so it was that internal processing of of all of that information in*

> *a way that I could then present to them in a way that didn't just seem like I was trying to get out of doing any work."*

Clearly P6 shows a desire to show their capability to do their job, including approaching issues and problems in a constructive way.

Furthermore, both P6 and P7 discussed finding the confidence to talk to people in authority challenging. P6 said,

> *"talking to people in positions of authority can become a bit, you know, could make come across as being a bit challenging was… you know, logistically, but also, you know, for from one's confidence and understanding, you know, talking to people at that level, that level of detail, but also that level of seniority and influence, etcetera. So yeah, I think that was that was a challenge. It was, it was the the talking to those people about what their opinions were without being completely just shoved out the door as being someone who was just bothering them when actually had a real need to talk to them about what their strategy was."*

Here, it is clear that there is definitely an element of hierarchy within the organisation structure that the decision-makers are aware of. This also introduces an interesting element of anxiety and worry that comes along with seeking approval and advice from senior management.

We are even able to see from the senior managers that we interviewed that they struggle with the hierarchical elements of the job, often feeling as though they are less senior than they actually are. For example, P7, the Chief Information Security Officer said,

> *"And I have had some coaching in terms of getting ready for a more senior position cause I do have that mindset that I just drive vans part time for the IT department and I'm still quite junior role. Whereas actually that's not the case if you've achieved information security officer."*

This reiterates that actually, even once you are one of the senior managers within the department, there can still be that issue with confidence and anxiety.

4.4 Conclusion

This study used a Critical Decision Method (CDM), cognitive task interview methodology to investigate the cognitive processes of cyber security experts when making security adoption decisions. Through qualitative analysis, five main themes were identified: use of executive function, socio-technological skills, adaptive cognition, hierarchical factors and negative bias. These themes identified key cognitive processes involved in decision-making within the cyber security context. Further, it does indicate that there is an element of expertise within this field, similar to that seen in other skilled professions (Lintern et al, 2018). These cyber security experts are able to think ahead to prepare to future problems/conflicts and see the bigger picture in their work when making adoption decisions.

The CDM methodology is useful as it provides the opportunity to understand how experts make key decisions and use their cognitive skills to handle fast-paced, high-pressured, challenging situations (Klein, 2001). This can have remarkable application to real-world training and interventions in the work-place, including removing barriers to build the cognitive skills to improve practitioners' performance (Klein, 2001). Thus, the findings in this paper could result in the development of scenario training for early-career cyber security individuals to develop their cognitive processes required to make judgements and decisions within their role. This means that individuals in this career can start thinking like experts, without the years of experience and multitude of mistakes it took for the experts to get to that point.

Limitations and future directions

Whilst this study involves a relatively small sample of experts, Crandall et al (2006) report that no more than 8-10 experts are usually needed for CTA interviews. Thus, having interviewed eight experts indicates that our sample is within the optimal range.   Ideally we also would have preferred to complete these in-depth interviews face to face and would have liked to spent more time with the interviewees to access their cognitive challenges.   Whilst online interviews can be an effective use of time for participants building a rapport to draw timelines of challenging decisions can be limited. We suggest that further research to explore this complex cognition should be face to face where depth of questioning and probing participants may be increased. Cognitive task methods have much to offer security research as they explore and examine 'work as is' rather than 'work as it maybe imagined'. We hope that the Discribe community will continue to unpack and examine the complex cognitive decision making processes of professionals working in security technology adoption, in an effort to communicate and collaborate utilising a multidisciplinary analysis of this evolving ecosystem.

5. Appendix A – Story Completion Information Sheet and Questionnaire

The Elicitation of Cyber Security Narratives

Participant information sheet

General Information

The aim of this study is to understand the process of security technology adoption. We appreciate your interest in participating in this study. You have been invited to participate as you have been identified by your organisation as someone who may find this area of decision making of interest. Please read through this information before agreeing to participate (if you wish to). The Principal Researcher is Professor Julie Gore (j.gore@bbk.ac.uk) who is attached to the Department of Organizational Psychology at Birkbeck College, University of London. The project is being completed in collaboration with the University of Sheffield and funded by the government's ESRC hub - Discribe: https://www.discribehub.org

Do I have to take part?

No. Please note that participation is voluntary. If you do decide to take part, you may withdraw at any point for any reason by leaving the online session.

How will my data be used?

We will take all reasonable measures to ensure that data remain confidential. The responses you provide will be stored in a password-protected electronic file on Birkbeck, University of London secure server and may be used in academic publications and conference presentations. Any identifiable information will be deleted as soon as it no longer required for the research. Research data will be stored for 5 years after publication or public release of the work of the research. For information about Birkbeck's data protection policy please visit: http://www.bbk.ac.uk/about-us/policies/privacy#9

Who will have access to my data?

The small research team led by Prof. Julie Gore will have access to the data at Birkbeck & The University of Sheffield. We would also like your permission to use the data in future studies, and to share data with other researchers (e.g. in online databases). Data will be de-identified before it is shared with other researchers or results are made public.

