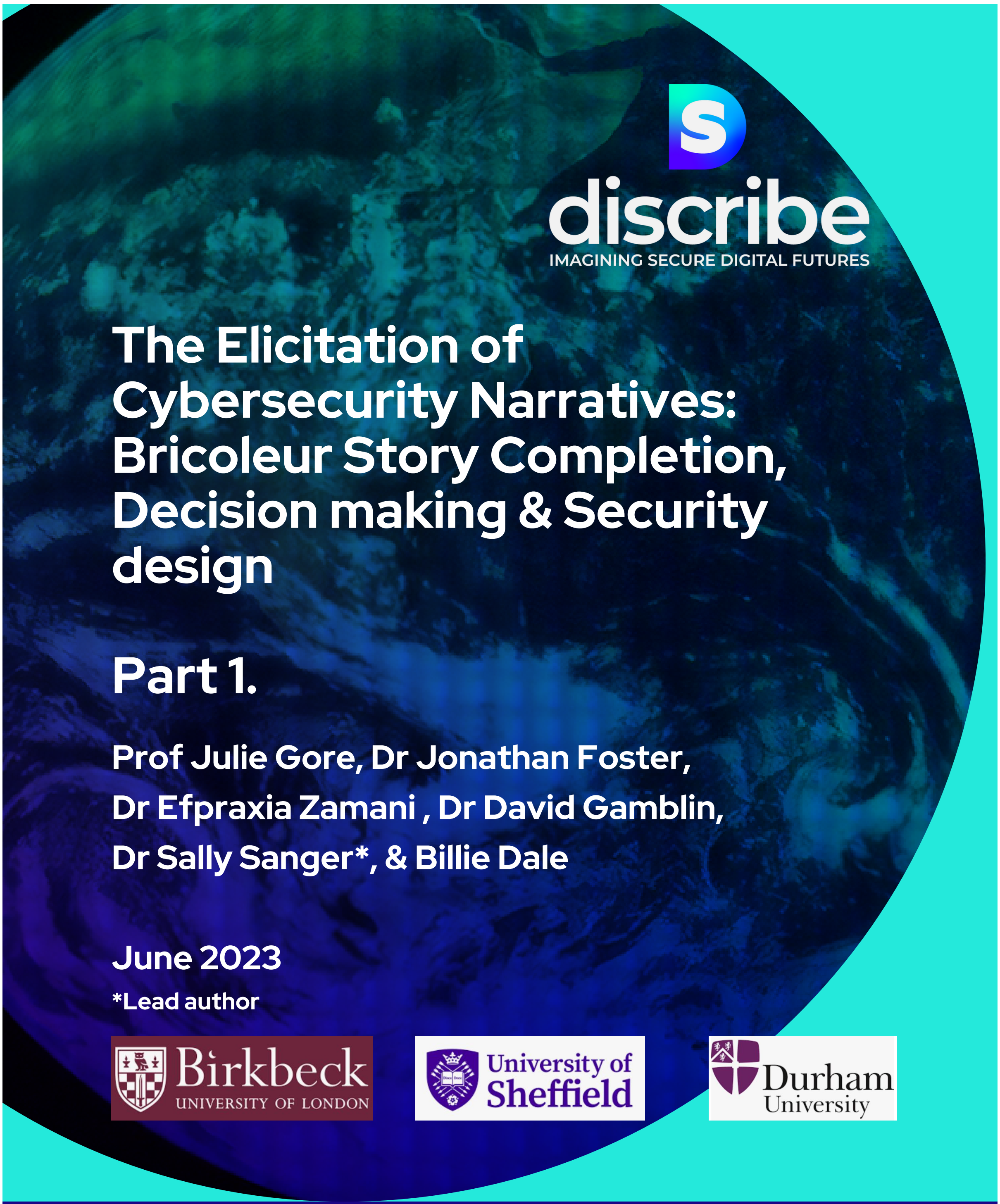


discribe

IMAGINING SECURE DIGITAL FUTURES

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

Part 1.

Prof Julie Gore, Dr Jonathan Foster,

Dr Efpraxia Zamani , Dr David Gamblin,

Dr Sally Sanger*, & Billie Dale

June 2023

*Lead author

Birkbeck UNIVERSITY OF LONDON

University of Sheffield

Durham University

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

UK Research and Innovation

Understanding the security technology adoption process: a rapid evidence review

1. Executive Summary

Purpose. Informed by a structurational model of technology, the purpose of this review is to provide an evaluation of the available research evidence in support of the benefits and risks, organisational conditions and consequences of security technology adoption. In doing so both academics and practitioners will be better able to understand not only the technical but also the organisational and social factors involved in the effective adoption of security technologies. The evidence review was guided by the following research questions: What are the expected/actual benefits and risks of adopting security technologies? What cognitive decision-making processes are utilised and shared in adoption discussions, policy or process? What regulatory, governance and other incentives are required to facilitate the process of security technology adoption? What are the organisational conditions and consequences of adopting security technologies? *Methodology*. A literature search of the multidisciplinary social sciences Scopus database was conducted. An initial keyword search identified a pool of 17621 potentially relevant articles. After screening of the titles and abstracts, and full-text for relevance, further discussion within the research team, and initial critical appraisal, 67 articles were included for the full evidence review. Of these articles, 31 were quantitative studies consisting of evidence mainly from cross-sectional studies or surveys and 26 were qualitative studies consisting of evidence mainly from theoretical papers together with a small number of case studies. The remaining 9 studies mainly consisted of mixed methods studies. Critical appraisal then assessed the articles against the CASP and CEBMa checklists. The evidence base was varied in its methodological quality with 29 articles assessed to be high quality, 27 to be of medium quality and 10 to be of low quality. *Findings.* 37 articles were on security technologies generally, with 29 on specific technologies, notably cloud computing (12) and blockchain (7) . 26 articles were in non-Western settings and 24 in Western settings, with 16 either referring to a mixture of settings or where the setting was not pertinent to the study. The sectors in which the studies were conducted were mainly general, non-specified or mixed (38), with specific sectors identified as government (8), banking (5), ICT (4), education (3), retail, sales & marketing (3), finance (2), oil & gas (2) and energy (1). Most articles focused on more than one of the research questions. In descending order of prevalence, articles studied organisational conditions (56), risks (35), regulations and other incentives (29), benefits (29), decision-making (26) and organisational consequences (23). The proportion of high-quality papers for each topic ranged from 65% for organisational consequences to 42% for decision-making. Expected benefits of adopting security technologies included high-quality evidence in support of perceived reputational benefits, although actual benefits were mainly financial, with medium-quality evidence in support of compliance benefits. The unexpected risks of adopting security technologies related to organisational and environmental, human, and technological factors. There was a substantial amount of consistent high and medium quality evidence that extra- and intra- organisational conditions like governance, culture, education and staff training are key enabling factors. There was also a small amount of high quality, consistent evidence that the period immediately following the adoption of new security technologies is a risky time with a higher occurrence of security breaches not simply due to better identification of issues. *Conclusions and implications*. The evidence base points to the need for a holistic approach to the adoption of security technologies. This approach combines an awareness of their expected benefits and risks with an awareness of the organisational conditions and consequences of the security technologies in use. In particular, practitioners should be aware that the process of security technology adoption carries not only expected benefits and risks but may also over time give rise over time to unexpected risks and unintended consequences. In sum, from a sociotechnical perspective, benefits of security technology by design should be supplemented with a recognition of the ongoing interaction that will be required between technology, actors and organisational structure. In order for their benefits to be realized and risks mitigated.

2. Background

The scaling up of digital services places organisations at an increased risk of exposure to security threats and forms of digital vulnerability. These include phishing, information leaks, ransomware attacks, and social engineering, to name only a few. To mitigate exposure to these risks, it is critical for organisations to consider the adoption of new security technologies. While much is known about organisational adoption of technologies in general, comparatively less is known about the effective adoption of security technologies (AoST), especially hardware security technologies. Security technologies "are concepts, policies, and components designed to minimize risk, identify vulnerabilities, and inform how and when to respond to potential incidents" (OpenPath, 2022). They offer deterrence, detection, prevention and/or response to cyber security incidents. Hardware security technologies achieve these ends via physical components (hardware) rather than software (Yasar, 2022). A recent study of 1,406 US IT and IT security experts found that 83% had adopted or were planning in the next 6 months to adopt hardware security technologies. This included, for example:

> "control-flow enforcement technology, hardware telemetry to inform malicious signals, cryptographic encryption and acceleration, virtualized machines, offload engines to enable greater cryptographic security and/or endpoint authentication and a trusted platform module (TPM) chip." (Ponemon Institute, 2022, p1)

Herath et al., (2020) stated that: "firm-based examinations of security implementations have received scant research attention" (p24), and Ihmouda et al., (2015) noted that "the literature focusing on information security effectiveness in organization[s] is sparse" (p9641). Wang et al., (2021) observed a lack of research into:

> "the ongoing, recursive relationship between technology and the people in organizations…the generative nature of technology and how organizations perceive affordances and constraints and consequently shape technology" (p2)

This lack of knowledge also extends to the security aspects involved in the effective adoption of technologies such as blockchain, cloud computing and biometrics.

Knowing more about the effective adoption of new security technologies - their benefits and risks, the decision-making processes involved, and the organisational conditions and consequences pertinent to realising the benefits and mitigating any risks – is of interest to a range of stakeholders. These include internal organisational stakeholders such as business managers, technology and risk managers, information officers, and technology developers. They also include external organisational stakeholders such as security technology designers, regulators, researchers and in many cases, the clients of organisations and citizens/society.

The purpose of this rapid evidence review (RER) is to systematically gather the evidence currently available on the issues involved in the adoption of security technologies, especially hardware technologies. The review provides a balanced assessment of the issues for the benefit of internal and external organisational stakeholders who are considering such adoptions. To the best of our knowledge, there is no extant review examining the evidence for the effective adoption of new security technologies in general and new hardware security technologies in particular.

3. Objectives and research questions

3.1 Primary objective

To conduct a rapid evidence review of the literature in order to gain an understanding of the issues relevant to the process of security technology adoption, particularly hardware security technology. This includes exploring the current evidence for why and how organisations adopt security technologies and the organisational changes that may be required before or once the process of adoption has begun.

3.2 Research questions

RQ1: What are the expected / actual benefits and risks of adopting new security technologies?
RQ2: What cognitive decision-making processes are utilised and shared in adoption discussions, policy, or processes?
RQ3: What regulatory, and other incentives are required to facilitate the process of security technology adoption?
RQ4: What are the organisational conditions and consequences of adopting new secure technologies?

4. Methodology

4.1 Inclusion/exclusion criteria

Table 1: Inclusion/exclusion criteria

Inclusion criteria	Exclusion criteria
Study covered: Adoption of new security technology hardware Adoption of other new security technology Security aspects of non-security technologies Study had a focus on outcomes found	Study did not refer to security technology or the security aspects of adopting technologies or the process of security technology adoption
Study population: Organisational employees with a role in the procurement, design, implementation, and use of security technologies	Studies of students or general populations excluded
Original study	Study did not contain original data
Study settings: any sector	
Time period: 2000 onwards	
Publication: English language, peer reviewed	
Conceptually related cases, here signifying cases using a similar theoretical framework to identify lessons learnt (Yin, 2009)	

4.1.1 Context

For the RER, we were not restricted to any type of organisation or industrial sector. A risk of increased exposure to security threats and digital vulnerabilities is shared by all organisations and industrial sectors who operate in a digital ecosystem. Within the organisational context, we anticipated that the specific nature of a business, its digital services and mix of products, together with the current technologies in place, would act as important contextual conditions. Given the early-stage nature of the adoption of new security technologies, we were interested in the expected benefits and risks, decision-making processes, organisational conditions and consequences, as well as studies detailing actual findings in relation to these topics.

4.1.2 Study designs

Qualitative, quantitative and mixed methods studies were included, if they explored stakeholders' perceptions, and attitudes, towards AoST.

4.1.3 Drivers

Several drivers were posited to play a role in effective and ineffective AoST. These included general and sectoral regulations, corporate governance, corporate reputation, organisational policy, and client perception; market price; decision-making processes; as well as technology and risk strategy, employee roles and education and training. The role of security threats - actual or anticipated - within a specific or organisational sectoral context could also play a role.

4.1.4 Outcomes

We anticipated that we would need to differentiate between the expected and actual benefits/risks etc. in response to AoST. We wanted to identify how AoST mitigated the risk of exposure to security threats via examining organisational conditions and consequences, reduced the possible occurrence of digital vulnerabilities, and supported a more secure and safer business environment.

4.2 Databases and search terms used

We had originally planned to search for relevant papers within the following academic databases:

- Scopus
- EBSCO Business Source Premier
- Proquest ABI/INFORM Collection & ASSIA
- PsycINFO
- Web of Science

We began by searching Scopus using the chosen keywords and retrieved more than 17,000 academic papers (see Flowchart 1). We then applied the same search to the ASSIA database. Whilst many titles were returned, these mostly overlapped with those from Scopus. In light of this, and the extremely high number of papers found in Scopus, we chose to restrict our work to Scopus only. This choice assumed that the majority of directly relevant papers would be included in the Scopus pool, that any missing ones (potentially identified through the other databases) would be too few to make a considerable impact on our findings and that, therefore, we would still be able to capture important findings. We note that even after data cleaning, a large number of papers remained (14,669). Therefore, in what follows, findings refer to papers identified through Scopus only. As this was a time-limited rapid evidence review citation checking, hand searching, and grey literature were also not included.

The original keyword sets were produced with the aim of identifying papers related to hardware security technologies only. However, after applying the inclusion/exclusion criteria (see section 3.1), the pool of papers reduced very significantly. We therefore chose to expand the remit of the evidence review and incorporate other technologies, which, although not hardware security technologies, were very much related to cyber security and security practices according to literature and received practice. We included a dedicated section (Section 4.7) on these which covers: **cloud computing**, **blockchain**, **biometric and 2FA**, **cryptography**, **mobile payment systems**, **smart cities**, and **information security management systems**. Not all the above are distinct technologies, but some are larger systems (for example smart cities require an assemblage of technologies, cryptography denotes a set of practices and techniques, whereas cloud computing is a technology that requires both software and hardware). What they do have in common however is that they are all discussed in the literature as systems, technologies and techniques that can either provide an additional layer of security on existing information systems, can provide enhanced security as an added value, or require special security-related considerations. Despite the fact that our review casts a wider net to include some software, the lessons reported here can also be adapted for hardware security technologies.

Table 2: Key search terms used

	AND	AND
Secur*	Tech*	
Secur*	Tech*	Adopt*
Secur*	Tech*	Implement*
Org*	Tech*	Adopt*
Org*	Tech*	Implement*
Org*	Tech*	Decision*
Reg*	Tech*	Adopt*
Reg*	Tech*	Implement*
Gov*	Sec*	Tech*
Gov*	Tech*	Org*
Org*	Tech*	Chang*

4.2.1 Search string 1

(KEY (secur*) AND KEY (tech*) AND KEY (adopt*)) AND
(LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011) OR LIMIT-TO (PUBYEAR , 2010) OR LIMIT-TO (PUBYEAR , 2009) OR LIMIT-TO (PUBYEAR , 2008) OR LIMIT-TO (PUBYEAR , 2007) OR LIMIT-TO (PUBYEAR , 2006) OR LIMIT-TO (PUBYEAR , 2005) OR LIMIT-TO (PUBYEAR , 2004) OR LIMIT-TO (PUBYEAR , 2003) OR LIMIT-TO (PUBYEAR , 2002) OR LIMIT-TO (PUBYEAR , 2001)) AND
(LIMIT-TO (LANGUAGE, "English")) AND
(LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ENVI") OR LIMIT-TO (SUBJAREA , "AGRI") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "ENER") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "HEAL") OR LIMIT-TO (SUBJAREA , "NURS") OR LIMIT-TO (SUBJAREA , "MULT"))

● Secur* tech* adopt*	627

Using String 1 but substituting the following keywords

● Secur* tech* implem*	1962
● Org* tech* implem*	1917
● Org* tech* adopt*	2081

Please see Appendix 1 for the remaining search strings used

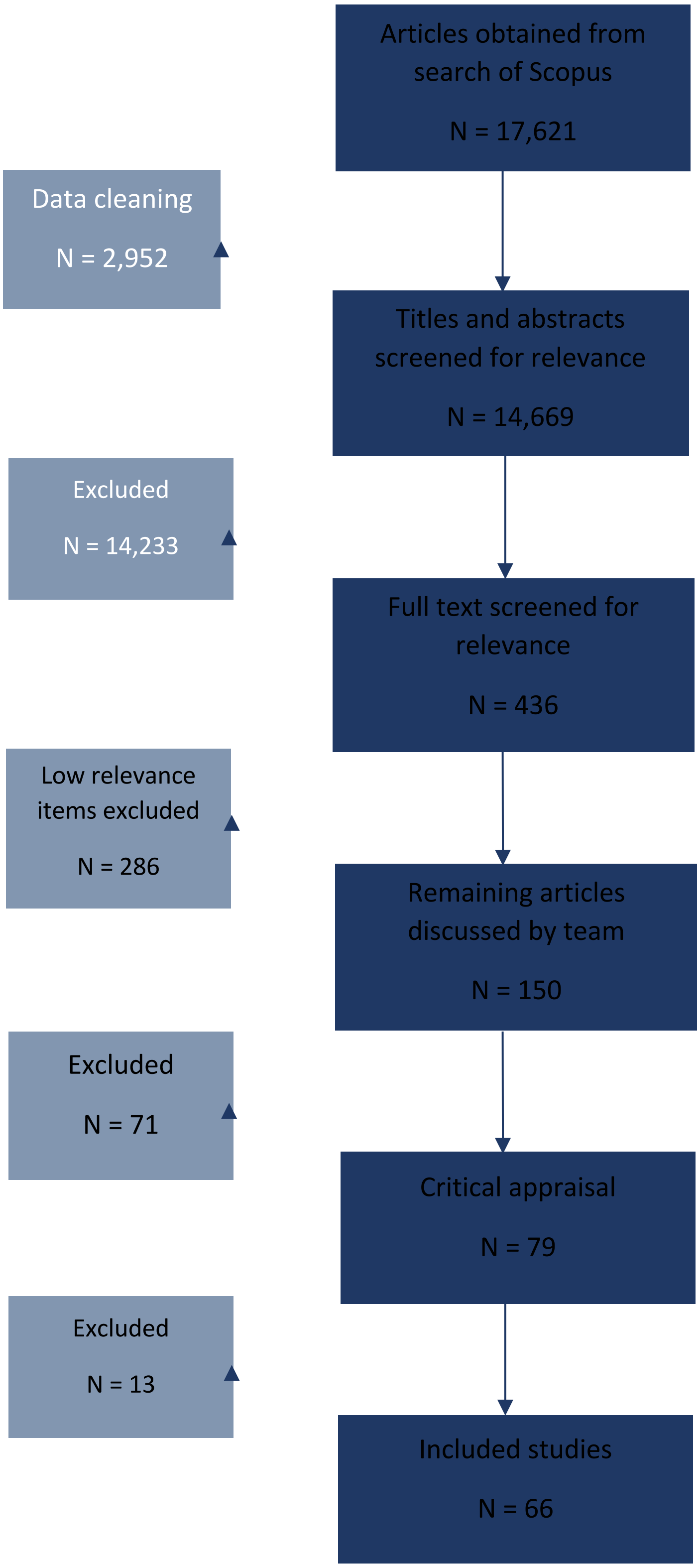
4.2.2 Remaining search results

a)	Org* tech* decision*	4000
b)	Reg* tech* (& keyword implement*)	2101
	Reg* tech* (& keyword adopt*)	1050
c)	Gov* sec* tech*	1946
d)	Gov* tech* org*	1344
e)	Org* sec* change*	593

Total number of articles obtained from searches of Scopus: 17,621

4.3 Study evaluation and selection:

Flowchart 1: Study evaluation and selection


Articles obtained from search of Scopus
N = 17,621
Data cleaning
N = 2,952
Titles and abstracts screened for relevance
N = 14,669
Excluded
N = 14,233
Full text screened for relevance
N = 436
Low relevance items excluded
N = 286
Remaining articles discussed by team
N = 150
Excluded
N = 71
Critical appraisal
N = 79
Excluded
N = 13
Included studies
N = 66

4.3.1 Data cleaning and assessment for relevance

A total of 17,621 articles were retrieved from the initial searches. Duplicate articles, conference/workshop proceedings, irrelevant journals (e.g., overly technical) and low quality/predatory journals were then removed leaving 14,669 articles. The following data for these was collected and entered into an Excel table: authors, title of article, year of publication, source title, DOI, abstract, author's keywords. The abstracts and titles were initially scanned by JF and EZ for relevance using the inclusion/exclusion criteria above (Section 3.1) and reduced to 436.

Articles were then screened in full by SS who assessed:
a) relevance to the research questions and the criteria in Section 3.1,
b) presence of an organisational context,
c) inclusion of items on mitigating risk.
Articles were scored as 3 (highly relevant, N = 33), 2 (of medium relevance, N = 117) or 1 (low relevance, N = 286). Items of low relevance were excluded at this stage leaving 150 papers. These were discussed by the full team and the number of papers further reduced to 79.

4.3.2 Critical appraisal

The articles were then critically appraised by SS, using the following checklists as appropriate:

- Critical Appraisal Skills Programme checklists for:
  - Qualitative Papers
  - Systematic Reviews
- Centre for Evidence Based Management checklists for:
  - Appraisal of a cohort or panel study
  - Appraisal of a cross-sectional study (survey)
  - Appraisal of a case study
  - Appraisal of a meta-analysis or systematic review
  - Appraisal of a qualitative study
- A checklist for the assessment of conceptual papers created from the Journal of Consumer Research's evaluation criteria for conceptual papers (Evaluating Conceptual Papers - Journal of Consumer Research (consumerresearcher.com))and Jaakkola's 2020 paper on designing conceptual articles. See Appendix 2
- A checklist for the appraisal of design science research developed from Hevner et al., (2004) (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.1725&rep=rep1&type=pdf). See Appendix 3

Where more than one checklist was used for an article, the resulting score was averaged out. The final number of studies included in the evidence base was 66. Please see Appendix 4 for a list of the included studies.