Who has reviewed this study?

This project has been reviewed by, and received ethics clearance from Birkbeck, University of London's Research Ethics Committee.

What are the procedures of taking part?

If you decide to take part, you will be asked to complete the online questionnaire on the subsequent pages, and then invited to a follow-up online interview. The questionnaire will present you with 'story stems', which are short introductions to stories related to security adoption, and you will be asked to complete the stories by typing your response into the text boxes. This should take about 20-30 minutes. No background knowledge is required. The data you provide will help us to understand the every day work processes and thinking around security adoption. We are interested in a range of stories different people tell – there is no right or wrong way to complete the stories.

What are my participation rights?

Participation in this research guarantees the right to withdraw, to ask questions about how your data will be handled and about the study itself, the right to confidentially and anonymity (unless otherwise agreed), the right to refuse to answer questions and to be given access to a summary of the findings (if requested).

What if I want to withdraw my information?

If you wish to withdraw responses or any personal data gathered during the study you may do this without any consequences.

Any further questions?

If you have any questions or require more information about this study before, during, or after your participation, please contact Professor Julie Gore at j.gore@bbk.ac.uk.

For information about Birkbeck's data protection policy please visit: http://www.bbk.ac.uk/about-us/policies/privacy#9. If you have concerns about this study, please contact the School's Ethics Officer at: BEI-ethics@bbk.ac.uk. School Ethics Officer School of Business, Economics and Informatics Birkbeck, University of London London WC1E 7HX. You also have the right to submit a complaint to the Information Commissioner's Office https://ico.org.uk/

Thank you for your consideration,

Prof. Julie Gore, Principal Investigator j.gore@bbk.ac.uk
Dr David Gamblin, Co-investigator d.gamblin@bbk.ac.uk
Ms Billie Dale, Research Assistant billie.dale@bbk.ac.uk

Department of Organizational Psychology, Birkbeck, University of London,
Clore Management Building, Malet Street, Bloomsbury, London. WC1E 7HX

Consent Informed Consent

Please read the following items and tick the appropriate box below to indicate whether you agree to take part in this study.

1. I have read the information above in full and I understand the purpose of this research.
2. Any questions I had have been answered, and I understand I may ask further questions at any time.
3. I understand what is involved in participating, that it is voluntary, and that I may withdraw at any stage during the survey or interview.
4. I understand the results may be used for academic publications, such as journal articles.
5. I agree to take part in this study under the conditions set out above.

I agree to take part in this research ___________________________________

Instructions for Participants

We are gathering lots of different views and are a part of a much larger project funded by the ESRC's Discribe network. Discribe is a groundbreaking social science-led digital security related programme, part of the UK Government's wider Digital Security by Design (DSbD) Programme to drive the development of DSbD technology. The data you provide will help us to understand the every day thinking around security related decision making. You can read more about Discribe here: https://www.discribehub.org

You are invited to complete four stories related to security adoption decisions — this means that you read the opening sentences of a story and then write what happens next. There is no right or wrong way to complete the story, and you can be as creative as you like. The stories are based upon fictional events. We are interested in the many different stories that people can write. Please don't spend too long thinking about what might happen next — just write about whatever first comes to mind. Because collecting in-depth stories is important for our research, please write a story that is at least four sentences and spend 5-10 minutes responding to each story.

Question 1

It's 2024. A new hardware has recently been proven to reduce cyber vulnerability by 70% without interrupting users' usual activities. A and B - who are senior/strategic managers in organisation X - are having a meeting to discuss whether organisation X should become one of the first organisations in the world to adopt this new hardware.

What is most likely to happen? Please use your imagination to complete the story.

____

____

____

____

____

Question 2

C who works in organisation Y received an email from the IT department two weeks ago, requesting all employees to complete a software update within one month, which was related to a new hardware adopted across organisation Y to increase cyber security. C came to work this morning, only to find his / her work computer locked by a ransomware attack.

What is most likely to happen? Please use your imagination to complete the story.

____

____

____

____

____

Question 3

After a six-months transition period, organisation Z has implemented the new hardware to increase cyber security across all departments. Head of IT department D has just sent out an organisation-wide email announcing this milestone, before he / she gets an urgent call from E, the head of another department, reporting a severe data leak which requires an immediate solution.

What is most likely to happen? Please use your imagination to complete the story.

____
____
____
____
____

Question 4

It has been 5 years since F, the principle legal advisor of organisation W, called for the first meeting of senior management level regarding the adoption of the new hardware to increase cyber security. These meetings have been more and more frequent over these years, and today is the 17th meeting where proposals for incentives are being discussed.

What is most likely to happen? Please use your imagination to complete the story.

____
____
____
____
____

6. Appendix B – Cognitive Task Analysis Interview Protocol

The Elicitation of Cyber Security Narratives

Setting up the interview:

We are conducting research as part of a Discribe DSbD grant to study how people in organisations make security adoption decisions. In particular, we want to understand the cues that lead an individual to adopt security technology, policies or practices. To do this, we are interviewing a range of people to find out what is important to them when making such decisions. Once we understand the different cues and strategies in making security adoption decisions, we can support translating this knowledge to a range of users.

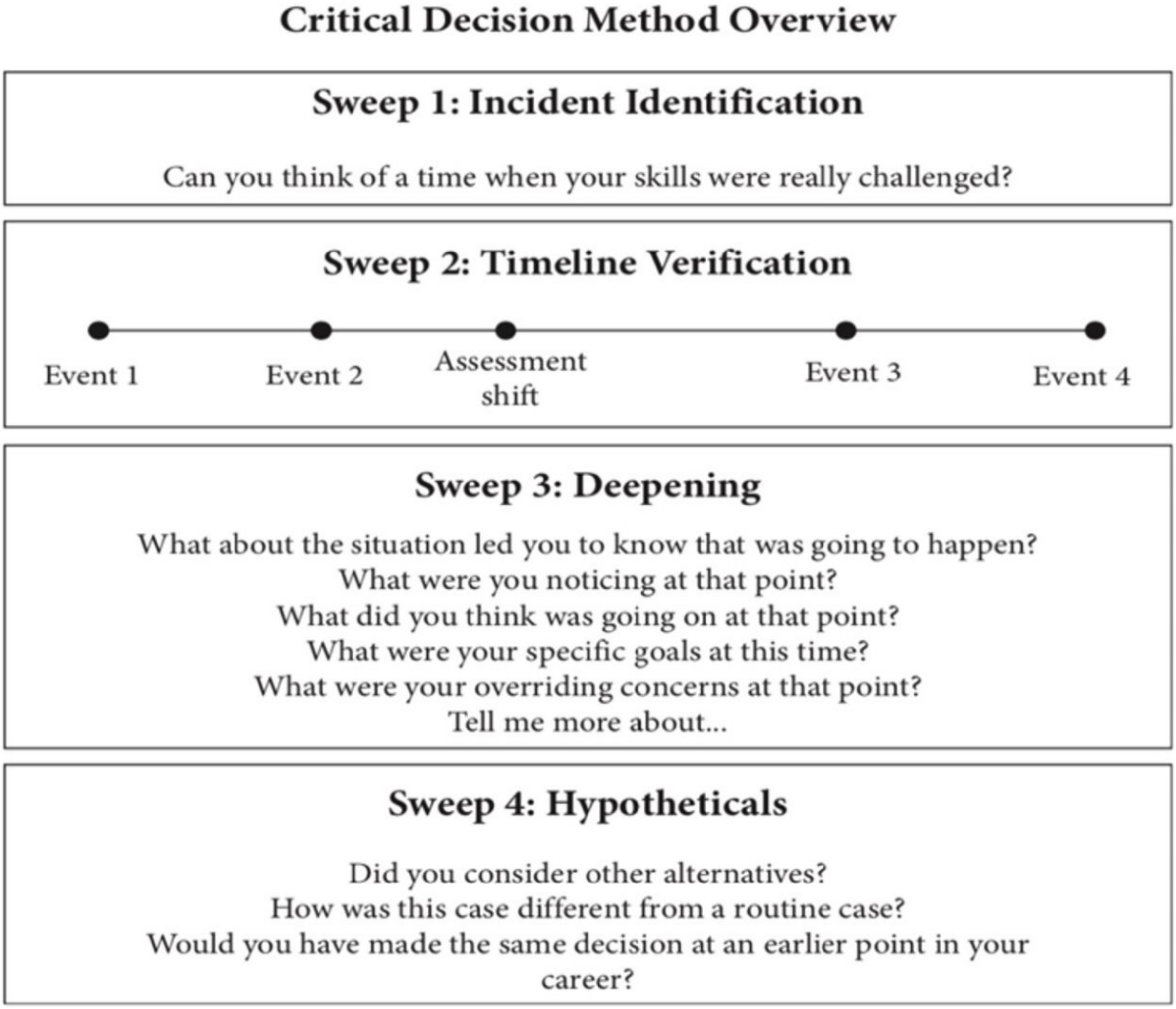
There are three parts of the discussion today. First, we will ask some questions about your background, training and experience. In the second part, we will ask about your thoughts on the story stems we are developing, and third we will ask questions relating to some of your experiences where you were involved in security adoption decisions.

Do you have any questions before we begin?

Before we get started, we would like to request your permission to record this discussion. The Teams recording will automatically be transcribed, treated as confidential and shared only with the research team. If at any point you feel like you want to tell us something but don't want it to be recorded, just let me know and we will turn off the recording function.

Background questions

1. What is your current role ?
2. How long have you been in that role?
3. How long have you been making security adoption decisions ?



Critical Decision Method Overview

Sweep 1: Incident Identification

Can you think of a time when your skills were really challenged?