4.4 Data extraction and coding

The following was extracted to a Word table for the 66 final items:

- Study author / year
- Research design / type of study
- Sample size
- Setting: this included sector, type of employee
- Highlights / main findings
- Topics covered: using the following codes
  - B – Benefits, C - Consequences, D = Decision-making processes, G – Regulations or other incentives, M – Mitigating risks, O – Organisational conditions, R – Risks
- Whether findings were expected or were actually found in practice
- Research design codes (see Table 3 below),
- Whether qualitative, quantitative, or mixed methods

- A grade for the methodological quality of article, calculated from appraising and scoring each final article against the quality criteria (e.g. novelty, clarity of argument, evidence in support of claims made) for the appropriate checklist (e.g. conceptual article, qualitative paper, cross-sectional study), and presented as a percentage (see section 4.3.2 for checklists and associated rubric).

Research designs as assessed at 5/12/22 (13 papers have 2 codes):

Table 3: Research designs

Research design	**Code**	**Number of papers**
Systematic review or meta-analyses of cross-sectional studies	A	3
Uncontrolled studies with a pre-test	B	0
Cross-sectional studies or a survey	C	28
Case studies	D	10
Case reports	E	0
Traditional literature reviews	F	4
Theoretical papers	G	28
Other	H	6

Quantitative = 31; Qualitative = 26; Mixed methods = 7; Unclear = 2; Total = 66

5. Results

4.1 The benefits of adopting new security technologies

4.1.1 Definition

A 'benefit' is commonly defined as an "advantage, profit, good" (OED) caused by something for someone. The benefits of adopting secure technologies are the positive outcomes of the adoption for the business/organisation implementing the technologies. In terms of business, a benefit can be a tangible good (such as cost savings) or an intangible one (such as improved reputation/brand) that ultimately contributes to achieving the business objectives of the organisation.

4.1.2 Main findings [1]

4.1.2.1 Overview of the evidence

This section reports the main findings related to part of the research question RQ1: 'What are the expected / actual benefits and risks of adopting security technologies?'. **The evidence base for this comprised 29 papers of mixed quality with 15 assessed as of good methodological quality (HQ), 10 as of medium quality (MQ) and four as low (LQ)**. This included articles covering the perceived or actual benefits of adopting secure technologies generally (9 papers), plus papers focused wholly or in part on specific technologies[2] (23). These included cloud computing (10 papers), blockchain (5 papers), biometric authentication (2), cryptography (2), mobile payment systems (1) and Information Security Management Systems (1). Information about specific technologies is covered in Section 4.7. Fifteen of the 29 studies focused on the adoption of technologies within specific sectors: retail-related (3), government (3), banking (3), ICT (2), civil society (1), education (1), manufacturing (1) and finance (1). Thirteen of the 29 focused solely on developing countries, including India (4 papers), the Middle East (Iran (2), Saudi Arabia (1), UAE (1)), Jamaica (1), Bangladesh (1), Mauritius (1), Taiwan (1) and Indonesia (1).

4.1.2.2 Expected benefits of adopting secure technologies

These fell broadly into the following categories, here ranked in descending order of occurrence: reputational benefits e.g., improved image/increased trust in the company; improved financial performance (these first two topics were equally prevalent); risk reduction; and compliance-related. These categories are linked as they can impact one another. For example, there was **good or medium quality evidence** from several papers using different methodologies, that reputational benefits were expected as a result of adopting secure technologies (Berlilana et al., 2021; Gangwar & Date 2015; Donalds & Barclay 2022; Herath et al., 2020). This could lead to increased trust/confidence from customers (Luo & Choi, 2022) and business partners (Gangwar & Date 2015), which could then lead to competitive advantage with the retention of customer loyalty and attraction of new customers (Berlilana et al., 2021), so improving financial performance. There was **high quality evidence** that AoST was also expected to improve financial performance in other ways, including increasing market share due to having secure transaction processes (Berlilana et al., 2021) and decreasing losses due to the prevention of security incidents (Herath et al., 2020). Krishna & Sebastian 2021 (HQ) hypothesised that improvements to the national economy might also come from secure technology adoption. However, this was not later supported by his evidence, although

[1] Please note that the following codes are used throughout: HQ – High quality paper (scored 70% or above), MQ – medium quality paper (scored 50-69%), LQ – low quality paper (scored less than 50%).

[2] Please note there is some overlap between these categories with three of the papers covering both general and specific technologies.

Krishna & Sebastian (2021) claim this may be due to a measurement error. It is interesting that while reputation was the most frequently occurring category, the high-quality evidence focused on the link between AoST and financial performance.

There was **good quality evidence,** unsurprisingly, that AoST was expected to aid risk management leading to better security, risk reduction and fewer successful cyber threats (e.g., Herath et al., 2020 HQ, Gangwar & Date 2015, MQ). Others noted that it would be expected to improve compliance with both legal requirements, and standards and regulations e.g., Donalds & Barclay 2022 (HQ). Berlilana et al., 2021 (HQ), expected that cyber security technology's significant influence on the achievement of both tangible and intangible organisational benefits would be mediated by organisational security readiness, i.e., the willingness and ability of the organisation to change how it actioned security. This is interesting and draws attention to the importance of the right conditions for creating successful information security.

4.1.2.3 Actual benefits of adopting secure technologies

These fell into the same categories as expected benefits, but here there was more evidence for improved financial performance than for reputational benefits, which ranked second jointly with risk reduction followed by compliance-related. The links between finance and reputation were again evident (Berlilana et al., 2021, and Donalds & Barclay 2022). The latter quoted an interviewee as saying:

> "we are in the business of trust, [therefore], if the business cannot prove to [customers, business partners, etc.] that it can handle their data in terms of CIA [confidentiality, integrity, availability], then there is no way [they] will be doing business with us. This in turn impacts revenue and market share." (p67)

Berlilana et al. (2021), found that AoST in practice led to greater customer loyalty, and confirmed that significant positive correlations existed between security adoption and both tangible and intangible benefits.

> "this study also proves that cyber security readiness and technology have a significant influence on the performance of organizational tangible and intangible benefits mediated by organizational security readiness" (p16)

This included improved sales and revenue growth and a better competitive position in the market. El Khoury et al.'s paper (2022) explored the relationship between e-government (the use of digital technology to enable the development of electronic government services, and the exchange of electronic information between government departments and between government and business and government and citizens), business performance (measured by "book value per share, enterprise values, and cash flow" p10) and cyber security using secondary international data from 3,961 IT firms in 34 countries. He found a significant positive association between cyber security and performance, concluding that this:

> "suggests that the development of robust and reliable cyber policies and systems is a prerequisite to better performance" (p17)

As would be expected, AoST led to reductions in data breaches and improved security, e.g., of internal processes (Berlilana et al., 2021), thus improving risk management. Finally, Jackson (2016) found that it improved compliance with organisational requirements.

4.1.3 Conclusion

It can be seen from this analysis that the evidence regarding the expected / actual benefits of adopting secure technologies was of mixed quality. With a tendency to focus more on the possible benefits, rather than demonstrating the realisation of the benefits in practice. This is perhaps not surprising as these technologies are relatively recent. Most papers focused on one specific technology, with cloud computing attracting the most research attention, perhaps because it has been available in a limited form since the 1990s (Shein 2022). Finance-related sectors (retail, finance, and banking) were the most frequently studied. This led to some difficulty in assessing the quality of some articles when data had to be withheld by authors due to commercial confidentiality. This issue has been carefully considered in assessments. Key benefits identified for adopting secure technologies were reputational, financial, risk-related, and compliance-related, with reputational being of less importance than had been expected, and impact on financial performance being of greater (actual) importance.

4.2 Risks involved in the adoption of security technologies

4.2.1 Definition

A risk is defined as "1. (Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility. Frequently with *of*." (OED). Risk can also be seen more neutrally as anything leading to unexpected outcomes which could be positive or negative (Cagliano et al., 2015). For example, a policy change may be unexpected but turn out to be beneficial (a risk with a positive outcome). However, in these papers the term risk is only used as having negative connotations.

Sivan-Sevilla (2021), following Fichtner, 2018 and other authors, saw risks as involving "threats, reference objects, judgement of the seriousness of the problem, and practices to deploy" (p696) He argued that institutional structures, values, and policies will cause variance in the meaning organisations place on this, stating:

> "scholars have found variance in the way these risks are framed and governed across policy domains and political systems." (p697)

This emphasises the importance of context when discussing risk. It also, again, shows the interrelated nature of our topics: what the risks are seen to be and how they are prioritised depends on decision making around risk framing, which is affected by institutional conditions (in the widest sense, including national structures) and policies. These in turn would be influenced by regulations and incentives. Therefore, this section needs to be considered in the context of the other findings.

4.2.2 Main findings

4.2.2.1 Overview of the evidence

This section reports the main findings related to part of the research question RQ1: 'What are the expected / actual benefits and risks of adopting security technologies?' but focuses on unexpected risks found in practice in the existing literature rather than common ones, as expected risks have been well covered elsewhere (see Section 4.2.2.2). **The evidence base for risk as a whole comprised 35 papers of mixed quality with 16 assessed as of good methodological quality, 12 as of medium quality and 7 as low.** This included articles covering the risks of adopting secure technologies generally (21 papers), plus papers focused wholly or in part on specific technologies (14), notably cloud computing (9), block chain (4) and smart cities (1). There is very little overlap between these categories with only one paper covering both general and specific technologies. Risk in relation to specific technologies is dealt with in Section 4.7. Sixteen of the 35 studies focused on the adoption of technologies within specific sectors: banking (3), government (3), oil and gas (2), ICT (2), health (1), energy (1), education (1) civil security (1), home security (1) and retail (1). Fifteen of the 35 focused only on developing countries, including the Middle East (UAE (2), Saudi Arabia (1), Qatar (1) and Iran (1)), India (4), Jamaica (1), Bangladesh (1), Korea & China (1), Korea only (1) and Mauritius (1).

4.2.2.2 Introductory remarks about the risks of adoption of new security

Before focusing on unexpected risks, it needs to be acknowledged that there are many risks of different types (e.g., technological, environmental, human, organisational) that can affect the adoption of any secure technology, which have been well covered in the literature and are likely to be routinely expected and identified as part of a risk assessment. These include, for example:

1) Inadequate risk assessment and planning which fails to highlight problems in advance

2) Fear of change
3) Lack of funds
4) Seeing security as a threat to functionality
5) Loss of, or difficulty accessing, necessary technical skills
6) Lack of resources including network and other infrastructure
7) Insufficient time for staff familiarisation
8) Inadequate training
9) Other priorities remaining unfunded
10) Cyberattacks increasing while there is a knowledge gap in the time before staff get up to speed
11) Risks caused by new essential partnership arrangements

(For evidence in support of these risks see e.g., Luo & Choi 2022, Donalds & Barclay 2022, Armenia et al., 2021, Qian et al., 2012, AlAbdulkarim & Lukszo 2010, Cannoy & Salam 2010, Kefallinos et al., 2009). Material covering expected risks can also focus on specific technologies (e.g., Swamy 2013 on cloud computing, p75-77) or sectors (e.g., Kefallinos et al., 2009 on e-government, p82-85)

Failure to adopt and/or fully implement the new security technology may in turn lead to reputational and financial losses, data breaches and failures of compliance as discussed in the benefits section.

Risks can also be expected to interrelate (Lee et al., 2016, AlAbdulkarim & Lukszo 2010) and to impact on other cyber systems in a ripple effect (Lee et al., 2016, AlAbdulkarim & Lukszo 2010, Jackson 2016). There is a need for holistic, systemic assessment of risks rather than siloed approaches (Damenu & Beaumont 2017, Cannoy & Salam 2010), with non-technical factors now acknowledged as being as important as technical ones (Al-Darwish & Choe 2020). Risks also change over time as new threats develop, so the process of dealing with them should never be viewed as a one-off event (this in itself forms a risk to cyber security, according to Sivan-Sevilla 2021).

4.2.2.3 Unexpected risks of adopting new security technologies

This section explores some of the unexpected actual risks of adopting new security technologies in general. These were found in the literature and presented as unexpected by the company/organisation or the researcher. They have been divided into the following categories:

1) Technology
2) Organisational
3) Environmental
4) Human or actor-related factors [3].

The **evidence quality is mixed** with 7 papers categorised as high quality, 3 as medium quality and 4 as low quality.

TECHNOLOGY FACTORS

These are factors specifically relating to the technologies, both those available and those already in situ and the risks they pose. Clearly, these will vary according to the hardware/software involved but the following points were noted: Lee et al., 2016 (HQ) found an unexpected inadequate attention to uncertainty in technology road-mapping, contributing to the idea that risk assessment and

[3] Technology-organisation-environmental factors form a common technology adoption model used by many authors in the full evidence base (e.g., for use with risk see Raut et al., 2018, Khayer et al., 2021, Priyadarshinee et al., 2017 & Chiniah et al., 2019, all in relation to cloud computing).

management is not a one-off activity but a process that needs repeating as it is impossible to predict when new risks will arise. This also supports the argument for becoming 'futures literate':

> "avoid[ing] placing undue emphasis upon the predictability, certainty, unity, or clarity of the future… this involves resisting the assumption that present and historic trends are inevitable and will continue (chronocentrism)…This means looking beyond the future as a continuation of the recent past and present" (Liveley & Coles-Kemp, 2022, p10).

Al-Darwish & Choe 2020 (LQ) noted that there was inadequate closure of risk exposure gaps, with emphasis on resolving technical problems in quantity rather than quality. Groner & Brune 2012 (LQ) also provided evidence for inadequate security awareness due to technical complexity amongst German SMEs:

> "In particular, the study revealed that important IT security solutions like single sign-on and multi-factor authentication still suffer from a comparably low adoption due to their technical complexity and high implementation costs" (p86)

ORGANISATIONAL FACTORS

Organisational factors are those that relate to the nature or activities of organisations including business aims, structure, culture. Schinagl & Shahim 2020, (MQ) found that organisations did not adequately follow the principles of High Reliability Organisations, and that risks included:

> "ignoring problems until they grow unavoidable, mistaking security policy/compliance with operational reality, relying on oversimplified risk management tools and security frameworks, and inadequately preparing for security events and incidents." (p281)

Again, this indicates the importance of planning ahead and thinking beyond immediate adoption and implementation. Armenia et al. (2021), Donalds & Barclay (2022), Lee et al., (2016) and Anderson (2010), all noted the importance of correct assessment of risks. This should not be a one-off process (Lee et al., 2016) and again requires a holistic approach:

> "The accuracy of risk estimates heavily depends on establishing linkages between processes, resources and organizational objectives, insights into the interdependence of systems, and a comprehensive perspective of enterprise-wide…services" (Anderson 2010, p2)

ENVIRONMENTAL FACTORS

Environment refers to the organisation and industry's environment:

> "Environment relates to those operational facilitators and inhibitors; significant among them are competitive pressure, trading partners' readiness, socio-cultural issues, government encouragement, and technology support infrastructures such as access to quality ICT consultants (Jeyaraj et al., 2006; Zhu et al., 2003; Al-Qirim, 2006)" (Awa & Ojiabo 2016, p905).

There was only a small amount of evidence for unexpected environmental risks. Schinagl & Shahim (2020) noted new risks arising with outsourcing and distributed infrastructures (as in the case of cloud computing), including compatibility issues and security risks. This could occur as responsibility remains with the originating business, although control of the infrastructure is shared with the external service provider. This was supported by Thalmann et al., (2014), in a high-quality study, (not included here as it is of software only).

HUMAN FACTORS

These are people-related factors, risks caused by human responses to / interaction with new security technology adoption. Human risks can begin from well-before implementation. The perception of risk varies with different individuals and stakeholder groups (Groner & Brune 2012) and these groups will have different levels of influence over the adoption agenda. Failure to correctly perceive and identify the risks, threats, system & data needed when planning can lead to decision-making failures from the beginning (Armenia et al., 2021, Donalds & Barclay 2022) which will clearly be unexpected for the organisation. Anderson (2010) also noted the unexpected underestimation of risk brought by a network of multiple diverse technology and partners, an issue that spans both technology and human factors.

4.2.3 Conclusion

This section has focused on risks that were unexpected. Risk in this body of evidence is primarily viewed by the authors as negative and something to be avoided. Risks may be framed in different ways to meet the different priorities of different organisations; therefore, certain types of risks will be more important to some than others. It is not possible to say what the most important risks are as each organisation needs to assess this in context. There was some emphasis on the importance of planning ahead and developing ways to deal with uncertainty as this is inevitable. There is clear evidence that it is necessary to take an approach to risk assessment and mitigation that is both ongoing (risk should not be a one-off activity) and holistic (including consideration of all four categories and recognising that risks may interrelate). Several authors emphasise that technological problems should not be the sole focus and that organisational, human, and environmental risks are all important, e.g.,

> “It is generally accepted that success is less about selecting the right technology and more about managing organizational capabilities, facing regulatory constraints and environmental pressures and anticipating social, political and psychological issues of people involved; in other words effectively assessing risks and governing technological structures, within context” (Kefallinos et al., 2009, HQ, p73)

Organisational factors in particular have not received adequate attention in organisations in the recent past which can lead to very serious issues. Topics covered in the Organisational Conditions and Organisational Consequences sections (Section 4.5 & 4.6) offer ways to mitigate risks.

4.3 Cognitive decision-making processes that are utilised and shared in adoption discussions, policy, or processes

4.3.1 Definition

Decision-making is defined as follows:

> "to decide; to come to a judgement, conclusion, or resolution" (OED)

Many different models of the process exist (e.g., Taherdoost 2018 or Alshammari & Rosli 2020). It is common to find steps like these in them:

1) assess and evaluate the problem/ issue to be addressed and purpose of the decision-making
2) establish goals
3) gather information, define options
4) evaluate the options
5) make the decision, select amongst the options
6) implement the decision
7) monitor & evaluate the outcomes

Orlikowski (1992) talks about two phases of adoption, a) design and b) use with additional possibilities for re-design, which she uses for the purpose of analysis in relation to technology adoption. Both will clearly involve decision-making and will be covered in this section.

4.3.2 Main findings

4.3.2.1 Overview of the evidence

This section reports the main findings related to research question RQ2: 'What cognitive decision-making processes are utilized and shared in [organisational] adoption discussion, policy or process?' **The evidence base for this comprised 26 papers of mixed quality with 11 assessed as of good methodological quality, 10 as of medium quality and five as low**. This included some articles covering decision-making in relation to specific technologies (12), notably cloud computing (8 papers), but also biometric authentication (2), blockchain (1), and mobile payment systems (1). Five of the 12 articles also comment on general technology. Six of the 26 studies focused on the adoption of technologies within specific sectors: finance (2), e-banking (1), health (1), ICT (1) and retail (1). Fourteen of the 26 focused only on developing countries, including the Middle East (Saudi Arabia (2), no specific country (1), UAE (1) and Iran (1)), India (2), Jamaica (1), Bangladesh (1), China (2), Korea and China (1), Mauritius (1) and Taiwan (1). Decision-making in relation to specific technologies is dealt with in Section 4.7.

4.3.2.2 Decision-making processes

A substantial proportion of the evidence base focused around the factors that need to be considered when adopting new security technology (see Section 4.3.2.3) rather than the evaluation process as such or the decision-making process as a whole. However, two papers (both MQ) did discuss these. Laux et al., 2011 briefly defined the innovation decision-making process as involving:

> "a series of choices and actions that are taken over time and through which individuals or organizational members evaluate a new idea and decide whether to incorporate the innovation into ongoing practices (Rogers 2003). The decision stage of the innovation-decision process is the point at which an organization adopts or rejects an innovation" (p226)

This draws on Rogers' 'Diffusion of Innovations' theory (2003). The authors also drew attention to other research on the adoption of innovations but again focusing on the factors affecting decisions. It should be noted that this paper focused on biometric authentication.

Goldman (2012) explored the decision-making process in relation to new technology in greater detail, obtaining the views of 15 IT decision-makers in SMEs. He argued that improvements in IT acquisition decisions lead to improvements in an organisation's security approach:

> "Whether or not decision criteria are security specific, poor acquisition decisions may result in future problems implementing security controls or integrating security technologies (e.g. monitoring) within existing infrastructure." (p351)

The paper stated that although most participants did not follow a standardised decision-making procedure they did have "a fairly regular/defined process" (this was not specified). He argued against reliance on heuristic decision-making and was in favour of a considered approach.

> "[Using an] ongoing process refinement and formalization (e.g., checklists, baselines) can increase the probability of success. In addition, consideration of decision making as a process (Zeleny, 1981) and the utilization of multi-stage, multiple-perspective strategies can reduce the loss of fidelity that frequently accompanies heuristic approaches" (p351-2)

Different aspects of making decisions covered included:

- Analysing requirements

- Using good quality sources of information:

  "quality of acquisition was determined by factors including utilization of quality research sources, weighing multiple options, and learning from previous acquisition projects" (p351)

This included using good quality information to decide on a vendor and to establish a sense of trust, as well as good communication with them. Appropriate information sources should be used, without reliance on peer recommendations, marketing material or search engine results. He noted that in practice "many participants often gave a boost to well known, mainstream options, without a thoughtful explanation" (p355). Instead, he advised that "prudent participants noted a reliance on specialized, objective, and/or evidence-driven resources" (p355). Failure to develop trust and to establish good communication, both internally and with the vendor, was presented as one of two common sources of failure for projects, alongside lack of evaluation and testing. Goldman stated that users should be engaged and involved from the beginning.

- Setting goals and decision criteria. (He notes common criteria as being: "[provides] the desired functionality, ease and cost of management, usable operating interface, and solutions that were generally "simpler."" (p355))

- Planning: Goldman noted that it was common to find a lack of planning and that that meant a lack of guidance which hindered the decision-making process.