Sweep 2: Timeline Verification

Sweep 3: Deepening

What about the situation led you to know that was going to happen?
What were you noticing at that point?
What did you think was going on at that point?
What were your specific goals at this time?
What were your overriding concerns at that point?
Tell me more about...

Sweep 4: Hypotheticals

Did you consider other alternatives?
How was this case different from a routine case?
Would you have made the same decision at an earlier point in your career?

FIGURE 1 Four sweeps of the critical decision method.

Sweep 1: Incident Identification
I'd like you to think about the security adoption decisions that you have made. Tell me about a time that really stands out as a *challenging* case. It may have been challenging because of the way in which the decision was presented to you or your team, or because of a particular individual or a tech challenge.

Sweep 2: Timeline Verification
Draw a timeline out on the board and include the big points (to be further filled in during sweep 3)
Look for decision points, places to probe, gaps in the timeline and ambiguity.
Probe statements like "I just knew...", "Something felt wrong..."

- Can you provide a 2 minute overview of the decision ?
- How many minutes/hours/days from being asked to adopt the security measure to implementing it, did this take
- Identify challenging points in early management of the process
- Ask about any decisions that altered your train of thought

Sweep 3: Deepening

- Where were you when you learned of need for the security measure ? What were you doing? Where was the rest of your team?
- Timing- time of year, time of day ?
- What was your role at the time?
- Who told you about security requirement ?
- What information did you initially have? What more did you want to know?
- Was the history/info reliable? Was anything confusing/contradictory?
- Who else was taking care of the security adoption decision ? What were their impressions?
- Did you seek advice/input from others?
- Describe the operational requirements needed to complete your task.

Sweep 4: What If Queries

- Describe your differential. Why were you considering different options ?
- Did your prior experience with security influence how you completed the task?
- How did this experience change how you think about security adoption ?
- What would you have done differently?
- What if the requirement had been seen by a provider at a different level of the organisation / internal/external?
- Did your team challenge your understanding of the security adoption measure ?
- What were the learning points that you took away from this experience?
- How comfortable do you feel in managing security adoption decisions ?

7. References

AlAbdulkarim, L. O., & Lukszo, Z. (2010, April). Information security implementation difficulties in critical infrastructures: Smart metering case. In *2010 International Conference on Networking, Sensing and Control (ICNSC)* (pp. 715-720). IEEE. https://doi.org/10.1109/ICNSC.2010.5461569

Ahmed, V. & Al-Haddad, S. (2021). The use of social engineering to change organizational behavior toward information security in an educational institution. *Journal of Information Systems Security,* 17(2), 103-124. ISSN: 1551-0123

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, *11*(3), Article 3. https://doi.org/10.3390/fi11030073

Alhumayzi, M., Batista, L., Benson, V. (2023). Factors affecting employees' acceptance of blockchain in the higher education institutions. 25th *International Conference on Enterprise Information Systems, ICEIS - Proceedings,* 2, 297 – 303

Ali, M.B., Wood-Harper, T. & Mohamad, M. (2018). Benefits and challenges of cloud computing adoption and usage in higher education. *International Journal of Enterprise Information Systems,* 14(4), 64-77. ISSN 1548- 1115

Ali, M.B. (2019). Multiple perspective of cloud computing adoption determinants in higher education: a systematic review. *International Journal of Cloud Applications and Computing (IJCAC),* 9(3), 21. DOI: 10.4018/IJCAC.2019070106

Alshahrani, M., Beloff, N. & White, M. (2022). Towards a blockchain-based smart certification System for higher education: an empirical study. *International Journal of Computing and Digital Systems,* 11(1) DOI: 10.12785/ijcds/110145

Arslan, M., & Roudaki, J. (2018). Examining the role of employee engagement in the relationship between organisational cynicism and employee performance. *International Journal of Sociology and Social Policy*, *39*(1/2), 118–137. https://doi.org/10.1108/IJSSP-06-2018-0087

Assante, M. J., & Tobey, D. H. (2011). Enhancing the Cybersecurity Workforce. *IT Professional*, *13*(1), 12–15. https://doi.org/10.1109/MITP.2011.6

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Benson, V., McAlaney, J., & Frumkin, L. A. (2019). Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1264–1269). IGI Global. https://doi.org/10.4018/978-1-5225-8897-9.ch062

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. *Sustainability*, *13*(24), 13761. https://doi.org/10.3390/su132413761

Bhargava, V. R. (2020). Firm Responses to Mass Outrage: Technology, Blame, and Employment. *Journal of Business Ethics*, *163*(3), 379–400. https://doi.org/10.1007/s10551-018-4043-7

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Bongiovanni, I. (2018). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, 86, 350–357. DOI: 10.1016/j.cose.2019.07.003

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, *51*, 101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Brown, O., Power, N., & Gore, J. (2022). Cognitive Task Analysis: Eliciting Management Cognition. Proceedings of the American Academy of Management https://doi.org/10.5465/AMBPP.2022.14419abstract