- Risk assessing: some participants required risk assessments to be carried out or had security policy requirements that set out acquisition requirements. However:

> “security was generally addressed only in the technical domain, without regard for risk control in accordance with business requirement” (p359)

- Business case development
- Familiarisation, evaluation, and development of training

After the decision and before implementation, Goldman (2012) found that users tended to test and evaluate their choice, e.g., in a sandbox environment, and that they also developed customised training and documentation to aid staff. He noted an absence of other planning that could have helped:

> “Less common was the development of change plans that might include implementation timelines, process impact analyses, and policy implementations. We noted that approaching acquisition as a project in general provides greater structure to the process and consideration of more variables” (p356)

Goldman (2012) noted that acquisition failure could be hard to undo, as faulty components or processes became embedded over time:

> “organizations were often unmotivated or lacked time and resources to evaluate new options. Consequently, participants reported they would continue to use faulty components and often had to re-engineer processes or develop other workarounds to continue operations; such measures (often complex or inconvenient) would often negate any advantage that could have been gained by implementing the new component.” (p356)

This shows that technology and human factors influence one another: the technology is too established to appear changeable which limits human achievement of the benefits possible through it. Therefore, participants respond by creating ‘workarounds’, altering the technology and affecting their practice (see Orlikowski 1992’s structurational model of technology).

Goldman (2012) indicated reasons why improvements in acquisition of IT improved security posture:

> “Both require critical, analytical thinking – if an organization is unwilling or unable to devote time and resources to building business cases and analyzing requirements, critical information also may not be considered. As a result, an acquired component or a security process might fail to meet its business purpose or may disrupt other components or processes…If an acquisition does not consider the total environment or future considerations, it may be difficult to integrate security features later (Chung and Nixon, 1995).” (p360)

Recommending project management training to aid the process, he concluded that:

> “organizations should avoid performing these processes ad hoc or reactively. Instead, orderly, repeatable, and measurable procedures should be developed to guide this process” (p361)

4.3.2.3 Factors requiring decisions

As the Goldman (2012) paper suggested, decision-making requires careful thought about multiple factors including the categories of technological, human, organisational and environmental factors discussed in the preceding sections, and the material in the Organisational Conditions section (4.5) where the specific factors are explored. There was overall agreement for this in the evidence base e.g., Sivan-Sevilla 2021, Wu & Saunders 2011, Ihmouda et al., 2015. These are all HQ or MQ papers. There was also much research done on the different factors, with no agreement on the most important. Several authors placed human factors as the most significant. Anderson 2010 (MQ) pointed out, for example, that:

> "Even in the presence of shared information and organizational contexts and circumstances, managers may arrive at very different conclusions concerning the level of resources that should be devoted to security because of differences in priorities, motivations, incentives, and value systems. While the information content of risk assessments is variable, so are the interpretations and responses thereto" (p2)

This is also relevant to organisational conditions of interaction with security technologies. How risk is conceptualised / framed is key and depends on the priorities and values of the human actors involved as well as those of the organisation. Donalds & Barclay 2022 (HQ) also identified value setting and value focused thinking as important. Goldman 2012 (MQ) argued that small organisations should focus on the human element first and stated that:

> "Instead of relying on technology (e.g., firewalls), gains in security posture [ability to identify, respond to and prevent attacks] may be more effectively realized by investing in training, as well as by improving attitudes and processes throughout the system development lifecycle (SDLC)." (p350)

Bu et al., 2021 (MQ) presented evidence for the importance of attitudes, stating that it is important to build positive ones and to ensure adequate understanding of factors including performance and effort expectancy as these significantly influence attitude. Attitude will impact behavioural intention and therefore actual behaviour.

Others found organisational factors to be the most important for consideration. For example, Sivan-Sevilla's 2021 study (HQ) found that in practice organisational factors were more important than the way risk was framed:

> "variance stemmed from the institutional configurations in each regulated sector and the consequent decision-making structures that had been institutionalized early on, rather than the framing of cyber risks" (p694)

He provided information about decision-making structures and actors in three sectors, finding that, in each case subsequent developments were determined by previous policy paths. The actors both drew on what had gone before, and in so doing reinforced it, with the technology embedding in both the existing and changed policy context. Others who highlighted organisational factors included Khan et al., 2019 (HQ) Priyadarshinee et al., 2017 (MQ) (both in relation to CC) and Laux et al., 2011 (MQ) (in relation to biometric authentication) who noted that:

> "Security spending decisions like other IT initiatives must align with the highest priorities and missions of the organization "(p6)

Gokalp et al., 2022 (HQ), found environmental factors to be more important than either technical or organisational for the adoption of blockchain in supply chain management. Riley et al., 2009 (LQ) also rated environmental factors as important for biometric technology, arguing for consideration of cultural differences in perceptions, such as national levels of uncertainty tolerance or decision structures. Alizadeh et al., 2020 (MQ) thought technical factors the most important for the adoption of cloud computing in e-banking, followed by environmental, human, and organisational. Fu et al., 2022 (MQ), also found technical factors more important than either organisational or environmental, in relation to mobile payment systems.

Overall, this suggests the need for a holistic approach that takes account of all categories of factors but assesses these in the light of the particular context and technology involved.

4.3.2.4 Actors in decision-making

Wu & Saunders 2011, (HQ) explored decision-rights allocation, arguing for its importance, and providing a framework to aid it, so that the right people are involved in the types of decisions they are best qualified to adjudicate on.

> "This framework recommends the selection of decision rights allocation patterns that are proper to [particular] decision types to ensure good security decisions" (p28)

Decision-making is not a one-off process:

> "while adoption of IT is, indeed, oftentimes a strategic decision, it is never a one-off decision because the outcome of the decision and its implementation, i.e., new affordances and constraints, generate further needs for another round of IT adoption decisions." (Wang et al., 2021, p10 (HQ))

Additionally, employee decisions to implement technology to the full are as important as the decisions to adopt the new security system in the first place. There was strong research interest in the issue of obtaining employee compliance. Balozian et al., 2019 (HQ), looked at what motivated employees to comply and found that this differed amongst employee types:

> "Our results suggest that participation in the ISP [information security policy] decision-making process might prove to be a more effective approach to motivate lower-level employees toward compliance [but]…enhancing the meaningfulness of policy compliance could be the preferred method among higher levels of management." (p197)

Donalds & Barclay 2022 (HQ), and Alqahtani & Erfani 2021 (MQ) also looked at factors affecting compliance, the latter finding that:

> "effort expectancy, social influence, habit and hedonic motivation have significant impact on cyber security compliance in organizational perspectives" (p56-7)

4.3.2.5 Decision-making models/tools/methods

The evidence base provided many examples of technology adoption decision-making models, methods, or tools, created using different theoretical perspectives. For example, Lee et al., 2016 (HQ) looked at uncertainty in technology road-mapping, an important topic given that some future risks are inevitably unknown. They provided a tool for use in the follow-up phase of adoption which could help to model future conditions and assess ripple effects on organisational plans. Armenia et al., 2021 (HQ) offered a tool to aid risk evaluation and planning around cyber security investment decisions. It enabled assessment of the organisation's cyber-posture and then modelled the effects of diverse investment strategies. The tool could be used over time not just for decision-making about initial adoption. Donalds & Barclay 2022 (HQ) offered 30 objectives to assist with employee compliance and advocated Value Focused Thinking given that:

> "the determination of values is a critical step in the strategic decision-making process" (p62)

Tafokeng Talla & Robert 2019 (LQ) developed a theoretical model for assessing the factors influencing decisions around the adoption of information security, and Cannoy & Salam 2010 (LQ) provided a framework for information assurance policy compliance in health.

4.3.3 Conclusion

Overall, **the evidence for decision-making processes used and shared in the adoption of new security technology was of mixed quality** and focused mostly on the factors that need to be considered rather than the different cognitive processes themselves. There was no consensus amongst authors as to which type of factors were the most significant. Several new tools/frameworks were presented to help with assessing these factors. The emphasis on critical factors was also true for research focused on specific technologies.

The chief exception to the above was Goldman's 2012 work around the link between acquisition decisions and security posture, where different decision-making processes were discussed. He argued for the avoidance of ad hoc decision making and in favour of "orderly, repeatable, and measurable procedures" to guide the process. Several decision-making steps were extrapolated from the paper including analysing requirements, setting goals, planning, risk assessment, developing a business case, training, and documentation development. Goldman also argued for the importance of selecting and using high quality information.

4.4 Regulatory and other incentives required to facilitate the process of security technology adoption

4.4.1 Definitions

Lam & Seifert in a useful report on the UK regulations relevant to the adoption of security technologies stated that:

> "Protecting firms and consumers from…costs relies on the availability of effective technological defences, but also on the incentives of firms to develop and implement these new technologies, and of consumers to adopt secure behaviours with respect to their personal data." (2021, p6)

This includes regulations which here signifies:

> "A rule or principle governing behaviour or practice; *esp.* such a directive established and maintained by an authority." (OED)

Regulations include national and international legislation, societal norms governing behaviours and regulations imposed by a particular sector in order to be allowed to operate within it. This forms part of the external environment influencing the adoption of technology. There are also other types of incentives, e.g., personal incentives such as the desire to increase knowledge or to 'do the right thing', that can influence adoption of technology (Khan et al, 2019).

4.4.2 Main findings

4.4.2.1 Overview of the evidence

This section reports the main findings related to research question RQ3: 'What regulatory and other incentives are required to facilitate the process of security technology adoption?' **The evidence-base for this comprised 29 papers of mixed quality with 13 assessed as of good methodological quality, 12 as of medium quality and 4 as low.** This included articles covering regulation and incentives generally (13 papers), plus papers focused wholly or in part on specific technologies (16), notably blockchain (7) and cloud computing (5 papers); but also mobile payment systems (2), 5G (1), and biometrics (1). (Please note there is some overlap between these categories with some papers covering aspects of both general and specific technologies.) Fourteen of the 29 papers were set in specific sectors including e-government (4), banking (3), ICT (2), finance (1), e-commerce (1), retail (1), manufacturing (1) and health (1). Eleven of the 29 were set in non-Western contexts including UAE (2), China/Taiwan/Hong Kong (1), China only (1), Taiwan only (1), Lebanon (1), Iran (1), Saudi Arabia (1), Jamaica (1), India (1), and Mauritius (1). Regulations and incentives for specific technologies are dealt with in Section 4.7

4.4.2.2 Regulatory incentives

Laws will vary by nation: "governments all around the world take different measures for cyber-security-related challenges" (Luo & Choi 2022, p2108 (HQ). See also Schinagl & Shahim 2020 (MQ), and Kefallinos et al., 2009 (HQ)). This could become confusing and problematic when services cross jurisdictions:

> "Unclear or contradictory laws and regulations, balances among the executive, legislative and judicial branches, or negative norms and behavior can constrain efforts and lead to

> resistance to change and internal conflicts" (Kefallinos et al., 2009 p79. This is also **supported by low quality evidence** from Dhillon et al., 2016)

Radu & Amon 2021 (MQ) similarly found supra-national bodies taking differing approaches, e.g., the European Union and the 5 Eyes approach to the adoption of 5G. Kefallinos et al., (2009) noted the importance of "Formal and unambiguous jurisdiction assignment" p84. Goldman 2012 (MQ) reported that participants often had difficulties ascertaining which regulations applied to them with one participant suggesting a "'clearinghouse' or organization that provides a firm list of all specific requirements that apply to your organization" (p358). He also noted that there was little use of legal professionals to help with this although this could add clarity.

Regulations were seen as a powerful encouraging or constraining influence on the adoption of security technology e.g., Goldman 2012 (MQ), Cannoy & Salam 2010 (LQ). In terms of compliance Donalds & Barclay 2022 (HQ), Goldman and Cannoy & Salam, noted government regulations as key drivers:

> "All of our respondents mentioned government regulations such as HIPAA as the main driver for implementing formal compliance policies." (Cannoy & Salam 2010, p127)

Governments could undertake various actions to aid adoption and compliance other than passing direct legislation. For example, they could:

- Promote the benefits of new technologies: Clohessy & Acton 2019 (HQ), Fu et al., 2022 (MQ)
- Adopt the technologies themself so effectively promoting them: Clohessy & Acton 2019 noted that the adoption of CC increased once the government had taken it on
- Offer incentives: Clohessy & Acton 2019, Fu et al., 2022, Li 2015. For example, Li 2015 suggested governments could help e-tailers with financial support for adopting mobile payment systems: "sponsoring the e-tailer to cover a part of the fixed cost of using technologies." (p2120)
- Pass indirectly supportive legislation: laws that may not mandate technologies, but can encourage their adoption or implementation:

> "Six of the interviewees pointed out that the newly enacted GDPR triggered their organizations to adopt or consider blockchain technology to ensure compliance with the new data protection laws" (Clohessy & Acton 2019, p1479. See also Gokalp et al., 2022)

- Provide clarity about forthcoming legislation affecting a technology. Gokalp et al., (2022) noted that:

> "Organizations desire to be prepared if the market imposes policies and regulations based on blockchain, and the fear of "if policies and regulations are not established" is a barrier in front of the adoption of blockchain-based technologies (Holotiuk & Moormann, 2018)." (Gokalp et al.,2022, p110. See also Clohessy & Acton 2019)

Whilst the above examples all refer to specific technologies, these points are very likely to be true of other similar technologies.

Different sectors, like different governments, had different regulatory bodies, requirements, power structures, norms, reporting and audit requirements. Some were more highly regulated by the government than others (see e.g., Sivan-Sevilla 2021 (HQ), Donalds & Barclay 2022 (HQ), Goldman 2012 (MQ). Goldman 2012 and Donalds & Barclay 2022 noted that sectors that are highly regulated are more likely to be security conscious and to apply stricter sanctions internally. Sivan-Sevilla 2021 (HQ) found that government approached the governance of three sectors (health, finance, and non-critical industries) differently because of path dependency, despite equivalent levels of present risk. He showed that past human activity (in terms of previous legislation and policy development) had determined sectoral policy rather than the actual need called for by the existing level of risk.

> "For each regime, the government tried to improve risk management practices without diverging from previous policy paths considerably… health and financial industries encounter the increasing monitoring and enforcement capacities of top-down regulators. Non-critical sectors are still governed based on incentives and completely self-regulatory models, despite evidence-based hazard estimations and the perceived seriousness of the risk" (p716)

4.4.2.3 Financial penalties and rewards

Financial incentives (including impacts on financial performance) had an important role to play, and could be positive or negative, i.e., they could take the form of benefits that encouraged adoption and compliance with new security technology, or penalties that discouraged non-adoption or lack of compliance. Positive incentives included:

- Improvements to reputation which attracted customers
- Attaining competitive advantages, so maintaining or increasing market share
- Avoidance of penalties and fines

Negative incentives included:

- Risk of financial losses
- Damage to reputation
- Costs of repairs to system damage
- Loss of trust with partners, suppliers and customers and possible loss of contracts
- Reductions in stock price and shareholder value
- Penalties and fines

(Sivan-Sevilla 2021, Donalds & Barclay 2022. Both HQ)

Luo & Choi 2022 (HQ) discussed government penalty schemes and when these can actually be harmful. They developed a formula for when and how to use them:

> "If the benefit brought to consumers with the use of systems security enhancing technologies (such as blockchain) is greater than the per unit technology operations cost, and the fixed technology cost is relatively small, the adoption of technologies will be a good choice… the presence of systems security enhancing technologies also affects the optimal penalty" (p2123)

If penalties were to be implemented, then the penalty needed to be very harsh to be effective. Where financial measures were not appropriate, Luo & Choi (2022) advocated alliances between e-tailor and suppliers. Koskosas 2011 (MQ) noted bonus schemes as useful for introduction of new technology to timescale.

4.4.2.4 Social influences

Customer requirements e.g., around privacy provided important incentives e.g., Kefallinos et al., 2009 (HQ), Goldman 2012, and Schinagl & Shahim 2020 (both MQ).

> "Companies must put cyber security and privacy at the forefront of their business strategy to win the customers' hearts and to earn their trust" Schinagl & Shahim 2020, (p280)

This, of course, ultimately links with the protection of business reputation. Liu et al., 2020 (MQ) found that personal relationships within the workplace between supervisor and subordinate could also motivate compliance with information security directly, and indirectly via organisational commitment.

Krishna & Sebastian 2021 (HQ), Schinagl & Shahim (2020) and Alqahtani & Erfani (2021) (both MQ) found that the requirements of business partners were important incentives. Alqahtani & Erfani (2021) identified “social influence and habit [as] the strongest predictors of cyber security compliance by general users in organizational settings.” (p57).

Regardless of financial consequences, the need to keep up with peers, market leaders and the norms and requirements of an industry was noted as an incentive by Krishna & Sebastian (2021) and Herath et al., (2020). (Herath et al.’s 2020 findings both expected to find, and did find, this in practice).

4.4.2.5 Personal incentives

Alqahtani & Erfani 2021 (MQ) found that hedonic motivation was a moderate predictor of improved cyber security compliance in organisations. Balozian et al., (2019) provided **high quality evidence** that the effectiveness of incentives varies according to employee management level. His research “reveals that different levels of users may be affected by different types of coercive and empowering techniques regarding ISP compliance.” (p204). However, it should be noted that he assessed intention to comply not actual compliance.

4.4.3 Conclusion

The evidence for regulatory and other incentives required to facilitate security technology adoption was of mixed quality. Government regulations / support appeared to be the most important factors facilitating adoption with uptake because of social pressures next. There was little evidence about direct financial incentives, although indirect ones are effective. Government activity could go beyond the passing of legislation to encompass other forms of encouragement. Regulation was seen as the most important factor across specific technologies also. It would be interesting to examine how soft organisational level policies reflect or complement regulations for compliance or other purposes. Finally, again, there is no one-size-fits-all in terms of staff incentives.

4.4 Organisational conditions

4.5.1 Definitions

A ‘condition’ here indicates “Something that must exist or be present if something else is to be or take place; that on which anything else is contingent; a prerequisite” (OED). Here an organisational condition signifies a factor that will facilitate the adoption and implementation of new secure technologies. It may also mitigate risks. Mitigation signifies “…abatement or minimization of the loss or damage resulting from a wrongful act.” (OED 2a). Risk mitigation involves preparation for, and reduction of, the impact of risks on an organisation: it is “The practice of limiting risk exposure and reducing the chance of an incident” Difference between Risk Mitigation and Risk Management (linkedin.com) It also includes work after a risk has occurred to lessen the harms from it. (Organisations able to do this are sometimes referred to as ‘resilient’). This may be by ensuring that certain organisational conditions are put in place in advance of adoption or post implementation. Four types of risk mitigation strategies are often mentioned: risk acceptance, avoidance, limitation & transference.

4.5.2 Main findings

4.5.2.1 Overview of the evidence

This section reports the main findings related to part of research question RQ4: ‘What are the organisational conditions and consequences of adopting new secure technologies?’ **The evidence base for this comprised 56 papers of mixed quality with 24 assessed as of good methodological quality, 24 as of medium quality and eight as low.** This includes articles covering organisational conditions for adoption in general and 20 papers covering specific technologies, notably cloud computing (8 papers), but also blockchain (5), biometric authentication (4), mobile payment systems (1), smart cities (1) and 5G (1). Twenty-six of the 56 studies focused on the adoption of technologies within specific sectors: government (6), banking (4), ICT (3), retail-related (3) oil and gas industry (2), finance (1), manufacturing (1), civil security (1), hospitality & tourism (1), home security (1), energy (1), education (1) and health (1). Twenty-two of the 56 focused only on developing countries, including: India (4), China (3), UAE (2), Saudi Arabia (2), Iran (2), Jamaica (1), Bangladesh (1), Mauritius (1), Lebanon (1), Qatar (1), Malaysia (1), Indonesia (1), Korea (1) and Taiwan (1). Organisational conditions in relation to specific technologies are dealt with in Section 4.7

4.5.2.2 Conditions

These are discussed in descending order of prevalence, but it should be noted that importance in practice may vary according to the organisation, setting and technologies involved. There was no consensus amongst the authors as to the most important organisational conditions.

Organisational instruments: frameworks, models, sets of standards, codes of practice, policies

Much of the evidence discussed original or existing organisational instruments in the form of frameworks/models etc. for governance and security. These set out components of good information security governance, identifying what needs to be in place for the successful adoption and implementation of new security technologies.

In terms of existing standards / frameworks, Kefallinos et al., 2009 (HQ) suggested using:

- ISO/IEC 27002:2005 ‘Code of Practice for Information Security Management’ (ISO/IEC, 2005b) describing it as “is the only security-specific international ITG standard available” p78.
- COBIT (Control Objectives for Information and Related Technologies) framework

- ITIL (The Information Technology Infrastructure Library) set of best practices

Schinagl & Shahim 2020 (MQ) offered descriptions and assessments of existing models/frameworks grouped by the types of approaches to governance they identified (see Section 4.5.2.3). They also analysed process-oriented frameworks looking at governance over time, and cyber-system-specific ones. They concluded that there was no general agreement on a model, one size does not fit all, models need to be tailored to the organisation, and that:

> "A paradigm shift is required to move from internally focused protection of organisation-wide information towards an embedded and resilient view that considers an organisation's collaborative business environment (Horne et al., 2017; Kauspadiene et al., 2017)." (p272)

This needs to be embedded from an early stage, as with digital-security-by-design. See Da Veiga & Eloff 2007 (MQ) for other information governance security frameworks and Ihmouda et al., 2015 (MQ) for a list of information security effectiveness models.

New frameworks and models for different aspects of information security governance were put forward by many authors in the review:

Frameworks

- Information security governance frameworks: Da Veiga & Eloff 2007, Damenu & Beaumont 2017 (both MQ) Wu & Saunders 2011 (HQ)
- Information security culture frameworks: Al Hogail 2015 (MQ)
- Information security assurance and compliance frameworks: Cannoy & Salam 2010 (LQ), Alabdulkarim & Lukszo 2010 (MQ)
- Frameworks for assessing organisational security: Pathari & Sonar 2013 MQ
- Frameworks of factors affecting cyber security readiness: Berlilana et al., 2021 (HQ)

Models

- Models of factors affecting the adoption of security technology: Herath et al., 2020, (HQ), Tafokeng Talla & Robert, 2019 (LQ)
- Model for managing information security risks during new technology adoption: Qian et al., 2012 (HQ)
- Model of factors affecting cyber security: Rajan et al., 2021 (HQ)
- Model for developing an IT security infrastructure framework: Groner & Brune 2012 (LQ)

Miscellaneous (all high-quality evidence)

- Ranked list of elements for allocating roles and responsibilities for IT controls: Khan et al., 2019
- List of 30 objectives for maximising compliance with IS policies: Donalds & Barclay 2022
- Risk assessment tool for e-governance projects at implementation: Kefallinos et al., 2009

The components discussed in the following sub-sections frequently appeared within these frameworks / models as being important to the successful implementation of cyber security, information security governance and technology:

- education and training: Khan et al., 2019 (HQ), Gangwar & Date 2015 (MQ), Damenu & Beaumont 2017 (MQ), Da Veiga & Eloff 2007 (MQ), Al Hogail 2015 (MQ), Cannoy & Salam 2010 (LQ)
- information security strategy: Gangwar & Date 2015, Damenu & Beaumont 2017, Da Veiga & Eloff 2007, Al Hogail 2015, Cannoy & Salam 2010

- security policies and procedure: Gangwar & Date 2015, Damenu & Beaumont 2017, Da Veiga & Eloff 2007, Al Hogail 2015, Cannoy & Salam 2010
- information security culture: Gangwar & Date 2015, Damenu & Beaumont 2017, Da Veiga & Eloff 2007, Al Hogail 2015
- leadership, management support: Damenu & Beaumont 2017, Da Veiga & Eloff 2007, Al Hogail 2015
- relevant information security / incident response processes: Damenu & Beaumont 2017, Da Veiga & Eloff 2007. This included:
    - risk management and assessment program: Gangwar & Date 2015, Damenu & Beaumont 2017, Da Veiga & Eloff 2007, Khan et al., 2019
    - compliance and standards: Gangwar & Date 2015, Damenu & Beaumont 2017, Da Veiga & Eloff 2007, Khan et al., 2019
    - metrics, monitoring and auditing: Gangwar & Date 2015, Damenu & Beaumont 2017, Da Veiga & Eloff 2007, Al Hogail 2015
    - business continuity and disaster recovery: Gangwar & Date 2015, Da Veiga & Eloff 2007
    - asset management: Gangwar & Date 2015, Da Veiga & Eloff 2007
    - access control and identity management: Gangwar & Date 2015, Da Veiga & Eloff 2007

Interestingly, there was evidence that policies were often not properly enforced (Goldman 2012, MQ) despite their helpfulness in creating employee compliance (Donalds & Barclay 2022, HQ).

Organisational culture

Many researchers (e.g., Ahmed & Al-Haddad, 2020, Berlilana et al., 2021, Armenia et al., 2021, Donalds & Barclay 2022, Qian et al., 2012 (all HQ); Da Veiga & Eloff 2007, Koskosas 2011, Gangwar & Date 2015, Al Hogail 2015, Alqahtani & Erfani 2021, Ihmouda et al. 2015 (all MQ), Dhillon et al., 2016 and Cannoy & Salam 2010 (both LQ)), noted the importance of an organisation's information security culture.

> "organizational culture [is an] organizational factor that influence[s] organizations in adopting digital innovations or new technologies." (Berlilana et al, 2021 p5)

> "Research has also shown that building and sustaining a good security culture is extremely important in times of radical change" (Dhillon et al., 2016 p63)

Koskosas 2011 (MQ) defined organisational culture as:

> "a system of learned behavior, which is reflected on the level of end-user awareness and can have an effect on the success or failure of the information security process… In the context of information security, behavior can be considered as the perception of organizational norms and values associated with information security" (p84)

He stated that staff need to be active participants in security and act as advocates for an organisation's information security norms and standards. Gangwar & Date 2015 (MQ) pointed out that an information culture is an important mechanism to empower employees to be aware of their responsibilities for information security. Al Hogail 2015 (MQ), interestingly, also found an information security culture to be:

> "far more effective than regulations that simply mandate employees' behavior. Without a proper information security culture, the enforcement of security policies through the

> traditional cycle is less likely to be effective than when employees know, understand, and accept the necessary precautions" (p164)

They proposed an Information Security Culture Framework, accompanied by an assessment instrument, to help organisations create an appropriate culture. They also presented three case studies of different organisations. Whilst their participants had a strongly positive attitude to information security each needed in practice to make several changes (notably in terms of awareness raising, training and the allocation of resources to carry these out). Donalds & Barclay 2022 (HQ) also argued for a culture of compliance and security awareness and the importance of improving attitudes. Berlilana et al., 2021 (HQ) noted that a positive culture enabled better readiness for dealing with cyber-attacks:

> "organizations that have good cultural support will be better prepared to face cyber-attacks. These findings support the findings of previous studies examining cyber security innovations" (p15)

Culture can act as both an enabler (as above) and a constraint on effective AoST. Negative information cultures received attention, with reactive approaches to information security management being criticised. For example, Qian et al., 2012, in a high-quality study of the oil and gas industry in Norway, noted the dangers of a reactive attitude to security where security concerns were only addressed following incidents:

> "a reactive approach to security risk management might trap the organization into blindness to minor incidents and low incident response capability, which can lead to severe incidents" (p859)

'Silo' mentality and the failure to take a holistic, systemic, or dynamic approach also led to problems there. (See also Armenia et al., 2021, Donalds & Barclay 2022, both HQ). Al-Darwish & Choe 2020 (LQ) found that a culture of complacency was also problematic and detailed the consequences that flowed from this, for example, inadequate staffing numbers and the development of procedures for the sake of compliance or audit rather than real effectiveness.

Resources

The adoption of new security technology will probably require resources other than staff skills, notably financial funding for IT (Qian et al., 2012, Donalds & Barclay 2022, Luo & Choi 2022, Armenia et al., 2021, Herath et al., 2020, (all HQ); Anderson 2010, and Koskosas 2011 (all MQ)). Li 2015 argued that the size of a firm is a factor related to this as:

> "Large firms tend to possess slack resources that can facilitate technological innovation adoption. Small firms, on the other hand, suffer from resource poverty due to a lack of financial resources, professional expertise and a short-range management perspective. Consequently, small firms tend to be slower in technological innovation adoption" (p22)

Large firms also have greater capacity for bearing failure costs and fines. Alliances and collaboration are noted by Rajan et al., 2021, Luo & Choi 2022 & Berlilana et al., 2021 (all HQ) as another important resource which aid information, knowledge, and skill sharing, and may help in practical ways:

> "if "Firm A" forms a logistics sharing alliance with "Firm B," then [this may ensure] "Firm B" can guarantee customers a promised delivery time (PDT)" (Luo & Choi, 2022, p2109.)

Existing processes

The processes already in place (e.g., for risk management, updating technology, access control, security assessment, incident response) may have an influence on the success of an organisation's adoption of new security technology (Armenia et al., 2021, Donalds & Barclay 2022, both HQ). The processes may need changes/improvements, or to be introduced if they are not already in place. Changes to technology are also likely to requires changes to the specific ways people work: see e.g., Qian et al., 2012 (HQ), Al Hogail 2015 (MQ). As previously mentioned, Sivan-Sevilla 2021 (HQ) discussed cyber risk governance noting how government policymakers were more heavily influenced in practice in developing risk frameworks by path dependency and existing processes than current risk framings. He identified three distinct frameworks in the USA and showed that:

> "variance stemmed from the institutional configurations in each regulated sector and the consequent decision-making structures that had been institutionalized early on, rather than the framing of cyber risks" (p692)

Risk management was frequently mentioned as an important factor e.g., Qian et al., 2012 (HQ), Gangwar & Date 2015, Anderson 2010 and Ihmouda et al., 2015 (all MQ). Qian pointed out the necessity for this to be an ongoing process:

> "static risk assessment method is less relevant for the case of this study, where the organization is going through operation transition, which is a complex, long-term, and dynamic process with feedback, delays, and trade-offs, among others. The risk picture will change along the way. It is necessary to consider how the transition affects the information security risks." (Qian et al., 2012, p868)

Koskosas 2011 (MQ) made the point that business processes requiring re-engineering should be considered prior to implementation. In his case study he found that:

> "as the re-engineering of business processes followed the introduction of e-banking, the bank had some difficulties in implementing those changes" (Koskosas 2011, p94)

Audit, evaluation, accountability, and disclosure

The need to pass audits was found by some to encourage compliance with correct security technology usage, e.g., Goldman 2012 (MQ):

> "Regulatory fear, passing audits, and meeting specific customer or third-party audit requirements were major external influences" (p358).

Donalds & Barclay 2022 (HQ), Gangwar & Date 2015 (MQ) and Cannoy & Salam 2010 (LQ) also noted auditing and the reporting of breaches as important for compliance. Cannoy & Salam 2010 noted that requirements to disclose support compliance and Li et al., 2015 (HQ) found that voluntary disclosure of breaches in company reports were largely reliable. Khan et al., 2019 (HQ) argued that roles, responsibilities, and accountability needed to be clearly allocated. Finally, Pathari & Sonar 2013 (MQ) produced a method to measure information security assurance and the effectiveness of controls.

Armenia et al., 2021 and Wu & Saunders 2011 (both HQ) drew attention to the importance of the appropriate allocation of responsibility including decision-making rights. The latter provided a framework to help with this.

Management support
Management support, particularly top management support, was frequently seen as a vital motivating factor in the adoption of new security technologies, see e.g., Kefallinos et al., 2009, Herath et al., 2020, Rajan et al., 2021, Balozian et al., 2019 and Donalds & Barclay 2022 (all HQ).

Medium and low-quality evidence also supported this as a factor that was both expected, and found, to be important in practice. Schinagl & Shahim 2020 (MQ) noted that its absence affected the information security culture and reduced the degree to which security became embedded. (See also Al-Darwish & Choe 2020 (LQ)). They found the issue was often a communication one whereby management found it hard to understand IT explanations, and IT staff did not understand the business requirements fully. Resource issues also played a part as it could be hard to demonstrate security technology's link with profitability.

Staffing, training, and education
Staffing was an important organisational condition for successful adoption. Without staff compliance in the form of accurate use of new technology and organisational security measures, any new adoption is unlikely to be successful. Partial use can also mean that the technology's full potential is not realised, and it is in reality only partially adopted.

Qian et al., 2012, Armenia et al., 2021 and Herath et al., 2020 (all HQ) among others raised the issue of education and training: e.g., do the existing staff have the required skill set, if not can they be retrained or is there a need for new specialised personnel, whether employed in-house or accessed out-of-house? The importance of education and training for ensuring successful adoption was the most frequently mentioned component in the information security frameworks listed in Section 4.5.7 and was highlighted in other high and medium quality studies also e.g., Rajan et al., 2021, & Donalds & Barclay 2022 (both HQ), Koskosas 2011, (MQ). For example:

> "In order to deal with insider risks, a firm needs to implement training and educational programs; security training should be given to advance knowledge and awareness (Straub and Welke, 1998; Zwilling et al., 2020), which helps transform people's attitudes and concerns regarding security (Johnson, 2006)." (Rajan et al., 2021, p3)

Armenia et al. 2021 noted that training and education needed to be ongoing, and Qian et al., 2012 that time to hire, train and address knowledge gaps caused by a new system post-training is essential. Goldman 2012 (MQ) stated:

> "Instead of relying on technology (e.g., firewalls), gains in security posture may be more effectively realized by investing in training, as well as by improving attitudes and processes throughout the system development lifecycle (SDLC)." (p350)

Governance arrangements
Schinagl & Shahim 2020 (MQ), found no one universally accepted definition of information security governance (ISG), rather different perspectives on it (see below), but they did state that definitions of it were ultimately all "related to the thought that senior executives and boards are responsible for security and the way it is incorporated into organisational structures" (p269). In the context of this paper, governance is taken as referring to sectoral and organisational information security governance and the methods that are used to facilitate adoption of, and employee compliance with, new security technology. This could include policies and procedures, Service Level Agreements (SLAs) and contracts.

Governance was important to the successful adoption of new security technologies:

> “The results show that governance enhances cyber security by providing financial support, effective cyber security policies, learning culture, and involvement in initiatives on information security within organizations (Wiley, McCormac, and Calic, 2020).” (Rajan et al., 2021 HQ, p8)

There were different approaches to governance, with the evidence in relation to new (often distributed) technologies showing a movement away from traditional hierarchical governance towards decentralised self-governance and collective decision-making. Khan et al., 2019 (HQ) provided guidelines for self-governance arguing for “the humane flows of collegial control and responsibility, as opposed to the inhumane flows of authority and power” (p1). Skarzauskiene et al., 2021 (MQ) appeared to call this community governance:

> “the Web 3.0 Blockchain stack is a more user-centric decentralized network. Web 3.0 focuses strongly on community governance and on the self-sovereignty on one’s own data, wealth, and other valuable assets [9–11]” (p1019-20)

Schinagl & Shahim 2020 (MQ) described the “traditional view of governance as a control and conformance mechanism” (p270) as inadequate. They characterised ISG approaches as moving over time from being solely about technical IT controls to a more holistic approach bringing human and organisational factors into account. They identified three main perspectives: the corporate governance perspective focusing on technical controls, the more holistic socio-technical perspective, and the resilient business perspective where security is aligned with business goals (p274 of their paper offers a summary of these approaches). Schinagl & Shahim 2020 argued that the socio-technical approach could focus too much on the individual which might bring bias, and that information security governance should be related to the organisational level where it should be seen as a strategic business issue with relevance to all employees:

> “It is more important to understand how ISG is related to business processes, e.g., how to align security with strategic drivers, such as the organisation’s mission, goals and objectives, to enable organisational resilience” (p270).

They argued for security-by-design, and supported a resilient, strategic approach rather than one focused only on prevention and operating ad hoc in response to problems. Breaches are inevitable; therefore, an organisation needs to be able to cope with them and continue to operate well during and after them. They described this approach as Digital Security Governance.

Technical and other infrastructures

The organisation’s existing technical infrastructure is important in terms of its compatibility with new systems e.g., Herath et al., 2020 (HQ):

> “To move toward change, one would need…attention to the particular technologies that were being implemented, and the systems and structures these technologies were being implemented into. Further, organizational transformation can then more readily occur if the systems and ways of doing things are aligned with their environments they serve. The new technologies need to work for the people that are using them.” (p358)

Obtaining a new system may require improving the existing security infrastructure, its resilience and/or threat detection capacity (Donalds & Barclay 2022, HQ). Herath et al., 2020 noted that the perceived complexity of the new technology in relation to the existing infrastructure could prove to be a deterrent factor.

The infrastructure of the company itself was also noted as an affecting condition: for example, Higgs et al., 2016 (HQ), noted that board level technical committees could provide confidence amongst stakeholders leading to the mitigation of abnormal stock returns.

4.5.3 Conclusion

There was a large amount of **mixed quality evidence** for organisational conditions that could facilitate the successful adoption of new technology or whose absence could constrain it. Specific factors highlighted through much of this were: organisational culture; support from management; staffing, training, and education; resources; technical and other infrastructures; existing processes; audit, evaluation and accountability, and organisational instruments. There was no consensus as to the most important organisational conditions, with several authors noting the importance of a holistic approach to adoption that explored all the factors and took account of context.

4.6 What are the organisational consequences of adopting security technologies?

4.6.1 Definition

The OED defines a consequence as “A thing or circumstance which follows as an effect or result from something preceding.” Here it signifies an outcome arising from the adoption of new security technologies. It is intuitive that benefits would be one set of such outcomes, and these are covered in Section 4.1.2. This section focuses on secondary benefits and consequences arising from enacted risks or possibilities.

Orlikowski (1992) defined the consequences of institutions’ interaction with technology as impacting “the institutional properties of an organization, through reinforcing or transforming structures of signification, domination, and legitimation” (p410). She noted that human activity may have both intended and unintended consequences:

> “For example, a company's adoption of electronic mail may have the intended consequence of increasing communication and information sharing, and the unintended consequence of reducing status barriers and social context cues (Sproull and Kiesler 1986).” (Orlikowski, 1992, p406)

Brous et al., 2020 following Orlikowski, noted that:

> “action taken by actors may have unintended consequences. For example, Mirvis et al. (1991) suggest that technology can influence the layers of hierarchy in companies, with regards to delegation of responsibilities, or chosen strategy (Buonanno et al., 2005), the suggestion being that technology is an important factor driving organizational behavior (Mendel et al., 2008; Subramanian & Nilakanta, 1996)”. (Brous et al., 2020, p6)

Alabdulkarim & Lukszo 2010 (HQ) pointed out that consequences can be direct or indirect, major or minor, and will also interrelate with each other. Risk and negative consequences are sometimes hard to distinguish. For example, there is a risk employees may not comply correctly with a system leading to consequences such as data breaches. Here lack of compliance is a risk, but it may also be a negative consequence arising from a different risk, e.g., a company provides inadequate training or familiarisation time, leading to the consequence of non-compliance.

Wang et al., 2021 (HQ) stated that IT adoption is an ongoing process involving a changing relationship between human actors and technology. He provided an interesting case study illustrating the iterative interplay between technology and people: human goals or the desire for certain benefits lead to the adoption of new technology embodying affordances which enabled achievement of these benefits. This in turn can lead to changes in organisational conditions (such as processes and routines) and human behaviours. Over time, because of external or internal developments, the IT becomes inadequate to current need (IT constraints), which in turn leads to the next iteration of technology.

4.6.2 Main findings

4.6.2.1 Overview of the evidence

This section reports the main findings related to part of the research question RQ4: ‘What are the organizational conditions and consequences of adopting new security technologies?’ **The evidence**

base for this comprised 23 papers of mixed quality with 15 assessed as of good methodological quality, 5 as of medium quality and 3 as low quality. This included articles covering the outcomes of adopting secure technologies generally (12), plus papers focused wholly or in part on specific technologies (11), notably cloud computing (5) and blockchain (3) but also biometric technology (1), smart cities (1) and mobile payment systems (1). Eleven of the 23 studies focused on the adoption of the technologies within specific sectors: retail-related (2), government (2), home security (1), oil and gas (1), education (1), hospitality & tourism (1), energy (1), health (1) and ICT (1). Eleven of the 23 focused only on developing countries, including the UAE (2), India (2), China (2), Korea (1), Bangladesh (1), Jamaica (1), Taiwan (1) and Iran (1). Consequences arising from specific technologies are dealt with in Section 4.7

4.6.2.2. Consequences

As Orlikowski (1992) noted, adoption of new security technology can lead to unexpected consequences. Krishna & Sebastian 2021 (HQ) found that that e-government development had a direct strong positive impact on cyber security commitment nationally and through this an indirect relationship to national prosperity:

> "While the development of e-government can be seen as having a first-order association with cyber security commitment, it also has second-order associations with business usage and economic prosperity" (p753)

Qian et al., 2012 (HQ) examined a case study of the transition of Norwegian oil and gas to integrated operations where ICT systems were used to connect offshore platforms, onshore control centres, and suppliers. The research investigated what would happen if the transition was undertaken reactively (after incidents had occurred) or proactively (before any incidents). Whilst the frequency of problematic incidents would remain the same, they found that the proactive organisation could expect a reduction in the severity of incidents and in costs of 56%.

However, consequences were not always positive. In relation to Secure Multiparty Computation, Kanger & Pruulmann-Vengerfeldt 2015 (MQ) noted that:

> "more often than not the adoption of new technologies disrupts existing practices, old habits and organizational routines — meaning that from the viewpoint of a potential adopter the new technology may be characterized by certain disadvantages as well." (p44)

Qian et al., 2012 (HQ) noted counter-intuitively that the time following the adoption of new technology was a risky period when security breaches could occur, calling it "a rich environment for breeding vulnerabilities and risks" (p859). This was because of the knowledge gaps created by the changes involved with new security technology adoption:

> "The operation transition is represented by the two chains of changing *work processes* and *knowledge*. Knowledge takes longer time to mature than work processes. Therefore, a *knowledge gap* will be generated and it drives *vulnerability*, thus *frequency of incidents" (*Qian et al., 2012, p862, their emphasis)

This could lead to overinvestment in security technology as the increase in incidents caused the perception of a worse situation than existed in reality. Higgs et al., (2016) in a high-quality paper, found a high level of uncertainty around the effect on data breaches of having a technology committee. Their findings, however, provided evidence that having a new technology committee, or, indeed, a risk or compliance committee, was associated with an increased number of incidents being reported in the first year of adoption. This is presented as more than simply increased ability to identify more breaches and, it could be suggested, may be due to the knowledge gap identified by Qian et al., 2012. This changed over time as the committee became more established. They found that internal breaches were more likely to occur where an organisation had a risk or compliance committee overseeing technology adoption, and external breaches were more likely with a technology committee. However, the consequences of a technology committee did include benefits:

> "We find that while external breach disclosures are accompanied by a negative return for firms without technology committees, firms with technology committees in place at the time the breach is disclosed do not experience significantly lower negative returns. Further, the magnitude of the return is not influenced by the age of the technology committee. Our interpretation is that the market views the existence of a technology committee as a mitigating factor in the severity of the ''bad news'' of the external breach disclosure" (Qian et al., 2012, p95)

Jardine 2020 (HQ) offered an alternative explanation to knowledge gaps for increases in security breaches after adoption of new technology, in the form of Risk Homeostasis Theory (RHT):

> "the introduction or adoption of new security technologies changes an individual's perceived risk, potentially leading to more risk-accepting behaviors that return risk levels to their original value. RHT could help to explain constant or even worsening cyber risk outcomes after new security technologies are introduced… new security technologies can make users feel safer, encouraging riskier behaviors that effectively offset or even exceed the security gains from new technologies." (p1572)

Whilst Jardine's article (2020) is about commercial antivirus software, he explicitly applies the same principle to hardware security elements e.g., physical entry restrictions to data centres (p1572). The RHT effect may fade with time so that the longer-term consequences of the adoption are that the organisation is neither worse nor better off.