Burke, S. (2020, April 2). *Coronavirus Is Creating A Global 'Work-At-Home' Culture*. CRN. https://www.crn.com/news/cloud/coronavirus-is-creating-a-global-work-at-home-culture

Burke, S. (2020, April 2). *Coronavirus Is Creating A Global 'Work-At-Home' Culture*. CRN. https://www.crn.com/news/cloud/coronavirus-is-creating-a-global-work-at-home-culture

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwar, L., & Van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety–developing the conceptual framework. *Ergonomics*, *58*(4), 548-564. https://doi.org/10.1080/00140139.2015.1015623

Chen, Y., Ramamurthy, K. (Ram), & Wen, K.W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems*, *55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Clark, V., Braun, V., Frith, H., Moller, N. (2019). Editorial Introduction to the Special Issue: Using Story Completion Methods in Qualitative Research. *Qualitative Research in Psychology*. 16: 1, 1-20

Clark, R. (2014). Cognitive Task Analysis for Expert-Based Instruction in Healthcare. In J. M. Spector, M. D. Merrill, J. Elen, & M. J. Bishop (Eds.), *Handbook of Research on Educational Communications and Technology* (pp. 541–551). Springer. https://doi.org/10.1007/978-1-4614-3185-5_42

Cognitive Requirements for Small Unit Leaders in Military Operations in Urban Terrain. (n.d.). Retrieved 7 September 2023, from https://apps.dtic.mil/sti/citations/ADA355505

Crandall, B., Klein, G. A., & Hoffman, R. R. (2006). *Working Minds: A Practitioner's Guide to Cognitive Task Analysis*. The MIT Press. https://doi.org/10.7551/mitpress/7304.001.0001

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dean, J. W., Brandes, P., & Dharwadkar, R. (1998). Organizational Cynicism. *Academy of Management Review*, *23*(2), 341–352. https://doi.org/10.5465/amr.1998.533230

Definition of accountability | Dictionary.com. (n.d.). Www.Dictionary.Com. Retrieved 23 May 2023, from https://www.dictionary.com/browse/accountability

Developing a Rapid Situation Awareness: Understanding the Challenges Faced by First Responders to Biological and Chemical Events. (n.d.). Retrieved 7 September 2023, from https://apps.dtic.mil/sti/citations/ADA408914

Dogruel, L., & Joeckel, S. (2019). Risk Perception and Privacy Regulation Preferences From a Cross-Cultural Perspective. A Qualitative Study Among German and U.S. Smartphone Users. *International Journal of Communication*, *13*(0), Article 0.

Donalds, C., & Barclay, C. (2022). Beyond technical measures: A value-focused thinking appraisal of strategic drivers in improving information security policy compliance. *European Journal of Information Systems*, *31*(1), 58–73. https://doi.org/10.1080/0960085X.2021.1978344

Dykstra, J. (2015). *Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems*. O'Reilly Media, Inc.

Eliciting and Representing the Knowledge of Experts (Chapter 11)—The Cambridge Handbook of Expertise and Expert Performance. (n.d.). Retrieved 7 September 2023, from https://www.cambridge.org/core/books/abs/cambridge-handbook-of-expertise-and-expert-performance/eliciting-and-representing-the-knowledge-of-experts/5F9D3BA780C53B8104ECF982933909CF

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Ernst & Young. (2018) Is cybersecurity about more than protection? EY's global information security survey 2018-19. *Ernst & Young.*

Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). *Cyber Security Behaviour In Organisations* (arXiv:2004.11768). arXiv. https://doi.org/10.48550/arXiv.2004.11768

European Council. 2021. Cybersecurity: how the EU tackles cyber threats. https://www.consilium.europa.eu/en/policies/cybersecurity/. Accessed 10 May 2021

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Fombrun, C. J. (2012). The building blocks of corporate reputation: Definitions, antecedents, consequences. In T. G. Pollock (Eds.) & M. L. Barnett (Eds.), *The Oxford Handbook of Corporate Reputation* (pp. 94-113). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199596706.013.0005

Gangwar, H., & Date, H. (2015). Exploring Information Security Governance in Cloud Computing Organisation. *International Journal of Applied Management Sciences and Engineering (IJAMSE)*, *2*(1), 44–61. https://doi.org/10.4018/ijamse.2015010104

Gatzert, N. (2015). The impact of corporate reputation and reputation damaging events on financial performance: Empirical evidence from the literature. *European Management Journal*, *33*(6), 485–499. https://doi.org/10.1016/j.emj.2015.10.001

Gatzert, N., Schmit, J. T., & Kolb, A. (2016). Assessing the Risks of Insuring Reputation Risk. *Journal of Risk and Insurance*, *83*(3), 641–679. https://doi.org/10.1111/jori.12065

Gerhold, L., Schmidt, T., & Brandes, E. (2019). Making Use of Foresight to Capture the Co-Evolution of Security Technologies and Societal Development. *2019 IEEE International Symposium on Technology and Society (ISTAS)*, 1–5. https://doi.org/10.1109/ISTAS48451.2019.8937996

Gonzalez Arrieta et al. (2021). "It's not actually that horrible": exploring adoption of two-factor authentication at a University. *CHI* 2018, April 21–26, 2018, Montréal, QC, Canada. DOI: 10.1145/3173574.3174030

Gore, J., Banks, A. P., & McDowall, A. (2018). Developing cognitive task analysis and the importance of socio-cognitive competence/insight for professional practice. *Cognition, Technology & Work*, *20*(4), 555–563. https://doi.org/10.1007/s10111-018-0502-2

Gore, J., Flin, R., Stanton, N., & Wong, B. L. W. (2015). Applications for naturalistic decision-making. *Journal of Occupational and Organizational Psychology*, *88*(2). https://doi.org/10.1111/joop.12121

GOV.UK. (2023). Cyber security breaches survey 2023: education institutions annex, **Cyber security breaches survey 2023: education institutions annex - GOV.UK (www.gov.uk)**, accessed 04.07.23

Granic, A. (2022). Educational technology adoption: a systematic review. *Education and Information Technologies,* 27(7), 9725-9744. DOI:10.1007/s10639-022-10951-7.

Granic, A. (2022). Educational technology adoption: a systematic review. *Education and Information Technologies,* 27(7), 9725-9744. DOI:10.1007/s10639-022-10951-7.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, *3*(1), 49-58. https://doi.org/10.1093/cybsec/tyw018

Gunn, C. P., & Taylor, I. M. (2021). Using the Think Aloud Protocol to Measure Desire-Goal Conflict and Conflict Resolution in a Postural Persistence Task. *Measurement in Physical Education and Exercise Science*, *25*(2), 87–94. https://doi.org/10.1080/1091367X.2020.1835663

Haney, J., Acar, Y., & Furman, S. (n.d.). “It’s the Company, the Government, You and I”: User Perceptions of Responsibility for Smart Home Privacy and Security. *Proceedings of USENIX Security 2021*, 411–428. https://www.usenix.org/conference/usenixsecurity21/presentation/haney

Herath, T. C., Herath, H. S. B., & D’Arcy, J. (2020). Organizational Adoption of Information Security Solutions: An Integrative Lens Based on Innovation Adoption and the Technology-Organization- Environment Framework. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *51*(2), 12–35. https://doi.org/10.1145/3400043.3400046

HESA. (2023). Higher Education Staff Statistics: UK, 2021/22. Higher Education Staff Statistics: UK, 2021/22 | HESA. Accessed 04.07.23.

Information Commissioners Office (ICO). Findings from ICO information risk reviews of information security in the higher education sector April 2017 to March 2018. Findings from ICO information risk reviews of information security in the higher education sector, accessed 04.07.23.

Ifenthaler, D. & Egloffstein, M. (2020). Development and implementation of a maturity model of digital transformation. *TechTrends,* 64, 302–309, Doi.org/10.1007/s11528-019-00457-4

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jenkins, N. A. S., Paul M. Salmon, Laura A. Rafferty, Guy H. Walker, Chris Baber, Daniel P. (2017). *Human Factors Methods: A Practical Guide for Engineering and Design* (2nd ed.). CRC Press. https://doi.org/10.1201/9781315587394

Jr, D. J. L., Perumalla, D. K., & Siraj, D. A. (2021). *ICCWS 2021 16th International Conference on Cyber Warfare and Security*. Academic Conferences Limited.

Li, N., Zhang, X. & Limniou, M. (2023). A country’s national culture affects virtual learning environment adoption in higher education: a systematic review (2001–2020). *Interactive Learning Environments*, 31(7), 4407-4425. DOI: 10.1080/10494820.2021.1967408

Majeed, A & Ali, M. (2018). How Internet-of-Things (IoT) making the university campuses smart? QA higher education (QAHE) perspective. *IEEE,* 8th Annual Computing and Communication Workshop and Conference: 8-10 January 2018, Las Vegas, NV, US. 2018(Jan), 935-648 DOI: 10.1109/CCWC.2018.8301774

Kanter, D. L., & Mirvis, P. H. (1989). *The cynical Americans: Living and working in an age of discontent and disillusion* (pp. xxii, 329). Jossey-Bass.

Kelly, R. (2017, March 3). *Almost 90% of Cyber Attacks are Caused by Human Error or Behavior.* Chief Executive. Available at: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Klein, G. A. (2017). *Sources of Power, 20th Anniversary Edition: How People Make Decisions*. MIT Press.