> "new cyber security technologies can sometimes have ill effects on security outcomes in the short run and little-to-no effect over the long run." (Jardine 2020, p1571)

Other potential consequences that may not be apparent prior to adoption can include:

- Detrimental interaction with other systems in the organisations: Kefallinos et al. 2009, Donalds & Barclay 2022, Jackson 2016 (all HQ)
- Insider threats e.g., "fraud, sabotage, theft of intellectual property, and copyright violation" Armenia et al., 2021, p2. See also Donalds & Barclay 2022 (both HQ)
- Glitches and delays to work caused by system problems: Jackson 2016 (HQ)

Cannoy & Salam 2010 (LQ) stated that a holistic approach is needed so that "As technology grows…all aspects of the security program grow with it." (p128). This was supported by Dhillon et al., 2016 (LQ) who provided a detailed case study of the merger of two customer relationship management systems during the merger of two companies. They noted that this introduced several negative outcomes in terms of effects on the organisational culture and on use of the system. Employees were expected to comply with controls but circumvented them:

> "Simply implementing a customer relationship system and hoping that communication needs will be addressed is not sufficient. What is required is linking technical solutions to the formal rules and obligations of various stakeholders, which necessitates the need for formal structures which support the technical edifice. After all, managing security is a holistic

> activity, and there is a need to maintain integrity amongst formal and technical components." (Dhillon et al., 2016, p69)

They set out principles for creating a good information security culture, including the importance of establishing good communication structures, clarity re responsibilities and accountability, and avoiding over-engineered solutions. They emphasised the importance of sustaining the culture once established:

> "The new AirTelco/Relicom organization indeed did a good job in creating such an environment. However, there was no means for them to ensure continuous improvement and the integration of cultural processes for a sustained cultural integration. Failure to do so usually causes disillusionment and results in employees abandoning their integrative efforts – which is a serious security concern." (p68)

Lee et al., 2016 (HQ) provided a tool to examine systematically different possible future consequences of technology adoption by incorporating scenario analysis into technology road-mapping, which he described as:

> "a dynamic framework that enables the evolution of a complex system to be mapped and shared, supporting the development and deployment of innovation and strategy" (p165)

Lee et al.'s 2016 tool included the ability to calculate possible interactions between activities and also ripple effects on organisational plans. It was designed to help diagnose vulnerabilities in organisational plans and to facilitate expert agreement in the period after initial adoption.

4.6.3 Conclusion

There was **limited, mixed quality evidence** for the consequences of adopting new security technology. Both positive and negative consequences were identified. Positive consequences included indirect improvements to national prosperity, improvements to business confidence and better information management. Contra-intuitively there were several negative outcomes from adopting new security technology including increased numbers of data breaches. These may not simply be due to improvements in identification brought by the new technology, but by knowledge gaps or RHT.

4.7 Specific technologies

4.7.1 Cloud computing (CC)

4.7.1.1 Overview of the evidence

Cloud computing was the specific technology most frequently researched in relation to security, with 13 papers covering it (however it is important to note that Priyadarshinee et al., 2017 and Raut et al., 2018 draw on the same raw data). Table 4 indicates the paper's authors, dates, levels of quality of the evidence, which topics were covered, the sector and setting. **The quality of the evidence was mixed ranging from high quality (3 papers) to low (4 studies), with the largest category being medium quality (6).** Only four of the 13 studies focused on the adoption of CC within a specific sector: government (1), banking (1) ICT (1) and manufacturing (1). However, two other papers also included manufacturing as one amongst a variety of sectors. The majority of the evidence came from studies in Asian settings, rather than Western settings. The evidence consistently noted reductions in cost and scalability as major expected benefits of CC.

Table 4

Authors / Date	**Quality of evidence**	**Topics covered***	**Sector**	**Setting**
Khayer et al., 2021	High	B, C, D, O, R	General	Bangladesh
Raut et al., 2018	High	B, C, D, O, R	Various including manufacturing	India
Khan et al., 2019	High	C, D, G. O. R	General	UAE
Gangwar & Date, 2015	Medium	B, G, O, R	Manufacturing	India
Park et al., 2016	Medium	C, R	General	Korea & China
Sener et al., 2016	Medium	G, O	General	Unclear
Priyadarshinee et al., 2017	Medium	B, C, D, O, R	Various including manufacturing	India
Alizadeh et al., 2020	Medium	B, D, G, O	E-banking	Iran
Alassafi et al., 2016	Medium	B, D, R	Government	Saudi Arabia
Golightly et al., 2022	Low	B, R	General	Western
Swamy, 2013	Low	B, D, G, O, R	General	Western
Chiniah et al., 2019	Low	B, D, G, O, R	ICT	Mauritius
Hashemi et al., 2015	Low	B	General	Unclear

*Topics covered = B – Benefits, C – Consequences, D = Decision-making processes, G – Regulations or other incentives, O – Organisational conditions, R – Risks.

4.7.1.2 Findings

Benefits

The **high-quality evidence** agreed that the expected benefits of adopting CC included reduced costs and scalability (Raut et al., 2018 and Khayer et al., 2021). This was also supported by **medium quality evidence** (Gangwar & Date 2015, Alizadeh et al., 2020, Alassafi et al., 2016 and Priyadarshinee et al., 2017). Other expected benefits supported by at least one source of **good quality or one highly ranked medium quality evidence paper** (Gangwar & Date 2015) included: increased annual revenue, access to hitherto inaccessible or unaffordable resources, enhanced market share and consequent competitive advantages, improved efficiency, portability of services (they are device-independent), reduced time and energy (e.g., on installation or maintenance), environmental sustainability, improved business agility and flexibility as services can be changed relatively quickly, greater ease and convenience, better reliability as problems are dealt with centrally, improved performance expectancy, improved security, and better communication and coordination with partners for better market integration. Alassafi et al., 2016 also noted CC could offer centralised auditing, and Priyadarshinee et al., 2017 expected benefits from virtualisation, the ability to access cloud provider expertise, and improved customer service.

Raut et al., 2018 (HQ) & Priyadarshinee et al., 2017 (MQ) found that CC adoption improved actual business performance. Priyadarshinee et al., stated that CC will:

> "impact the success of an organization relative to transactions, capital investments, and total possessions. Better success will also affect an organizations skill to deliver better reoccurrence to the stockholders, and increase its money share capability, that will progress market place [sic] of the organization as well as the business performance" [sic] (Priyadarshinee et al., 2017, p358)

There was also **low-quality evidence** to support CC as providing actual benefits: these were broad network access, resource pooling, scalability, efficient management of expenditure, auditability, virtualisation, and improvement to brand image as cloud computing is a green technology (Golightly et al., 2022, Swamy 2013). Golightly et al., added:

> "Private Cloud…has benefits such as high protection and storage capacity, improved data transfer speed…and easy-to-use payment systems to significantly reduce energy and maintenance costs…Public Clouds, which are simple to use and efficient, can deal with an unlimited quantity of computing resources, high data security at the physical and software levels using large data centers, fast and simple implementation of…new information system[s]." (p2)

As regards implementation in specific sectors, the **medium quality evidence** includes analysis of the expected benefits of adopting CC in e-banking (Alizadeh et al., 2020) and in Saudi government agencies including ministries, universities, and telecommunications agencies (Alassafi et al., 2016). The benefits expected were the same as detailed above with the addition of reduced waste of resources and increased capacity (Alizadeh et al., 2020). Alassafi et al. 2016 found that improvements to security and auditing were expected to be statistically significant. The **available evidence (albeit LQ),** covering the actual adoption of CC in the ICT sector in Mauritius and that from e-government, supported the general expected benefits. Hashemi et al. 2015, also noted an expectation of better disaster recovery (as this would no longer rely on in-house expertise) and of software and hardware currency (updating would come automatically from the cloud provider).

Risks

The risks of CC have been well studied: for information on common issues please see Gangwar & Date 2015, Alassafi et al., 2016, Priyadarshinee et al., 2017 (all MQ) and Swamy 2013 (LQ). For example, Gangwar & Date 2015 found three significant risks: unauthorised access to data, shared infrastructure (data leakage between users) and the unavailability of data; but did not present these as unforeseen. Below details the unexpected risks observed. Table 5 shows risk mitigation factors that were found to be effective for different specific technologies and is referred to throughout these risk sections.

Table 5: Risk mitigating factors for specific technologies

Effective incentive	**CC**	**BC**	**5G**	**Mobile payments**	**Biometric authentication**
Regulation	Sener et al., 2016, Swamy 2013, Alizadeh et al. 2020, Chiniah et al., 2019	Gokalp et al., 2022, Clohessy & Acton 2019	Radu & Amon 2021	Fu et al., 2022	Venkatraman & Delpachitra 2008, Li 2015
Frameworks & policies	Khan et al., 2019, Gangwar & Date 2015 Sener et al., 2016	Al Ketbi et al., 2021			
Audit, accountability & disclosure	Khan et al., 2019, Gangwar & Date 2015, Swamy 2013	Carvalho et al., 2021			
Management support	Gangwar & Date 2015, Sener et al., 2016	Gokalp et al., 2022, Clohessy & Acton 2019			Venkatraman & Delpachitra 2008, Li 2015
Training & education	Khan et al., 2019, Gangwar & Date 2015				
Information security culture	Gangwar & Date 2015				
Financial penalties & rewards		Ciaian et al., 2021, Luo & Choi 2022			Li 2015
Personal motivation	Khan et al., 2019				
Social influences		Gokalp et al., 2022			

TECHNOLOGY RISK FACTORS

Raut et al., 2018 (HQ) draws attention to the impossibility of a risk-free environment due to frequent developments in technologies which may bring new uncontrollable or unavoidable risks that could not have been foreseen.

ORGANISATIONAL RISK FACTORS

The evidence here was of medium / low quality. Gangwar & Date 2015 claimed that Boards of Directors need to "focus upon proper alignment between ISG [Information Security Governance] and the organization's overall business strategy and their adequate implementation", suggesting that organisations were not doing that (enough) at the time. However, in practice they only found 1 out of 5 organisations poor on this. They also found that four out of five of their case studies were poor in providing awareness and education to employees. Two of the companies in their study lacked transparency, failing to provide users with enough information about data protection. They also stated that:

> "It is important for companies to understand the significance of jointly developing risk scenarios for the cloud service with the cloud service providers for consistent risk

> assessment approaches in terms of impact analysis criteria and definition of likelihood" (Gangwar & Date 2015 p57)

Swamy 2013 noted the dangers for organisations of inadequate training/ understanding of a system, potentially leading to unauthorised ways of using it:

> "While cloud computing allows organizations to be agile and meet computing requirements expeditiously, it also allows employees to take initiative and circumvent checks and balances of data management that present potential challenges to the organization." (Swamy 2013 p74)

ENVIRONMENTAL RISK FACTORS

Park et al., 2016 classified risk affecting CC adoption into compliance risk, information leakage risk, fault recovery risk & service interruption risk based on previous studies (so these are not unexpected risks). However, he found that fault recovery & service interruption risks were only insignificantly related to the non-adoption of CC in China. The situation differed in Korea where these were of significant impact "fault recovery risk, compliance risk and service interruption risk are negatively related with acceptance intentions" (p493). Both countries were found to be less worried about leakage risk if they trusted their providers. Raut et al., 2018 noted a general lack of studies of emerging economies.

HUMAN RISK FACTORS

Priyadarshinee et al., 2017 noted the importance of risk in relation to cloud computing, with perceived IT security risk (PITR) being the second most important predictor of its adoption, following trust. Raut et al., 2018 also supported this, presenting PITR's influence as a new or unusual finding of moderate significance. (He also found risk analysis to have a direct but less significant effect on CC adoption and stated that this too was a new finding). Park et al., 2016 noted that there was generally little research into the effects of security risks on actor intentions to adopt CC (Park et al., 2016).

CLOUD COMPUTING RISKS IN SPECIFIC SECTORS

Alassafi et al., 2016, Khan et al., 2019 and Chiniah et al.'s 2019 studies were of CC adoption in specific sectors. Alassafi et al.'s 2016 research into adoption in Saudi Government only covered commonly known / expected risks. Khan et al., 2019, looking at the IT sector in the UAE, provided **high quality evidence** indicating that research is still needed on the risks of inadequate technical skills on CC migration projects. They stated that:

> "The highest competency and skill required is being able to manage risks, compliance, and security [especially in relation to CC vendors]" (Khan et al., 2019 p9)

Chiniah et al., 2019 found that there was a lack of data about the business outcomes of investing in CC in a study of the ICT sector in Mauritius.

Decision-making

Research around decision-making focused on the factors requiring decisions, with the following deemed important for CC:

TECHNOLOGICAL

- Perceived IT security risk: Raut et al., 2018 (HQ), Alasaffi et al., 2016 (MQ)
- Performance expectancy / benefits of the technology: Khayer et al., 2021 (HQ), Sener et al., 2016 (MQ), Alasaffi et al., 2016, Swamy 2013 (LQ)

- Data security and privacy: Khayer et al., 2021, Alizadeh et al., 2020 (MQ), Swamy 2013, Sener et al., 2016
- Complexity: Alizadeh et al., 2020, Sener et al., 2016
- Compatibility: Alizadeh et al., 2020, Sener et al., 2016

ORGANISATIONAL

- Management style : Raut et al., 2018, Swamy 2013
- Absorptive capacity or “the capacity of sensing, acquiring, assimilating and exploiting external knowledge”: Khayer et al., 2021, p81, see also Swamy 2013
- Culture of innovation: Swamy 2013
- Top management support: Swamy 2013, Sener et al., 2016
- Viewing IT departments as business units not cost centres. Swamy 2013 described this as leading to more and faster innovation, as it enables the value of security to be shown
- Cost savings: Swamy 2013
- Monitoring: Swamy 2013
- Fear of loss of control of the system: Swamy 2013
- Compliance: Swamy 2013
- Organisation size : Sener et al., 2016
- Organisation IT resources : Sener et al., 2016

ENVIRONMENTAL

- Degree of vendor lock-in and dependency on vendor: Alizadeh et al., 2020
- Competitive pressure: Sener et al., 2016
- Trading partner pressure: Sener et al., 2016
- Social factors: Alasaffi et al., 2016
- Government policy & legislation: Sener et al., 2016
- Country based infrastructure: Sener et al., 2016

HUMAN

- Trust : Raut et al., 2018, Khayer et al., 2021, Sener et al., 2016
- Effort expectancy : Khayer et al., 2021

Khan et al., 2019 (HQ) looked at the determinants of role assigning and taking in relation to CC, finding organisational and human factors to be important. They argued that high technical competency is not essential outside the migration period, but that business skills are more important. Identifying the necessary competencies to ensure successful implementation decisions, they found that:

> “This research has highlighted ‘*people’s competencies, skills and mind-set*’ at evaluating and managing CC vendors as the dominant element. The ability to ‘*evaluate and manage CC vendors*’, particularly in terms of ‘*risk, compliance and security management*’ emerged as the highest desired competency.” (Khan, et al., 2019, p15, their emphasis)

They advised collegial or team decision-making as the most effective. Alizadeh et al., 2020 (MQ) thought technical factors the most important for the adoption of cloud computing in e-banking, followed by environmental, human, and organisational. This shows the same lack of consensus as to the relative importance of key factors as was found in relation to new security technology in general.

Original models for assessing the factors affecting adoption of CC were also presented in **mixed quality evidence** (Raut et al., 2018, Priyadarshinee et al., 2017, Alasaffi et al., 2016, Chiniah et al., 2019) Raut et al., 2018 (HQ), for example, provided a new hybrid modelling approach (SEANIS) for analysing the factors influencing cloud computing adoption. This approach was a hybrid of structural equation modeling, artificial neural network and interpretive structural modelling and was presented as applying to developing economies. They stated that:

> “This research is intended to help the decision and policy-makers in understanding the cause-effect relationship between the factors and identifying the critical determinants of CC implementation, which will help in taking effective decisions” (p99)

Alizadeh et al., 2020 & Priyadarshinee et al., 2017 both agreed that decision-making requires careful thought about multiple factors including the categories of technological, human, organisational and environmental factors discussed above.

Regulation and incentives

Regulations were seen as a powerful encouraging or constraining influence on the adoption of security technology. Speaking in relation to cloud computing Alizadeh et al., 2020 (MQ), citing Chang et al. (2007) stated:

> “governmental policies have a positive effect on the efforts of organisations in adoption of new information technology systems.” (p415)

Sener et al., 2016, on the other hand, noted that current legislation discouraged the move to new technology:

> “Government policy and regulations and its preferential strategies can encourage or discourage the adoption of the Cloud-EIS [Enterprise Information System]…present laws and regulations are critical in adoption of new technologies…if the government mandates firms to comply with cloud-specific standards and protocols, firms will be more apt to adopt cloud computing [for EIS]” (Sener et al., 2016, p60)

However, although here they said that government regulations “profoundly impact” adoption, elsewhere they noted that this is among the most “insignificant” of the critical factors they identified, so this evidence is somewhat contradictory.

Khan et al., 2019 (HQ) found that 8.7% of participants had personal motivations for CC adoption:

> “People are rewarded by being allocated to cloud-related tasks, so as to give them opportunity for growth, motivation, recognition, and the challenge of learning new technologies” (p14)

Table 5 indicates the incentives that were noted as effective by the authors for particular technologies.

Organisational conditions

Raut 2018 explored “driving factors” behind the adoption of CC that need to be in place for successful adoption. These included internal financial processes, organisational innovativeness and corporate strategy, plus other factors such as technical capability. Innovativeness was also noted as a driving factor by Swamy 2013 & Priyadarshinee et al., 2017. Other organisational factors assisting adoption of CC (or potentially hindering it if absent) were:

- Management style: Raut et al., 2018, Swamy 2013, Khan et al., 2019, Priyadarshinee et al., 2017
- Top management support : Swamy 2013, Alizadeh et al., 2020, Sener et al., 2016

- Absorptive capacity or "the capacity of sensing, acquiring, assimilating and exploiting external knowledge": Khayer et al., 2021, p81, Swamy 2013
- Having an adaptive culture: Swamy 2013, Chiniah et al., 2019
- Appropriate security culture: Gangwar & Date 2015, Sener et al., 2016
- Viewing IT departments as business units not cost centres, as this allowed them to demonstrate value: Swamy 2013
- Technical readiness in terms of infrastructure and skills: Khayer et al., 2021
- Resources: Sener et al., 2016, Chiniah et al., 2019, Alizadeh et al., 2020. In practice Alizadeh et al., found this was not important possibly because "Iranian banks generally have significant resources and are managed with public costs," (p422)
- Staff knowledge and skills, training: Alizadeh et al., 2020, Chiniah et al., 2019, Khan et al., 2019.
- Perceived value of CC: Alizadeh et al., 2020
- Perceived risk: Priyadarshinee et al., 2017
- Information security governance: Gangwar & Date 2015 found that Indian directors of manufacturing companies using cloud services saw information security governance as an "integrant [sic] component for the success of corporate strategy and its value creation in the organizations" (p52).

Finally, some cloud computing-related frameworks / models were presented by Khayer et al., 2021, Alassafi et al., 2016, Sener et al., 2016 and Golightly et al., 2022.

Consequences

Khan et al., 2019, (HQ) found that adoption of cloud computing could lead to the following consequences:

- Loss of control: after adoption control was shared with cloud service providers. This led to a need for changes to the organisation, work patterns and style of management.
- The need to move away from 'siloed' thinking: "silos within IT and other autonomous business units needs to be broken down to ensure cross functionality [25], leading to a participative role-taking decision-making process" (p4)
- CC vendors take control of the technical aspects of CC, meaning that there is less of a need for technical skills in the purchaser
- There is a greater need for business skills, with the most important being the ability to successfully evaluate and manage vendors as regards risk, security, and compliance
- Small organisations may rely too heavily on CC providers for technical skills
- The reduction in the requirement for IT skills can "act as a catalyst to facilitate the relocation of people to different departments or to expose them to new career paths" (p14)

As noted earlier, Park et al., 2016 (MQ) identified four types of cloud security risk (information leakage, fault recovery, compliance risk, service interruption). The consequence of these occurring will be customer discontent which may extend to the supplier in general, not just a particular system.

4.7.2 Blockchain

4.7.2.1 Overview of the evidence

Blockchain was the next most frequently researched technology in relation to security, with 7 papers covering it. Table 6 indicates the paper's authors, date, which topics were covered, the sector and the setting of the evidence. **The evidence was mostly high quality with only one paper outside this category, and of medium quality.** Only three of the seven studies focused on the adoption of CC within one specific sector: e-commerce (2) and finance (1). Settings were varied.

Table 6

Authors / Date	**Quality of evidence**	**Topics covered***	**Sector**	**Setting**
Luo & Choi, 2022	High	B, G, O, R	E-commerce supply chains	Non-specified
Clohessy & Acton, 2019	High	B, G, O	General	Western
Carvalho et al., 2021	High	C, G, O, R	General	Non-specified
Ciaian et al., 2021	High	B, G, R	Finance	Non-specified
Gokalp et al., 2022	High	B, C, D, G, O, R	E-commerce supply chains	Western / Turkey
Garg et al., 2021	Hight	B	Banking	India
Al Ketbi et al., 2021	Medium	C, O, R	Various	UAE

*Topics covered = B – Benefits, C – Consequences, D = Decision-making processes, G – Regulations or other incentives, O – Organisational conditions, R – Risks.

4.7.2.2 Findings

Benefits

There was **high quality evidence** that adopting blockchain was expected to bring the financial, reputational, risk and compliance benefits generally expected of new security technology. It also brought additional benefits, for example, adopting blockchain was expected to lead to greater privacy as it is a distributed network with no single central authority. Through this it could unite non-trusting partners of different types as well as divergent types of records and activities (Ciaian et al., 2021, Gokalp et al., 2022). Other expectations included the immutability of data once entered and the usefulness of the validation function (Ciaian et al., 2021, Gokalp et al., 2022, Clohessy & Acton, 2019). Clohessy & Acton 2019 also expected faster transaction times, and Gokalp 2022 noted that it should provide good data provenance, robustness, and increased sustainability.

Clohessy & Acton's 2019 case studies of 20 companies (HQ) found the actual benefits to include performance management benefits, supply chain traceability, reduced complexity, higher speeds and lower costs (although Ciaian et al., 2021, found that the cost incentives for adopting blockchain only had a weak effect on uptake). Clohessy & Acton 2019 also noted that "enhanced security, efficiency and transparency…is associated with blockchain transactions." (p1481).