Klein, G. A., & Calderwood, R. (1991). Decision models: Some lessons from the field. *IEEE Transactions on Systems, Man, and Cybernetics*, *21*(5), 1018–1026. https://doi.org/10.1109/21.120054

Klein, G., & Militello, L. (2001). 4. Some guidelines for conducting a cognitive task analysis. In *Advances in Human Performance and Cognitive Engineering Research* (Vol. 1, pp. 163–199). Emerald (MCB UP). https://doi.org/10.1016/S1479-3601(01)01006-2

Laborde, S., Dosseville, F., & Raab, M. (2013). Introduction, comprehensive approach, and vision for the future. *International Journal of Sport and Exercise Psychology*, *11*(2), 143–150. https://doi.org/10.1080/1612197X.2013.773686

Lintern, G., Moon, B., Klein, G., & Hoffman, R. R. (2018). Eliciting and Representing the Knowledge of Experts. In A. M. Williams, A. Kozbelt, K. A. Ericsson, & R. R. Hoffman (Eds.), *The Cambridge Handbook of Expertise and Expert Performance* (2nd ed., pp. 165–191). Cambridge University Press. https://doi.org/10.1017/9781316480748.011

Lloyd, C. E. M., Mengistu, B. S., & Reid, G. (2022). “His Main Problem Was Not Being in a Relationship With God”: Perceptions of Depression, Help-Seeking, and Treatment in Evangelical

Christianity. *Frontiers in Psychology*, *13*. https://www.frontiersin.org/articles/10.3389/fpsyg.2022.831534

Lupton, B., & Sarwar, A. (2021). Blame at Work: Implications for Theory and Practice from an Empirical Study. *Business and Professional Ethics Journal*, *40*(2), Article 2.

Lupton, B., & Warren, R. (2018). Managing without blame? Insights from the philosophy of blame. *Journal of Business Ethics*, *152*, 41-52.

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010, September). A cognitive task analysis for cyber situational awareness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 54, No. 4, pp. 279-283). Sage CA: Los Angeles, CA: Sage Publications.

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*, *95*, 101846. https://doi.org/10.1016/j.cose.2020.101846

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

Marotta, A., & Pearlson, D. K. (n.d.). *A Culture of Cybersecurity at Banca Popolare di Sondrio*.

Martin, J., Frost, P., & O'Neill, O. (2004). *Organizational Culture: Beyond Struggles for Intellectual Dominance*. https://doi.org/10.4135/9781848608030.n26

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*, 2823-2836. https://doi.org/10.1007/s13042-018-00906-1

Martins, A., & Elofe, J. (2002). Information Security Culture. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), *Security in the Information Society: Visions and Perspectives* (pp. 203–214). Springer US. https://doi.org/10.1007/978-0-387-35586-3_16

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., & Skourlas, C. (2014). Human factor and information security in higher education. *Journal of Systems and Information Technology*, *16*(3), 210–221. https://doi.org/10.1108/JSIT-01-2014-0007

Militello, L., Dominguez, C., Ebright, P., Moon, B., Russ, A., & Weir, C. (2014). Tailoring Cognitive Task Analysis (CTA) Methods for Use in Healthcare. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*(1), 758–762. https://doi.org/10.1177/1541931214581138

Mimecast. (2016, June 7). *Will Cyber Insurance Payout for Evolving Email Attacks*. Mimecast. https://www.mimecast.com/resources/press-releases/nearly-half-of-organizations-unsure-if-cyber-insurance-will-payout-for-evolving-email-attacks/

Moller, N. P., Clarke, V., Braun, V., Tischner, I., & Vossler, A. (2021). Qualitative story completion for counseling psychology research: A creative method to interrogate dominant discourses. *Journal of Counseling Psychology*, *68*(3), 286–298. https://doi.org/10.1037/cou0000538

Nair, P., & Kamalanabhan, T. J. (2010). The impact of cynicism on ethical intentions of Indian managers: The moderating role of seniority. Journal of international business ethics, 3(1), 14.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization science*, *3*(3), 398-427.

Orlikowski, W. J. (1993). CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly*, *17*(3), 309–340. https://doi.org/10.2307/249774

Panno, A., Anna Donati, M., Chiesi, F., & Primi, C. (2015). Trait Emotional Intelligence is Related to Risk-Taking Through Negative Mood and Anticipated Fear. *Social Psychology*, *46*(6), 361–367. https://doi.org/10.1027/1864-9335/a000247

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making, 9*(2), 117-129.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Public Company Cybersecurity Disclosures (Release Nos. 33-10459, 34-82746). Published February 21, 2018.

Pupion, P-C. (2010). ICT adoption and crisis management: the case of a public education organization. *Problems and Perspectives in Management,* 8(4), 15-22. ISSN: 1727-7051

Rahman, M. R., Hezaveh, R. M., & Williams, L. (2023). What Are the Attackers Doing Now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A Survey. *ACM Computing Surveys*, *55*(12), 241:1-241:36. https://doi.org/10.1145/3571726

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open*, *11*(1), 21582440211000049.

Reichers, A. E., Wanous, J. P., & Austin, J. T. (1997). Understanding and managing cynicism about organizational change. *Academy of Management Perspectives*, *11*(1), 48–59. https://doi.org/10.5465/ame.1997.9707100659

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: An uneasy partnership? *Information Management & Computer Security*, *20*(4), 296–311. https://doi.org/10.1108/09685221211267666

Renaud, K., Orgeron, C., Warkentin, M., & French, P. E. (2020). Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. *Public Administration Review*, *80*(4), 577–589. https://doi.org/10.1111/puar.13210

Rindova, V. P., & Fombrun, C. J. (1999). Constructing competitive advantage: the role of firm–constituent interactions. *Strategic management journal*, *20*(8), 691-710.

Sagie, A., Birati, A., & Tziner, A. (2002). Assessing the costs of behavioral and psychological withdrawal: A new model and an empirical illustration. *Applied psychology*, *51*(1), 67-89.

Schraagen, J. M. (2008). *Naturalistic Decision Making and Macrocognition*. Ashgate Publishing, Ltd.

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice*, *124*, 523–536. https://doi.org/10.1016/j.tra.2018.06.033

Shropshire, J.D, Warkentin, M. & Johnston, M.A. (2010). Impact of negative message framing on security adoption. *The Journal of Computer Information Systems*, 51(1), 41-51. Universities UK. (2023). Higher education in numbers. Higher education in numbers (universitiesuk.ac.uk) , accessed 04.07.23.

Sivan-Sevilla, I. (2021). Framing and governing cyber risks: Comparative analysis of US Federal policies [1996–2018]. *Journal of Risk Research*, *24*(6), 692-720.

Skarlicki, D. P., Kay, A. A., Aquino, K., & Fushtey, D. (2017). Must heads roll? A critique of and alternative approaches to swift blame. *Academy of Management Perspectives*, *31*(3), 222-238.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, *177*(3), 1333–1352.

Smith, J. A. (2015). *Qualitative Psychology: A Practical Guide to Research Methods*. 1–312.

Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. Interdisciplinary Journal of Contemporary Research in Business, 5(7), 329-354

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management*, *58*, 102298. https://doi.org/10.1016/j.ijinfomgt.2020.102298

Stanton, N.A., Salmon, P.M., Rafferty, L.A., Walker, G.H., Baber, C., & Jenkins, D.P. (2013). *Human Factors Methods: A Practical Guide for Engineering and Design* (2nd ed.). CRC Press. https://doi.org/10.1201/9781315587394

Sunstein, C. R. (2003). Hazardous Heuristics. *The University of Chicago Law Review, 70*(2), 751-782. https://doi.org/10.2307/1600596

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, *17*(2), 179–186. https://doi.org/10.1007/s10799-015-0252-2

Vaughan, P., Lenette, C., & Boydell, K. (2022). 'This bloody rona!': Using the digital story completion method and thematic analysis to explore the mental health impacts of COVID-19 in Australia. *BMJ Open*, *12*(1), e057393. https://doi.org/10.1136/bmjopen-2021-057393

Vaughan, R., Laborde, S., & McConville, C. (2019). The effect of athletic expertise and trait emotional intelligence on decision-making. *European Journal of Sport Science*, *19*(2), 225–233. https://doi.org/10.1080/17461391.2018.1510037

Walker, G. H., Stanton, N. A., Jenkins, D., Salmon, P., Young, M., & Aujla, A. (2007). Sociotechnical Theory and NEC System Design. In D. Harris (Ed.), *Engineering Psychology and Cognitive Ergonomics* (pp. 619–628). Springer. https://doi.org/10.1007/978-3-540-73331-7_68

Ward, P., Gore, J., Hutton, R., Conway, G. E., & Hoffman, R. R. (2018). Adaptive Skill as the Conditio Sine Qua Non of Expertise. *Journal of Applied Research in Memory and Cognition*, *7*(1), 35–50. https://doi.org/10.1016/j.jarmac.2018.01.009

Watson, A., & Lupton, D. (2022). What Happens Next? Using the Story Completion Method to Surface the Affects and Materialities of Digital Privacy Dilemmas. *Sociological Research Online*, *27*(3), 690–706. https://doi.org/10.1177/13607804221084343

Weierich, M. R., Wright, C. I., Negreira, A., Dickerson, B. C., & Barrett, L. F. (2010). Novelty as a dimension in the affective brain. *NeuroImage*, *49*(3), 2871–2878. https://doi.org/10.1016/j.neuroimage.2009.09.047

Wells, P. & Ingley, C. (2019). Governance and leadership implications for academic professionals in the era of technological disruption. *Journal of Management and Governance,* 23, 21–32. https://doi.org/10.1007/s10997-018-9424-x

Whitworth, B., & De Moor, A. (Eds.). (2009). *Handbook of research on socio-technical design and social networking systems*. IGI Global.

Wyld, D.C. (2009). Help! Someone stole my laptop!: How RFID technology can be used to counter the growing threat of lost laptops. *Journal of Applied Security Research*, 4(3), 363-373. DOI: 10.1080/19361610902930196

The Discribe Hub+ is funded by UKRI through ESRC
Grant no: ES/V003666/1.
For more information about the Hub+ please visit
www.discribehub.org

© 2021 Discribe Hub+ Creative Commons4.0
BY-NC-SA licence.
www.discribehub.org/copyright