High quality evidence is available from Gokalp et al., 2022 and Luo & Choi 2022 regarding the expected benefits of adopting blockchain in the retail sector, specifically in relation to supply chains. This included, e.g., increased efficiency, decreased costs, the security benefits of decentralisation, and improved transparency and trust. New benefits mentioned included efficient inventory management, improved customer satisfaction and compliance and the ability to obtain real-time, accurate product information. Garg et al., 2021, in another **high quality study**, provided a useful list of the expected benefits of implementing blockchain in the finance sector, divided into 3 categories: institutional factors (cultural, regulatory and governance benefits); market factors (performance and business process benefits) and technical factors (benefits linked to data quality, distributed ledger characteristics, infrastructure factors and information exchange & transactions). These are accompanied by references to supporting research. An interesting addition to the list of possible benefits is the suggestion of blockchain as a green technology.

Risks

For a helpful list of expected risks together with their controls please see Al Ketbi et al., 2021 (p323-6, MQ). The following focuses on unexpected risks.

TECHNOLOGY FACTORS

Carvalho et al., 2021 (HQ) noted the following risk as new: ‘poisoning’ of blockchains (adding private, illicit, or sensitive data to them) with the risk of invading privacy or data protection. He also noted other forms of unwanted blocks in chains, e.g., those containing erroneous or malicious data. In all these cases the ‘right to be forgotten’ principle was impaired by blockchain’s immutability.

ORGANISATIONAL FACTORS

Carvalho et al., 2021 noted a general lack of dispute resolution mechanisms in organisations for resolving difficulties with blockchain. Two on Al Ketbi et al’s 2021 list of risks were identified as not covered by existing controls, specifically:

- Unclear vision on the used consensus mechanisms for signing, verifying, and publishing blocks on the respective platform
- Unclear vision on the data type to be stored on the respective platform

BLOCKCHAIN RISKS IN SPECIFIC SECTORS

Luo & Choi’s 2022 (HQ) study of blockchain in e-commerce supply chains explored risk / benefit ratios to participants, and produced the following formula:

> “the adoption of technologies can increase the cyber-security level and bring benefit to all members when the benefit brought to consumers with the use of technologies (b) is greater or slightly less than the per unit technology operations cost (c) and the fixed technology cost (TIT) is not very high.” (p2120)

Ciaian et al., 2021 (HQ) noted the risk of collusion between bitcoin users, however, it is not clear if this was unexpected. Gokalp et al., 2022 (HQ), looked at the adoption of blockchain in supply chain management (SCM), finding environmental factors to be the most important:

> “Supply chain partners need to use a common SCM system structure; thus, the decision for transitioning to blockchain-based SCMs is mainly affected by environmental dynamics.” (p113)

System providers need to “clarify the benefits and challenges of employing blockchain technologies in the supply chain” (p116) to assist purchasers’ decisions.

Please see Table 5 for risk mitigation factors

Regulation and incentives

Again, regulations were seen as a powerful encouraging or constraining influence on the adoption of security technology (Gokalp et al., 2022). As noted previously, governments could undertake various actions to aid the adoption of blockchain other than passing direct legislation. Clohessy & Acton 2019 detail the following points: governments could:

- Promote the benefits of new technologies
- Adopt the technologies themself so effectively promoting them (they noted that the adoption of blockchain increased once government had taken it on)
- Offer incentives, financial or otherwise

- Pass indirectly supportive legislation: laws that may not mandate technologies, but can encourage their adoption or implementation:

  > "Six of the interviewees pointed out that the newly enacted GDPR triggered their organizations to adopt or consider blockchain technology to ensure compliance with the new data protection laws" (Clohessy & Acton 2019, p1479)

Gokalp et al., 2022 noted that governments could provide clarity about forthcoming legislation affecting a technology.

> "Organizations desire to be prepared if the market imposes policies and regulations based on blockchain, and the fear of "if policies and regulations are not established" is a barrier in front of the adoption of blockchain-based technologies (Holotiuk & Moormann, 2018)." (Gokalp et al.,2022, p110. See also Clohessy & Acton 2019)

In terms of financial incentives Ciaian et al., 2021 noted mining rewards and costs as effective incentives for adoption and correct use of blockchain. Regardless of financial consequences, the need to keep up with peers, market leaders and the norms and requirements of an industry was noted as an incentive by Gokalp et al., 2022, who also found that the requirements of business partners were important incentives.

Conditions

Four papers on blockchain and organisational conditions were found of mixed quality (3 HQ and 1 MQ). Conditions important for the implementation of blockchain noted were:

- Top management support: Clohessy & Acton 2019, Gokalp et al., 2022
- Organisation size and/or resources: Clohessy & Acton 2019, Gokalp et al., 2022
- IT infrastructure: Gokalp et al., 2022
- Organisational readiness: Clohessy & Acton 2019
- Training: Clohessy & Acton 2019
- Clear decision-making attribution and accountability: Carvalho et al., 2021
- Accountability: Carvalho et al., 2021
- Dispute-resolution mechanisms & policies: Carvalho et al., 2021, who did not find these in practice

Gokalp et al., 2022 found that in practice:

> "The local ranking results of organizational context show that the organizations' IT resources (0.528) and financial resources (0.224) have comparably high local weights followed by top management support (0.116) and organization size (0.086). These results indicate that tangible and intangible technological resources and the amount of investment allocated for the decision of transition to the blockchain-based SCM systems are the most critical determinants of organizational adoption." (p114)

Al Ketbi et al., 2021, produced a new information security controls framework for BC as they found that there was a lack of governance in this area.

Consequences

Carvalho et al., 2021 (HQ) explored incorrect or malicious data loaded onto blockchain and how to deal with this, (given BC immutability), including identifying three possible solutions: 'do nothing', 'rollback', & 'overturn'. Each brought their own consequences, for example, with rollback:

> "all the transactions, no matter whether they are legitimate or not, are also erased when rolling back to a previous safe block. This might bring serious consequences. For example, consider the case when the attacker uses the stolen money to buy products from a vendor before the attack is detected. By rolling back to a block before the attack, that vendor might end up losing his/her money and be at a loss, while the original owner gets his/her money back" (p5)

Carvalho et al., 2021 stated that their key message was that it is essential to have dispute resolution committees to manage such issues. Gokalp et al., 2022 (HQ) found that a consequence of adoption of CC by the dominant partner in a supply chain could be that the other partners had to adopt the same technology.

4.7.3 Biometric & 2-Factor authentication (2FA)

4.7.3.1 Overview of the evidence

Biometric authentication was researched by three authors in relation to security, and 2-Factor Authentication by one. Table 7 indicates the paper's authors, dates, which topics were covered, the sector and the setting of the evidence. **The evidence was mixed quality**. Settings were predominantly Western and involved finance-related organisations.

Table 7

Authors / Date	Quality of evidence	Topics covered*	Sector	Setting
Li 2015 (2FA)	High	G, O	Finance	China
Venkatraman & Delpachitra, 2008	Medium	B, G, O, R	Banking	Western
Laux et al., 2011	Medium	B, D, O	Finance	Western
Riley et al., 2009	Low	C, D, O, R	General	India / South Africa / UK

*Topics covered = B – Benefits, C – Consequences, D = Decision-making processes, G – Regulations or other incentives, O – Organisational conditions, R – Risks.

Benefits

Two medium quality studies were available on the expected benefits of biometric authentication technology, in banking (Venkatraman & Dalpachitra, 2008) and in the financial sector, specifically credit unions (Laux et al., 2011). Venkatraman & Dalpachitra expected benefits would comprise competitive business advantage, improved productivity, and profitability because of greater consumer confidence in services using biometric authentication, and a reduction in security risks. Laux et al., 2011 added: that indicators cannot be easily compromised, duplicated, or used by anyone else, ease of use, increased speed of transaction times and reduced operating costs. They found that these factors were less important in their effect on adoption than readiness and external pressures e.g., from competitors, but stated that this might be to do with the nature of credit unions.

> "The culture of many credit unions supports this emphasis on simultaneous competition and cooperation with other institutions in their competitive environment. This suggests that it is important to consider the nature of the technology in combination with the firm's characteristics and industry position when examining stand-alone technologies such as biometrics" (p239)

Risks
Please see Table 5 for risk mitigating factors.

Decision-making
Riley et al., 2009 (LQ) rated environmental factors as important for biometric technology, arguing for consideration of cultural differences in perceptions, such as national levels of uncertainty tolerance or decision structures. Laux et al., 2011 (MQ) noted that:

> "Security spending decisions like other IT initiatives must align with the highest priorities and missions of the organization "(p6)

They stated that little research had been done on what affects decisions to adopt biometric authentication in organisations. They explored the factors affecting this in credit unions, finding that:

> "intent to adopt is driven by competitive factors [part of external pressures], an organization's financial resources [part of readiness], and the perceived benefits associated with the technology" (p221)

Security and privacy were an important factor, unsurprisingly. Riley et al., 2009 (LQ) looked at perceptions of biometric authentication in three different countries (the UK, South Africa, and India), finding unexpected cross-cultural differences, e.g., that Indians were more receptive to, and less worried about, the technology than either the British or South Africans.

> "Respondents from the United Kingdom…did not rate the technology in a positive way and large-scale consumer facing implementations in the context would likely face significant resistance." (p305)

Regulations and incentives
Regulations were seen as a powerful encouraging or constraining influence particularly on the adoption of 2FA (Venkatraman & Delpachitra 2008, MQ, Li 2015 HQ). For example:

> "government regulation has the strongest influence on OSPs [online security performances] and the adoption of 2FA" (Li 2015, HQ, p25)

In his paper on 2FA Li also suggested governments could help e-tailers with financial support for adopting mobile payment systems: "sponsoring the e-tailer to cover a part of the fixed cost of using technologies." (p2120)

Negative incentives encouraging 2FA adoption included:

- Risk of financial losses
- Damage to reputation
- Costs of repairs to system damage
- Loss of trust with partners, suppliers and customers and possible loss of contracts
- Reductions in stock price and shareholder value
- Penalties and fines

(Li 2015 HQ)

Conditions
There was a small amount of research in this area that suggested management support was not as important as commonly thought. Laux et al., 2011, for example, was surprised to find it not important for biometric adoption. They put this down to adoption being a requirement "in response

to pending legislative or industry association actions" (2011, p237) so the decision to adopt was out of management hands. This is interesting in indicating that security technologies may at times be adopted out of necessity and for compliance, rather than because of expected benefits, yet compliance ranked lowest overall as a benefit, see Section 4.1. Laux et al., 2011 (MQ), found that the organisational factors affecting intention to adopt biometrics included "financial resource readiness" and they produced "an organizational-level adoption model for biometrics" (p223). Venkatraman & Delpachitra 2008 (MQ) identified management and leadership factors as expected to be critical for successful adoption of biometrics, finding these only moderately important in practice. Li, on the other hand, found management support very important for adoption of 2FA.

Venkatraman & Delpachitra (2008) also cited availability of resources in the form of skilled staff, a viable security plan, robust infrastructure, and staff training programmes as necessary for successful adoption. Organisational culture was important: a 'silo' mentality and the failure to take a holistic, systemic, or dynamic approach could led to problems. Riley et al., 2009 (LQ), argued that organisational culture was important and needed to take account of national characteristics.

4.7.4 Cryptography

Table 8

Authors / Date	Technology studied	Quality of evidence	Topics covered*	Sector	Setting
Bierwisch et al., 2015	Homomorphic encryption	High	G, O	Finance	China
Kanger & Pruulmann-Vengerfeldt, 2015	Secure Multiparty Computation (SMC)	Medium	B, G, O, R	Banking	Western

*Topics covered = B – Benefits, C – Consequences, D = Decision-making processes, G – Regulations or other incentives, O – Organisational conditions, R – Risks.

Information on the general benefits of two cryptographies was found. Bierwisch et al., 2015, (HQ) expected homomorphic encryption to enable organisations to secure stored cloud data. Kanger & Pruulmann-Vengerfeldt 2015 (MQ) stated that Secure Multiparty Computation (SMC) adoption would mean that no prior anonymization of personal information and no filtration was needed. The authors expected that benefits would include high responsiveness, an ability to share all data, reduction of dependence on individual ethical integrity compared with traditional methods, reduction of incentives to withhold information as values cannot be seen anyway, improved speed and cost savings.

Kanger & Pruulmann-Vengerfeldt (2015: 48) identified five main organisational categories that need to be in place for good Secure Multiparty Computation adoption including information, need, task-technology fit, resources, and organizational fit. They defined 'organisational fit' as "the extent to which new technologies can be seamlessly integrated with the existing organizational practices" (p54). In practice they found that "in many ways the challenges met by SMC are one's characteristic of emerging technologies in general" (2015, p44).

4.7.5 Mobile payment systems

There was one medium quality paper by Fu et al. 2022 (MQ), on the adoption of mobile payment systems by Taiwanese micro-retailers. Expected benefits were identified as cost reduction and efficiency improvement, both being of medium weight effect. Please see Table 5 for risk mitigating factors.

In terms of regulation Fu et al., 2022 identified the following as useful for increasing adoption

- Promote the benefits of new technologies
- Offer financial incentives

Fu et al., 2022 listed eight critical factors affecting the adoption of mobile payment tools by micro-retailers, including two organisational factors: organisation size and information maturity. Overall, he found that technological factors were more important than organisational or environmental. As regards decision-making processes, he advised micro-retailers to assess their information systems using external providers and then identify the appropriate form of mobile payment to meet the critical factors.

In terms of unintended consequences, Fu et al., 2022 stated that mobile payment system instability could cause system failure, and this could lead to damaged customer relationships:

> "A MP system that is unstable and causes an existing system to become inoperable will severely affect the front desk payment times, operational efficiency, and, consequently, consumer satisfaction" (p5)

4.7.6 Smart cities

Kitchin & Dodge 2019 provided **medium quality evidence** about smart cities in a 2019 paper, including a list of expected risks (p54). These included, firstly, a lack of expertise:

> "Given cost constraints and lack of strategic foresight, very few cities presently have core security teams or CERTs and are therefore underprepared to deal with a serious cyberattack." (p58)

Secondly, they noted a lack of attention to security risks in procurement decisions, and a piecemeal approach to adoption whereby new technology was "slotted in" to existing systems:

> "in an ad hoc fashion with minimal strategic foresight. Given the potential harms and the associated costs that can arise, this piecemeal and make-do approach needs to be discontinued to be replaced with a more systemic and coordinated approach" (Kitchin & Dodge 2019 p59)

They argued for a systemic, holistic approach to procurement not that took account of the whole organisation rather than departmental silos. They also noted inequality and the creation of opportunities for crime as "unintended consequences and new variances of traditional problems" (p48) in smart cities and argued that risk identification by vendors and city administrators was inadequate.

Negative incentives against adoption included:

- Risk of financial losses
- Damage to reputation
- Costs of repairs to system damage
- Loss of trust with partners, suppliers and customers and possible loss of contracts
- Reductions in stock price and shareholder value
- Penalties and fines

On the positive side, regardless of financial consequences, the need to keep up with peers, market leaders and the norms and requirements of an industry was noted as a positive incentive.

Kitchin & Dodge 2019 advocated that in the context of smart cities security-by-design as well as ongoing maintenance should be ‘baked in’ to procurement processes and contracts “with the extent to which the proposed solutions meet desired parameters directly influencing the evaluation of tenders (Cerrudo, 2015).” (p59). They argued that dedicated cyber security staff and advanced security training was needed for the implementation of smart cities, and that responsibilities need to be clear.

4.7.7 Information Security Management Systems

There was only one medium quality paper on this. Chehrehpak et al., 2014, analysing an Information Security Management System (ISMS) in an Iranian marketing department, identified the following as expected benefits: limiting outsider access to organisational information, better preservation and integration of information, improved reliability, accountability, reduced concerns about data loss if an employee left and reduced need to establish physical security equipment such as CCTV cameras. In practice they identified a direct significant relationship between its adoption and the following actual benefits: increased information security, improved e-commerce and online sales procedures and more efficient storage and less inappropriate use of information. They found weak correlation but significant relationships (at 95%) between adoption and increased trust between management and staff, and adoption and better sharing of information. They found that the effect of limiting internal access to unnecessary information was small and, surprisingly, there was no significant relationship between adoption and improved customer trust and confidence. This contrasts with Donalds and Barclay’s 2022 conclusions about the importance of trust (Section 4.1.3).

5. Synthesis

5.1 The nature of the evidence base

5.1.1 Purpose of review

The purpose of the review was to gain an understanding of the issues relevant to the process of security technology adoption. It focused on current evidence about risks and benefits resulting from adoption, decision-making processes involved, incentives including regulation, the organizational conditions that need to be in put in place for a successful adoption and mitigation of risks, and the consequences of these changes.

5.1.2 Research questions

RQ1: What are the perceived benefits and risks of adopting new security technologies?

RQ2: What cognitive decision-making processes are utilised and shared in adoption discussions, policy, or process?

RQ3: What regulatory and other incentives are required to facilitate the process of security technology adoption?

RQ4: What are the organisational conditions and consequences of adopting new secure technologies?

5.1.3 The evidence base overall

Whilst there are many studies of technology adoption, fewer were expected concerning AoST. Sixty-six relevant articles were found in practice which is a reasonable body of evidence and provides adequate material with which to answer the research questions. However, coverage of some specific technologies was sparse (see Section 5.5). **Assessment of the evidence base showed that the articles were mixed in methodological quality: there were 29 high quality papers, 27 medium quality and 10 low quality.** Thirty-seven of the 66 papers (56%) were on security technologies generally and 29 (43%) on specific technologies (notably cloud computing with 12 papers and blockchain with seven).

Heterogeneity was a notable characteristic of the evidence base in terms of other characteristics also. In terms of study designs there was an even split between qualitative and quantitative items with eight papers using mixed methods as well. A variety of methodologies were used, including more than one in the same paper at times. The largest sets of methods were a) surveys of varying sizes and type i.e., questionnaire or interview (28 items), b) theoretical papers e.g., presenting models, frameworks (28 items), c) case studies, usually including interviews, observation, and document analysis (10 items) and d) literature reviews of different types e.g., traditional (4), systematic (3 items) and e) analysis of websites/documentation (3). There was also a cohort study (1) and use of the Delphi method (1). There were no randomised controlled trials (RCTs) or meta-analyses which is perhaps unsurprising. It would be hard to introduce an adoption of new security technology as an intervention plus control because of the scale, complexity and level of change and commitment involved with adoptions.

Most studies focused on more than one of the research question topics. In descending order of prevalence these topics were organisational conditions (56 articles), risks (35 articles), regulations and other incentives (29 articles), benefits (29 articles), decision-making (26) and organisational consequences (23). The proportion of good quality papers for each topic ranged from 42% (decision-making) to 65% (consequences). It is interesting that although organisational conditions was the largest group of papers, the highest proportion of high quality evidence was for consequences. This might be a function of the collection of empirical data for actual consequences. Specific sectors focused on in the papers were: general, non-specified or mixed (38), government (8), banking (5), ICT (4), education (3), retail, sales & marketing (3), finance (2), oil and gas (2) and energy (1). The largest proportion of primary studies, unexpectedly, used evidence from non-Western settings, however only by a small amount (26 are set in non-Western, and 24 in Western settings). Seven papers included a mixture of countries and for nine the national setting was unclear or irrelevant (e.g., as with a systematic literature review). India and China were the commonest non-Western settings in terms of specific countries, although five different countries from the Middle East were also found.

Consistency of the evidence is dealt with in the next section.

5.1.4 The evidence base for each research question

RQ1: What are the perceived benefits and risks of adopting new security technologies?

Benefits
Evidence regarding the actual or expected benefits of adopting secure technologies was of mixed quality with over half of the papers (52%) being of good quality. Heterogeneity was again a distinguishing characteristic. There was a mixture of study designs, with quantitative, qualitative and mixed methods studies; surveys using questionnaires and/or interviews (15), case studies (6), theoretical papers (4), literature reviews (1 traditional and 2 systematic literature reviews). Articles focused more often on the expected benefits than actual, empirically proved ones which is perhaps not surprising as these technologies are relatively recent. Most papers (79%) focused on a single technology with cloud computing attracting the most research attention, perhaps because it has been available in a limited form since the 1990s.

Evidence from studies using different methods consistently supported the commonest benefits as being reputational, financial, risk and compliance related.

- Reputational: there was a **good range of high-quality evidence** for this of more than one type based on a sizeable number of questionnaires and in-depth interviews
- Financial: there was a larger range of evidence of more than one type for this, including questionnaires and in-depth interviews
- Risk: again, there was a good range of evidence types, including questionnaires and in-depth interviews.
- Compliance: there was **less good quality evidence** for this consisting of only two papers based on questionnaires and interviews.

There was only **limited and inconsistent evidence** that adoption of secure technology improved the national economy in actuality.

Risks
Evidence regarding risks in relation to adopting new security technologies was of mixed quality with nearly half of the papers (46%) being of good quality. There was again a mixture of study designs with quantitative, qualitative, and mixed methods studies; theoretical papers (17 papers), questionnaire and/or interview surveys (11), case studies (7), SLRs (2) and use of the Delphi method (1). Overall, there was more on 'expected', common risks and more articles on general security technology adoption than articles on specific technologies. Evidence from studies using different methods consistently supported the major categories of risk as being technological, organisational, environmental and human/actor-related for expected risks. For unexpected risks the following was found:

- Technological: there was a **small range of mixed quality evidence** for this from 2 types of papers (a questionnaire survey and two case studies)
- Organisational: there was a **good range of high and medium quality evidence** for this of more than one type from 5 papers, including a literature review, theoretical papers, interviews and a case study
- Environmental: there was little evidence for this other than a literature review of 76 papers, 41% of which relied on empirical data
- Human/actor-related: there was **mixed quality evidence** for this from more than one type of study, including interviews and a questionnaire survey.

RQ2: What cognitive decision-making processes are utilised and shared in adoption discussions, policy or process?

Evidence for decision-making processes was mixed with 42% of papers being assessed as of good quality. They included quantitative, qualitative, and mixed methods studies; questionnaire and/or interview surveys (17 papers), theoretical papers (7), case studies (1), a cohort study (1), an SLR (1) and the Delphi method (1). Articles were split evenly between those focusing on specific technologies and more general papers. There was little evidence found discussing decision-making as a process or on the stages of decision-making, with the majority of the material dealing with the content of decisions. The evidence consistently supported acknowledgement that four factors (technological, organisational, environmental and human/actor-related) were important, but there was no consistent agreement as to which was the most important, with different authors making the case for different factors.

RQ3: What regulatory and other incentives are required to facilitate the process of security technology adoption?

In this section **evidence was also mixed with 45% of papers assessed as of good quality**. Quantitative, qualitative, and mixed methods studies were included with specific study designs being theoretical papers (14), questionnaire or interview surveys (11), case studies (7), systematic literature reviews (3), traditional literature reviews (1), and the Delphi method (1). There were slightly more papers on specific technologies than general ones. The evidence consistently supported the importance of government support. Four types of incentives were identified:

- Regulatory: there was a **large amount of high quality evidence** for the importance of regulatory and other government-related incentives. This came from a range of types of types of evidence including document and website analysis, case studies, interview and questionnaire surveys.
- Financial: there was a **smaller amount of mainly high quality evidence** for the usefulness or otherwise of financial incentives such as bonuses. This was from more than one type of evidence including interviews and document analysis
- Social: there was a **good range of high and medium quality evidence** concerning social incentives (e.g., pressure from customers, peers or business partners). This was from a range of types of evidence including document analysis, questionnaire surveys and interviews
- Personal: there was a **small amount of high quality evidence** regarding personal incentives. Both studies were based on questionnaire surveys

RQ4: What are the organisational conditions and consequences of adopting new security technologies?

Organisational conditions

There was **a large amount of mixed quality evidence, with 43% of papers assessed as good.** Methods were quantitative, qualitative, and mixed, with specific study designs being questionnaire or interview surveys (21), theoretical papers (17), case studies (8), systematic literature reviews (3), traditional literature reviews (1), the Delphi method (1) and a cohort study (1). Most of the papers covered general security technologies. There was a substantial amount of **consistent high and medium quality evidence** for the importance of the right organisational culture, management support for the adoption and education and training of staff. Other factors were also recognised as important, and authors advocated a holistic approach with consideration of multiple factors.

Organisational consequences
The evidence quality here was mixed but this had by far the highest proportion of good quality papers at 65% of the evidence base. Methods were quantitative, qualitative, and mixed, with specific study designs being questionnaire or interview surveys (11), theoretical papers (10), case studies (2), systematic literature reviews (1) and the Delphi method (1). There was an even split between papers on specific technologies and papers on general security technologies. It is important to note that there was a small amount of **high quality, consistent evidence** that the period following the adoption of new security technologies is a risky time for an organisation when there may be more security breaches. There was no consensus on the explanation for this.

5.1.5 Specific technologies

5.1.5.1 Blockchain and cloud computing (CC)

Cloud computing accounts for 12 of the 32 papers (37.5%) on specific technologies and blockchain accounts for 7/32 (22%). Six of the seven papers for blockchain were of good quality, where the **evidence for cloud computing was mixed**, with only two high quality papers, 6 medium quality and 4 low quality ones. There are several possible explanations for this:

- There are many low quality blockchain studies, but these tend to be published in lesser quality journals, conferences etc. which have been excluded from this evidence base.
- CC has been around for longer than blockchain and therefore has more research on it which opens the opportunity for more poor as well as good quality studies.
- CC is less controversial than blockchain and sparks less debate. This may mean that blockchain researchers must prove their cases with greater rigour. Reviewers might be more critical when reviewing a manuscript
- CC is a more accessible concept and may attract researchers with less technical understanding or research skill than BC.

5.1.5.2 Biometric and Two-Factor Authentication

The evidence for this is mixed with one high quality paper, two medium quality ones and one low quality paper. The three highest quality papers all investigated finance-related organisations.

5.1.5.3 Other specific technologies

This covers:

- Cryptography: two papers, one of high quality, one of medium.
- Information Management Security Systems: one medium quality paper.
- Mobile payment systems: one medium quality paper
- Smart city technology: one medium quality paper
- 5G technology: one medium quality paper

Clearly, evidence in these areas is sparse which may suggest possibilities for future research.

5.2 What the evidence indicates

5.2.1 Benefits and risks of adopting new security technologies

New security technologies are adopted for the potential benefits they can actualise for an organisation if they are used. After critical quality assessment of the evidence this RER demonstrated that four main types of benefits were both expected and found in practice: reputational, financial, risk-related, and compliance-related. The review showed that benefits were intertwined especially reputation and finance. It was interesting to note that there was more evidence for actual business/financial benefits than for actual risk-reduction/compliance-related benefits. This suggested that adopting new security technologies can be seen as a useful business proposition and not solely as a security issue. Seeing security technologies as costs rather than as contributing to profitability has been a common barrier reducing enthusiasm for them, so this review provides evidence to challenge that.

In addition to these general benefits, specific technologies and sectors brought their own advantages. For example, the distributed nature of blockchain improved privacy and immutability of data. The pay-as-you-go nature of cloud computing brought improvements in scalability, and access to hitherto inaccessible resources, as well as 'green' advantages. Specific organisational conditions are also important and can determine differences in benefits achieved, e.g., Berlilana et al., 2021 (HQ) showed that organisational security readiness mediated the achievement of benefits in practice.

The four main categories of risk brought by adopting new security technology were technological, organisational, environmental and human/actor-related for both actual and unexpected risks. These categories encompassed many specific risks. There is clear evidence of the need for the holistic assessment of risks taking account of all the categories. Whilst technological factors are not now regarded as the only issues (as had been the case in the past) there was a suggestion that there may now be too much emphasis on human factors. Organisational factors, in particular, have not received adequate attention by organisations in the recent past which can lead to very serious issues.

There is also a need to recognise that risks can inter-relate and their impact may not be confined to the system adopted: they may affect other systems used by the organisation, and this needs to be taken into consideration in risk assessment. Managing risks is not a one-off event but needs to be considered throughout the lifecycle of the technology from initial planning onward. For example, it is not enough to form a supportive security culture initially and then allow it to lapse. This must be sustained over time. Uncertainty is an inevitable part of risk as some new technologies and changes in the organisation and its environment will not be foreseeable.

5.2.2 Consequences of adoption

As well as the achievement of benefits, adoption may lead to unexpected risks (discussed above) and unplanned organisational consequences. The evidence showed that it is important to recognise that the period shortly after adoption and implementation of new security technologies can be a risky one because of knowledge gaps engendered (probably particularly if inadequate attention is given to education and training, including time for familiarisation) and the dangers of risk homeostasis. Again, a holistic approach to assessing possible consequences is needed, and time is an important dimension. As with risks, it is important to plan ahead and the evidence base includes a tool for estimating unforeseen consequences (Lee et al., 2016, HQ).

5.2.3 Conditions / mitigating risks

Risks and unexpected consequences can be mitigated by good decision-making, implementation of the right organisational conditions, and by the adequacy of external supports such as regulations.

There is little on decision-making processes other than two MQ papers. Goldman's 2012 work makes it clear that a heuristic approach to decision-making is unhelpful. Instead, there is a need to adopt a defined process ("orderly, repeatable, and measurable procedures" as Goldman put it) and to plan: something which he identified as lacking at the time. Important decision-making steps extrapolated from the paper included analysing requirements, setting goals, planning, risk assessment, developing a business case, training, and documentation development. Goldman also argued for the importance of selecting and using high quality information. He and Laux et al., 2011 both agreed that the decision-making around adoption of new technologies is a process over time, not a one-off event. The need to ensure that the benefits of technology are realised through appropriate use meant that employee compliance was an important issue for researchers: decision-making does not stop with technology installation as its success depends on user engagement with the product.

Most of the research attention in this area concentrates on the factors or organisational conditions that need to be decided upon. The evidence base showed this includes technological, organisational, environmental, and human factors. There was no agreement on which was the most important category with this varying by technology and characteristics of the specific organisation. Specific organisational factors identified as particularly important for successful adoption and implementation included: organisational culture, management support and training and education (the last was the most frequently mentioned factor in the frameworks and models developed in the research to aid governance and security). Other factors included governance arrangements, resources, having the right infrastructure in place, having, or developing appropriate processes e.g., risk management, and ongoing audit and accountability.

The evidence also showed that government regulation was an important factor affecting uptake and adoption. Regulations could encourage or constrain this. Cross-national technologies brought particular issues and could be confusing, so Goldman 2012 recommended a clearinghouse to aid this. The evidence showed that governments could do more than simply legislate to encourage adoption, e.g., adopting technologies themselves would encourage uptake. There was less information on other incentives with the **evidence for financial incentives being mixed**. Social pressures and personal factors received some attention.

6. Conclusions

The evidence in this RER 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.

7. Limitations

As this is a rapid evidence review there is a possibility that some studies were missed. This may be particularly the case concerning legal compliance, and in terms of conference papers which were excluded. Only one database (Scopus) was used, but so much material was found that it was not deemed necessary or feasible to continue with other databases. There was no hand citation searching or searches of 'grey' literature for the same reason.

The material retained was focused on certain sectors such as business, energy, health, and ICT. Medical and scientific journals were excluded. As a result, the views of security technology designers are not here represented.

Articles assessed as of low relevance were excluded from the final data set, to make the evidence base manageable. However, low quality evidence has not been excluded if it remained relevant to a high or medium extent.

Finally, two of the critical appraisal sheets were not validated (for conceptual papers and for design science research. The latter was only used once.). However, they were based on evidence from experts in the respective fields.

8. Implications for practice

The research has several implications for practice and is particularly relevant to business organisations. Firstly, it conveys the importance of a holistic approach to adoption as requiring considerations of many different types of factors (technological, organisational, environmental and human/actor-related).

Secondly, once adopted the technology (even if a good risk assessment has been done) may still cause unexpected risks and unintended consequences. It is important to acknowledge and prepare for this as far as is possible with good future planning that takes uncertainty into account. The evidence base indicates tools that can assist this.

Thirdly, adoption is a process taking place over time and the period after installation is as important as that leading up to it. Education and training of staff are highlighted as an important factor along with a good security culture and management support throughout.

Fourthly, there is evidence indicating the importance of security by design and the need to include it from the start of system adoption (see Kitchin & Dodge 2019 and Schinagl & Shahim 2020).

Finally, in line with the Duality of Technology theory (Orlikowski 1992, Brous et al., 2020) there will be ongoing interactions between the technology and the organisation that need to be borne in mind by those considering implementing new technology. (See Wang et al., 2021 within the evidence base for a detailed case study illustrating this.) Writing about the Internet of Things, Brous et al., (2020) summarised:

> "adoption is a continuous cycle, as new knowledge and organizational forms provide new requirements and uses for the technology which drives further development of the technology. These new technological advances then, in turn have a social impact on the organization and people etc. Benefits of IoT are often only achieved once the institutional conditions of IoT adoption have been met, and the institutional consequences of IoT adoption have been accepted. These conditions and consequences often then lead to new insights, uses, and requirements." (Brous et al., 2020, p14)

Technology offers affordances for the achievement of benefits which can be realised when humans adopt and use it. The technology requires appropriate organisational conditions, and so impacts on the organisation, bringing working practice changes to some or all of the staff. These will then become embedded as the accepted way of working. However, the people/organisation using the system may bring ideas for use which were not expected by designers, or they may encounter unexpected issues. (“the use of IT in organizations is an outcome of compromise between the user's intention and the designer's intention” Wang et al., 2021 (HQ)). These may lead to unexpected impacts of the actors upon the technology e.g., the creation of workarounds, reconfiguration and other compromises which change the technology from its intended model. These too may become embedded, but over time organisational needs will change again, and new technology and ways of working appear. This requires further changes to the technology (or its replacement) which again will impact upon the organisation’s structures and staff work practices and behaviours. In short, as Wang et al., state:

> “The notions of emergent structure and enactment suggest that our attention should focus on the ongoing, recursive relationship between IT and people who use IT continuously, rather than on the functions of a technology and the one-off adoption and use of these functions” (2021, p2)

References

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 System Security, 17(2), 103-124.

Al-Darwish, A.I. & Choe, P. (2020). Application of a human factors-integrated information security framework to an oil and gas organization. In *Advances in Intelligent Systems and Computing* book series, 1018, 731-736. DOI: 10.1007/978-3-030-25629-6_114

Al Hogail, A. (2015). Cultivating and assessing an organizational information security culture; an empirical study. *International Journal of Security and Its Applications*, 9(7), 163-178. DOI: 10.14257/ijsia.2015.9.7.15

Al Ketbi, M., Shuaib, K., Barka, E. & Gergely, M. (2021). Establishing a security control framework for blockchain technology. *Interdisciplinary Journal of Information, Knowledge, and Management*, 16, 307-330. DOI: 10.28945/4837

AlAbdulkarim, L. & Lukszo, Z. (2010). Integrating information security requirements in critical infrastructures: smart metering case. *International Journal of Critical Infrastructures*, 6(2), 187-209

Alassafi, M.O., Alharthi, A., Alenezi, A., Walters, R.J. & Wills, G.B. (2016). Investigating the Security Factors in Cloud Computing Adoption: Towards Developing an Integrated Framework. *Journal of Internet Technology and Secured Transactions (JITST)*, 5(2), 486-494. DOI: 10.20533/jitst.2046.3723.2016.0061

Alizadeh, A., Chehrehpak, M., Nasr, A.K. & Zamanifard, S. (2020). An empirical study on effective factors on adoption of cloud computing in electronic banking: a case study of Iran banking sector. *International Journal of Business Information Systems*, 33(3), 408-428. DOI: 10.1504/IJBIS.2020.105833

Alqahtani, M.S.A. & Erfani, E. (2021). Exploring the relationship between technology adoption and cyber security compliance: A quantitative study of UTAUT2 model. *International Journal of Electronic Government Research,* 17(4), 40-62. DOI: 10.4018/IJEGR.2021100103

Alshammari, S.H. & Rosli, M.S. (2020). A review of technology acceptance models and theories. *Innovative Teaching and Learning Journal*, 4 (2), 12–22.

Anderson, E.E. (2010). Firm objectives, IT alignment, and information security. *IBM Journal of Research & Development*, 54(3). DOI: 10.1147/JRD.2010.2044256

Armenia, S., Angelini, M., Nonino, F., Palombi, G. & Schlitzer, M.F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems,* 147. DOI: 10.1016/j.dss.2021.113580

Awa, H.O. & Ojiabo, O.U. (2016). A model of adoption determinants of ERP within T-O-E framework. *Information Technology & People*, 29(4), 901-930. DOI 10.1108/ITP-03-2015-0068

Balozian, P., Leidner, D. & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, 59(3), 197-210. DOI: 10.1080/08874417.2017.1318687

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(13761). DOI: 10.3390/su132413761

Bierwisch, A., Kayser, V. & Shala, E. (2015). Emerging technologies in civil security—A scenario-based analysis. *Technological Forecasting and Social Change*, 101, 226-237. (E. Shala). DOI: 10.1016/j.techfore.2015.06.014

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. DOI: 10.1016/j.ijinfomgt.2019.05.008

Bu, F., Wang, N., Jiang, B. & Jiang, Q. (2021). Motivating information system engineers' acceptance of Privacy by Design in China: An extended UTAUT model. *International Journal of Information Management,* 60. DOI: 10.1016/j.ijinfomgt.2021.102358

Cagliano, A.C., Grimaldi, S. & Rafele, C. (2015). Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research,* 18(2), 232-248, DOI: 10.1080/13669877.2014.896398

Cannoy, S.D. & Salam, A.F. (2010). A framework for health care information assurance policy and compliance. *Communications of the ACM,* 53(3), 126-131. DOI: 10.1145/1666420.1666453

Carvalho, A., Merhout, J.W., Kadiyala, Y. & Bentley II, J. (2021). When good blocks go bad: Managing unwanted blockchain data. *International Journal of Information Management*, 57. DOI: 10.1016/j.ijinfomgt.2020.102263

Chehrehpak, M., Afsharian, S.P. & Roshandel, J. (2014). Effects of implementing information security management systems on the performance of marketing and sales departments. *International Journal of Business Information Systems*, 15(3), 291-306. DOI: 10.1504/IJBIS.2014.059752

Chiniah, A., Mungur, A.E.U. & Permal, K.N. (2019). Evaluation of cloud computing adoption using a hybrid TAM/TOE model. *Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing*, 863, DOI: 10.1007/978-981-13-3338-5_24

Ciaian, P., Kancs, d'A. & Rajcaniova, R. (2021). Interdependencies between mining costs, mining rewards and blockchain security. *Annals of Economics and Finance*, 22(1), 25–62. DOI: 10.48550/arXiv.2102.08107

Clohessy, T. & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption. An innovation theory perspective. *Industrial Management & Data Systems,* 119(7), 1457-1491. DOI 10.1108/IMDS-08-2018-0365

Da Veiga, A. & Eloff, J.H.P. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361-372. DOI: 10.1080/10580530701586136

Damenu, T.K. & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. *Information & Computer Security*, 25(3), 240-258. DOI 10.1108/ICS-07-2016-0053

Dhillon, G., Syed, R. & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & security*, 56, 63–69. DOI: 10.1016/j.cose.2015.10.001 0167-4048/

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. DOI: 10.1080/0960085X.2021.1978344

El Khoury, R., Nasrallah, N. & Harb, E.G. (2022). Did the intensity of countries' digital transformation affect IT companies' performance during covid-19? *Journal of Decision Systems*, DOI: 10.1080/12460125.2022.2094528

Fichtner, L. (2018). What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches. *Internet Policy Review,* 7(2), 1–19

Fu, H-P., Chang, T-S., Wang, C-N., Hsu, H-P., Liu, C-H. & Yeh, C-Y. (2022). Critical factors affecting the introduction of mobile payment tools by microretailers. *Technological Forecasting & Social Change*, 175. DOI: 10.1016/j.techfore.2021.121319

Gangwar, H. & Date, H. (2015). Exploring information security governance in cloud computing organisation. *International Journal of Applied Management Sciences and Engineering*, 2(1), 44-61. DOI: 10.4018/ijamse.2015010104

Garg, P., Gupta, B., Chauhan, A.K., Sivarajah, U., Gupta, S. & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological Forecasting & Social Change*, 163. DOI: 10.1016/j.techfore.2020.120407

Gokalp, E., Gokalp, M.U. & Coban, S. (2022). Blockchain-based supply chain management: Understanding the determinants of adoption in the context of organizations. *Information Systems Management*, 39(2), 100-121. DOI: 10.1080/10580530.2020.1812014

Goldman, E. (2012). The effect of acquisition decision making on security posture. *Information Management & Computer Security,* 20(5), 350-363. DOI 10.1108/09685221211286520

Golightly, L., Chang, V., Xu, Q.A., Gao, X. & Liu, B.S.C. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*, 14, 1–17 DOI: 10.1177/18479790221093992

Groner, R. & Brune, P. (2012). Towards an empirical examination of IT security infrastructures in SME. Eds. Josang, A. & Carlsson, B. Secure IT Systems. *Lecture Notes in Computer Science 7617*, 73-88. DOI 10.1007/978-3-642-34210-3

Hashemi, S., Monsaredi, K. & Hashemi, S.Y. (2015). Cloud computing for secure services in e-government architecture. *Journal of Information Technology Research*, 8(1), 43-61. DOI: 10.4018/JITR.2015010104

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. *The DATA BASE for Advances in Information Systems*, 51(2), 12-35. DOI: 10.1145/3400043.3400046

Hevner, A.R., March, S.T., Park, J. & Ram, S., (2004). Design science in IS research. *MIS Quarterly*, 28(1), 75-105. DOI: 10.1007/978-1-4419-5653-8

Higgs, J.L., Pinsker, R.E., Smith, T.J. & Young, G.R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, 30(3), 79-98. DOI: 10.2308/isys-51402

Ihmouda, R., Alwi, N.H.M. & Abdullah, I. (2015). Successful factors on e-government security social-technical aspect. *ARPN Journal of Engineering and Applied Sciences*, 10(20), 9640-9649.

Jaakkola, E. (2020). Designing conceptual articles: four approaches. *AMS Review,* 10,18–26. DOI: 10.1007/s13162-020-00161-0

Jackson, S. (2016). Understanding IS/IT implementation through metaphors: A multi-metaphor stakeholder analysis in an educational setting. *Computers in Human Behavior*, 55, 1039-1051. DOI: 10.1016/j.chb.2015.09.039 0747-5632/

Eds. Schmitt, B., Cotte, J., Giesler, M., Stephen, A. & Wood, S. 26 February 2021, Evaluating conceptual papers. *Journal of Consumer Research*, (Evaluating Conceptual Papers - Journal of Consumer Research (consumerresearcher.com)

Jardine, E. (2020). The case against commercial antivirus software: risk homeostasis and information problems in cyber security. *Risk Analysis*, 40(8), 1571-1588. DOI: 10.1111/risa.13534

Kanger, L. & Pruulmann-Vengerfeldt, P. (2015). Social need for secure multiparty computation. In *Applications of Secure Multiparty Computation*, Laud, P. & Kamm, L. (Eds.), 43-57. DOI:10.3233/978-1-61499-532-6-43

Kefallinos, D., Lambrou, M.A. & Sykas, E.D. (2009). An extended risk assessment model for secure e-government projects. *International Journal of Electronic Government Research*, 5(2), 72-92. DOI: 10.4018/jegr.2009040105

Khan, S.N., Nicho, M., Takruri, H., Maamar, Z. & Kamoun, F. (2019). Role assigning and taking in cloud computing. *Human Systems Management,* 38, 1–27. DOI 10.3233/HSM-180336

Khayer, A., Jahan, N., Hossain, M.N. & Hossain, M.Y. (2021). The adoption of cloud computing in small and medium enterprises: A developing country perspective. *VINE Journal of Information and Knowledge Management Systems*, 51(1), 64-91. DOI 10.1108/VJIKMS-05-2019-0064

Kitchin, R. & Dodge, M. (2019). The (in)security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology*, 26(2), 47-65. DOI: 10.1080/10630732.2017.1408002

Koskosas, I. (2011). E-banking security: A communication perspective. *Risk Management*, 13(1/2), 81–99. DOI: 10.1057/rm.2011.3

Krishna, B & Sebastian, M.P. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis. *Information & Computer Security*, 29(5), 737-760. DOI 10.1108/ICS-12-2020-0205

Lam, W.M.W. & Seifert, J. (2021). *Regulatory interactions and the design of optimal cyber security policies. Final Project Report* Prepared for the Digital Security by Design Social Science (Discribe) Hub+

Laux D., Luse, A., Mennecke, B. & Townsend, A.M. (2011). Adoption of biometric authentication systems: Implications for research and practice in the deployment of end-user security systems. *Journal of Organizational Computing and Electronic Commerce*, 21(3), 221-245. DOI: 10.1080/10919392.2011.590111

Lee, C., Kim J. & Lee, S. (2016). Towards robust technology roadmapping: How to diagnose the vulnerability of organisational plans. *Technological Forecasting & Social Change*, 111, 164-175. DOI: 10.1016/j.techfore.2016.06.022

Li, D.C. (2015). Online security performances and information security disclosures. *Journal of Computer Information Systems*, 55(2), 20-28. DOI: 10.1080/08874417.2015.11645753
Liveley, G. & Coles-Kemp, L. (2022). *Futures*. Discribe Hub+, UKRI, UK

Liu, C., Wang, N. & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, 54. DOI: 10.1016/j.ijinfomgt.2020.102152

Luo, S. & Choi, T-M. (2022). E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Productions & Operations Management*, 31, 2107–2126. DOI: 10.1111/poms.13666

OpenPath. (2022). Security Technology Overview & Industry Trends for 2022 (openpath.com). Accessed 23/5/23

Orlikowski, W.J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*,3(3), 398-427. DOI:10.1287/orsc.3.3.398

Oxford English Dictionary. (2023). Oxford University Press: Oxford

Park, S-T., Park, E-M., Seo, J-H. & Li, G. (2016). Factors affecting the continuous use of cloud service: focused on security risks. *Cluster Computing*, 19, 485–495. DOI 10.1007/s10586-015-0516-y

Pathari, V. & Sonar, R.M. (2013). Deriving an information security assurance indicator at the organizational level. *Information Management & Computer Security*, 21(5), 401-419. DOI 10.1108/IMCS-02-2013-0011

Ponemon Institute. (2022). Security Innovation: Secure Systems Start with Foundational Hardware. Ponemon Institute LLC: USA

Priyadarshinee, P., Raut, R.D., Jha, M.K. & Gardas, B.B. (2017). Understanding and predicting the determinants of cloud computing adoption: A two staged hybrid SEM - Neural networks approach. *Computers in Human Behavior*, 76, 341-362. DOI: 10.1016/j.chb.2017.07.027

Qian, Y., Fang, Y. & Gonzalez, J.J. (2012). Managing information security risks during new technology adoption. *Computers & Security*, 31, 859-869. DOI: 10.1016/j.cose.2012.09.001

Radu, R. & Amon, C. (2021). The governance of 5G infrastructure: between path dependency and risk-based approaches. *Journal of Cyber security*, 1–16. DOI: 10.1093/cybsec/tyab017

Rajan, R., Rana, N.P., Parameswar, N., Dhir, S., Sushil, & Dwivedi, Y.K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cyber security management. *Technological Forecasting & Social Change*, 170. DOI: 10.1016/j.techfore.2021.120872

Raut, R.D., Priyadarshinee, P., Gardas, B.B. & Jha, M.K. (2018). Analyzing the factors influencing cloud computing adoption using three stage hybrid SEM-ANN-ISM (SEANIS) approach. *Technological Forecasting & Social Change,* 134, 98-123. DOI: 10.1016/j.techfore.2018.05.020

Riley, C., Buckner, K., Johnson, G. & Benyon, D. (2009). Culture & biometrics: Regional differences in the perception of biometric authentication technologies. *AI & Society*, 24, 295–306. DOI 10.1007/s00146-009-0218-1

Rogers, E.M. (2003). Diffusion of Innovations, 5th Edition, Free Press. ProQuest Ebook Central,

Schinagl, S. & Shahim, A. (2020). What do we know about information security governance? “From the basement to the boardroom”: Towards digital security governance. Information & Computer Security, 28(2), 261-292. DOI 10.1108/ICS-02-2019-0033

Sener, U., Gokalp, E. & Eren, P.E. (2016). Cloud-based enterprise information systems: determinants of adoption in the context of organizations. *Communications in Computer and Information Science,* 639, 53-66. DOI: 10.1007/978-3-319-46254-7_5

Shein, E. (2022). A brief history of cloud computing. A Brief History of Cloud Computing | TechRepublic, downloaded 15/05/23

Sivan-Sevilla, I. (2021). Framing and governing cyber risks: comparative analysis of U.S. Federal policies [1996–2018]. *Journal of Risk Research*, 24(6), 692-720. DOI: 10.1080/13669877.2019.167379

Skarzauskiene, A., Maciuliene, M. & Bar, D. (2021). Developing blockchain supported collective intelligence in decentralized autonomous organizations. K. Arai et al. (Eds.): FTC 2020, *AISC 1290,* 1018–1031. DOI: 10.1007/978-3-030-63092-8_70

Swamy, S. (2013). Cloud computing adoption journey within organizations. P.L.P. Rau (Ed.): *Cross-Cultural Design: Cultural differences in everyday life*, *Lecture Notes in Computer Science,* 8024, part II, 70–78. DOI 10.1007/978-3-642-39137-8

Tafokeng Talla, L. & Robert, K.K.J. (2019). Factors influencing adoption of information security in information systems projects. Á. Rocha et al. (Eds.): WorldCIST'19, *AISC* 931, 890–899. DOI: 10.1007/978-3-030-16184-2_84

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, 22, 960-967. 10.1016/j.promfg.2018.03.137

Thalmann, S., Bachlechner, D., Demetz, L. & Manhart, M. (2014). Complexity is dead, long live complexity! How software can help service providers manage security and compliance. *Computers & Security*, 45, 172-185. DOI: 10.1016/j.cose.2014.05.012

Venkatraman, S. & Delpachitra, I. (2008). Biometrics in banking security: A case study. *Information Management & Computer Security*, 16(4), 415-430. DOI 10.1108/09685220810908813

Wang, D., Wang, J. & Xiang, Z. (2021). Imbrications of IT and hospitality organizations. *Annals of Tourism Research Empirical Insights*, 2(2). DOI: 10.1016/j.annale.2021.100021

Wu, Y. & Saunders, C. (2011). Governing information security: governance domains and decision rights allocation patterns. *Information Resources Management Journal*, 24(1), 28-45. DOI: 10.4018/irmj.2011010103.

Yasar, K. (June 2022). *TechTarget.* What is Hardware Security? (techtarget.com). Accessed 31/05/23
Yin, R.K. (2009). Case studies research: design and methods. 4th Edition. London: Sage.

Appendix 1: Remaining search strings

a) (KEY (org*) AND KEY (tech*) AND KEY (decision*)) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ENVI") OR LIMIT-TO (SUBJAREA , "AGRI") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "ENER") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "HEAL") OR LIMIT-TO (SUBJAREA , "NURS") OR LIMIT-TO (SUBJAREA , "MULT")) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011) OR LIMIT-TO (PUBYEAR , 2010) OR LIMIT-TO (PUBYEAR , 2009) OR LIMIT-TO (PUBYEAR , 2008) OR LIMIT-TO (PUBYEAR , 2007) OR LIMIT-TO (PUBYEAR , 2006) OR LIMIT-TO (PUBYEAR , 2005) OR LIMIT-TO (PUBYEAR , 2004) OR LIMIT-TO (PUBYEAR , 2003) OR LIMIT-TO (PUBYEAR , 2002) OR LIMIT-TO (PUBYEAR , 2001)) AND (LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (EXACTKEYWORD , "Controlled Study") OR EXCLUDE (EXACTKEYWORD , "Biomedical Technology Assessment") OR EXCLUDE (EXACTKEYWORD , "Diseases") OR EXCLUDE (EXACTKEYWORD , "Biological Organs") OR EXCLUDE (EXACTKEYWORD , "Nonbiological Model") OR EXCLUDE (EXACTKEYWORD , "Neural Networks") OR EXCLUDE (EXACTKEYWORD , "Support Vector Machines") OR EXCLUDE (EXACTKEYWORD , "Evidence Based Medicine")) AND (EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "MATH") OR EXCLUDE (SUBJAREA , "BIOC") OR EXCLUDE (SUBJAREA , "MATE") OR EXCLUDE (SUBJAREA , "CENG") OR EXCLUDE (SUBJAREA , "EART") OR EXCLUDE (SUBJAREA , "PHYS") OR EXCLUDE (SUBJAREA , "CHEM") OR EXCLUDE (SUBJAREA , "PHAR") OR EXCLUDE (SUBJAREA , "IMMU") OR EXCLUDE (SUBJAREA , "NEUR") OR EXCLUDE (SUBJAREA , "VETE") OR EXCLUDE (SUBJAREA , "DENT"))

b) (KEY (reg*) AND KEY (tech*) AND KEY (implement*)) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ENVI") OR LIMIT-TO (SUBJAREA , "AGRI") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "ENER") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "HEAL") OR LIMIT-TO (SUBJAREA , "NURS") OR LIMIT-TO (SUBJAREA , "MULT") OR EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "MATH") OR EXCLUDE (SUBJAREA , "BIOC") OR EXCLUDE (SUBJAREA , "MATE") OR EXCLUDE (SUBJAREA , "CENG") OR EXCLUDE (SUBJAREA , "EART") OR EXCLUDE (SUBJAREA , "PHYS") OR EXCLUDE (SUBJAREA , "CHEM") OR EXCLUDE (SUBJAREA , "PHAR") OR EXCLUDE (SUBJAREA , "IMMU") OR EXCLUDE (SUBJAREA , "NEUR") OR EXCLUDE (SUBJAREA , "VETE") OR EXCLUDE (SUBJAREA , "DENT")) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011) OR LIMIT-TO (PUBYEAR , 2010) OR LIMIT-TO (PUBYEAR , 2009) OR LIMIT-TO (PUBYEAR , 2008) OR LIMIT-TO (PUBYEAR , 2007) OR LIMIT-TO (PUBYEAR , 2006) OR LIMIT-TO (PUBYEAR , 2005) OR LIMIT-TO (PUBYEAR , 2004) OR LIMIT-TO (PUBYEAR , 2003) OR LIMIT-TO (PUBYEAR , 2002) OR LIMIT-TO (PUBYEAR , 2001)) AND (LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (EXACTKEYWORD , "Controlled Study") OR EXCLUDE (EXACTKEYWORD , "Biomedical Technology Assessment") OR EXCLUDE (EXACTKEYWORD , "Diseases") OR EXCLUDE (EXACTKEYWORD , "Biological Organs") OR EXCLUDE (EXACTKEYWORD , "Nonbiological Model") OR EXCLUDE (EXACTKEYWORD , "Neural Networks") OR EXCLUDE (EXACTKEYWORD , "Support Vector Machines") OR EXCLUDE (EXACTKEYWORD , "Evidence Based Medicine"))

c) (KEY (gov*) AND KEY (sec*) AND KEY (tech*)) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "HEAL") OR LIMIT-TO (SUBJAREA , "NURS") OR LIMIT-TO (SUBJAREA , "MULT") OR EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "MATH") OR EXCLUDE (SUBJAREA , "BIOC") OR EXCLUDE (SUBJAREA , "MATE") OR EXCLUDE (SUBJAREA , "CENG") OR EXCLUDE (SUBJAREA , "EART") OR EXCLUDE (SUBJAREA , "PHYS") OR EXCLUDE (SUBJAREA , "CHEM") OR EXCLUDE (SUBJAREA , "PHAR") OR EXCLUDE (SUBJAREA , "IMMU") OR EXCLUDE (SUBJAREA , "NEUR") OR EXCLUDE (SUBJAREA , "VETE") OR EXCLUDE (SUBJAREA , "DENT")) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011) OR LIMIT-TO (PUBYEAR , 2010) OR LIMIT-TO (PUBYEAR , 2009) OR LIMIT-TO (PUBYEAR , 2008) OR LIMIT-TO (PUBYEAR , 2007) OR LIMIT-TO (PUBYEAR , 2006) OR LIMIT-TO (PUBYEAR , 2005) OR LIMIT-TO (PUBYEAR , 2004) OR LIMIT-TO (PUBYEAR , 2003) OR LIMIT-TO (PUBYEAR , 2002) OR LIMIT-TO (PUBYEAR , 2001)) AND (LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (EXACTKEYWORD , "Controlled Study") OR EXCLUDE (EXACTKEYWORD , "Biomedical Technology Assessment") OR EXCLUDE (EXACTKEYWORD , "Diseases") OR EXCLUDE (EXACTKEYWORD , "Biological Organs") OR EXCLUDE (EXACTKEYWORD , "Nonbiological Model") OR EXCLUDE (EXACTKEYWORD , "Neural Networks") OR EXCLUDE (EXACTKEYWORD , "Support Vector Machines") OR EXCLUDE (EXACTKEYWORD , "Evidence Based Medicine")) AND (EXCLUDE (SUBJAREA , "ENVI") OR EXCLUDE (SUBJAREA , "ENER") OR EXCLUDE (SUBJAREA , "AGRI") OR EXCLUDE (SUBJAREA , "ARTS"))

d) (KEY (gov*) AND KEY (org*) AND KEY (tech*)) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ENVI") OR LIMIT-TO (SUBJAREA , "AGRI") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "ENER") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "HEAL") OR LIMIT-TO (SUBJAREA , "NURS") OR LIMIT-TO (SUBJAREA , "MULT") OR EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "MATH") OR EXCLUDE (SUBJAREA , "BIOC") OR EXCLUDE (SUBJAREA , "MATE") OR EXCLUDE (SUBJAREA , "CENG") OR EXCLUDE (SUBJAREA , "EART") OR EXCLUDE (SUBJAREA , "PHYS") OR EXCLUDE (SUBJAREA , "CHEM") OR EXCLUDE (SUBJAREA , "PHAR") OR EXCLUDE (SUBJAREA , "IMMU") OR EXCLUDE (SUBJAREA , "NEUR") OR EXCLUDE (SUBJAREA , "VETE") OR EXCLUDE (SUBJAREA , "DENT") OR EXCLUDE (SUBJAREA , "ENVI") OR EXCLUDE (SUBJAREA , "ENER") OR EXCLUDE (SUBJAREA , "AGRI") OR EXCLUDE (SUBJAREA , "ARTS")) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011) OR LIMIT-TO (PUBYEAR , 2010) OR LIMIT-TO (PUBYEAR , 2009) OR LIMIT-TO (PUBYEAR , 2008) OR LIMIT-TO (PUBYEAR , 2007) OR LIMIT-TO (PUBYEAR , 2006) OR LIMIT-TO (PUBYEAR , 2005) OR LIMIT-TO (PUBYEAR , 2004) OR LIMIT-TO (PUBYEAR , 2003) OR LIMIT-TO (PUBYEAR , 2002) OR LIMIT-TO (PUBYEAR , 2001)) AND (LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (EXACTKEYWORD , "Controlled Study") OR EXCLUDE (EXACTKEYWORD , "Biomedical Technology Assessment") OR EXCLUDE (EXACTKEYWORD , "Diseases") OR EXCLUDE (EXACTKEYWORD , "Biological Organs") OR EXCLUDE (EXACTKEYWORD , "Nonbiological Model") OR EXCLUDE (EXACTKEYWORD , "Neural Networks") OR EXCLUDE (EXACTKEYWORD , "Support Vector Machines") OR EXCLUDE (EXACTKEYWORD , "Evidence Based Medicine")) AND (EXCLUDE (EXACTKEYWORD , "Priority Journal") OR EXCLUDE (EXACTKEYWORD , "Note") OR EXCLUDE (EXACTKEYWORD , "Medical Research") OR EXCLUDE (EXACTKEYWORD , "Animals") OR EXCLUDE (EXACTKEYWORD , "Patent") OR EXCLUDE (EXACTKEYWORD , "Animal") OR EXCLUDE (EXACTKEYWORD , "Biomedical Research") OR EXCLUDE (EXACTKEYWORD , "Genetics And Reproduction") OR EXCLUDE (EXACTKEYWORD , "Astronomy") OR EXCLUDE (EXACTKEYWORD , "Cloning, Organism") OR EXCLUDE (EXACTKEYWORD , "Cloning") OR EXCLUDE (EXACTKEYWORD , "Drug Industry"))

e) (KEY (sec*) AND KEY (org*) AND KEY (change*)) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ENVI") OR LIMIT-TO (SUBJAREA , "AGRI") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "ENER") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "HEAL") OR LIMIT-TO (SUBJAREA , "NURS") OR LIMIT-TO (SUBJAREA , "MULT") OR EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "MATH") OR EXCLUDE (SUBJAREA , "BIOC") OR EXCLUDE (SUBJAREA , "MATE") OR EXCLUDE (SUBJAREA , "CENG") OR EXCLUDE (SUBJAREA , "EART") OR EXCLUDE (SUBJAREA , "PHYS") OR EXCLUDE (SUBJAREA , "CHEM") OR EXCLUDE (SUBJAREA , "PHAR") OR EXCLUDE (SUBJAREA , "IMMU") OR EXCLUDE (SUBJAREA , "NEUR") OR EXCLUDE (SUBJAREA , "VETE") OR EXCLUDE (SUBJAREA , "DENT") OR EXCLUDE (SUBJAREA , "ENVI") OR EXCLUDE (SUBJAREA , "ENER") OR EXCLUDE (SUBJAREA , "AGRI") OR EXCLUDE (SUBJAREA , "ARTS")) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011) OR LIMIT-TO (PUBYEAR , 2010) OR LIMIT-TO (PUBYEAR , 2009) OR LIMIT-TO (PUBYEAR , 2008) OR LIMIT-TO (PUBYEAR , 2007) OR LIMIT-TO (PUBYEAR , 2006) OR LIMIT-TO (PUBYEAR , 2005) OR LIMIT-TO (PUBYEAR , 2004) OR LIMIT-TO (PUBYEAR , 2003) OR LIMIT-TO (PUBYEAR , 2002) OR LIMIT-TO (PUBYEAR , 2001)) AND (LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (EXACTKEYWORD , "Controlled Study") OR EXCLUDE (EXACTKEYWORD , "Biomedical Technology Assessment") OR EXCLUDE (EXACTKEYWORD , "Diseases") OR EXCLUDE (EXACTKEYWORD , "Biological Organs") OR EXCLUDE (EXACTKEYWORD , "Nonbiological Model") OR EXCLUDE (EXACTKEYWORD , "Neural Networks") OR EXCLUDE (EXACTKEYWORD , "Support Vector Machines") OR EXCLUDE (EXACTKEYWORD , "Evidence Based Medicine") OR EXCLUDE (EXACTKEYWORD , "Priority Journal") OR EXCLUDE (EXACTKEYWORD , "Note") OR EXCLUDE (EXACTKEYWORD , "Medical Research") OR EXCLUDE (EXACTKEYWORD , "Animals") OR EXCLUDE (EXACTKEYWORD , "Patent") OR EXCLUDE (EXACTKEYWORD , "Animal") OR

EXCLUDE (EXACTKEYWORD , "Biomedical Research") OR EXCLUDE (EXACTKEYWORD , "Genetics And Reproduction") OR EXCLUDE (EXACTKEYWORD , "Astronomy") OR EXCLUDE (EXACTKEYWORD , "Cloning, Organism") OR EXCLUDE (EXACTKEYWORD , "Cloning") OR EXCLUDE (EXACTKEYWORD , "Drug Industry")) AND (EXCLUDE (EXACTKEYWORD , "Climate Change") OR EXCLUDE (EXACTKEYWORD , "Food Security") OR EXCLUDE (EXACTKEYWORD , "Attitude To Health") OR EXCLUDE (EXACTKEYWORD , "Adolescent"))

Appendix 2: Conceptual papers criteria

1. Does the paper provide a novel and "big" idea that provides considerably new insight?

2. Is the idea "unpacked"? Do the authors argue for the idea in a clear, powerful, coherent, and compelling way?

3. Are the claims sufficiently justified: is the chain of evidence clear? Quality of argumentation? (Jaakkola, 2020)

4. Is the idea differentiated from related ideas and concepts? [More relevant to typology papers]

5. Do the authors indicate what is inside and what is outside the scope of the idea? Do they indicate why the idea is important (e.g., it shifts beliefs in ways that have implications for future research and/or marketplace stakeholders)?

6. Does the paper adequately represent prior research, and is it likely to lead to new future research? What novel research questions does the idea generate, and is a research agenda well specified?

Added from Jaakkola, 2020

7. Does the paper explain: "how and why the theories and concepts on which it is grounded were selected" Jaakkola p19

8. Does the paper explain why particular information sources are selected, and how are they analyzed?

Appendix 3: Hevner's seven guidelines for design science research.

1. **Design as an artifact:** Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.

2. **Problem relevance:** The objective of design-science research is to develop technology-based solutions to important and relevant business problems.

3. **Design evaluation:** The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.

4. **Research contributions:** Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.

5. **Research rigor:** Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.

6. **Design as a search process:** The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.

7. **Communication of research:** Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Taken from: Hevner, A.R., March, S.T., Park, J. & Ram, S., (2004). Design science in IS research. *MIS Quarterly*, 28(1), 75-105. DOI: 10.1007/978-1-4419-5653-8, p83

Appendix 4: Included studies

Authors / Date	Quality of evidence	Topics covered*	Technologies covered	Sector	Setting
Ahmed & Al-Haddad,	High	D, O	General	Education	Western
Alabdulkarim & Lukszo, 2010	High	C, R	Smart metering	Energy	Western
Armenia et al., 2021	High	C, D, O, R	General	General	Western
Balozian et al., 2019	High	D, G, O	General	General	Lebanon
Berlilana et al., 2021	High	B, O	General	General	Indonesia
Bierwisch et al., 2015	High	G, O	Biometric technology: homomorphic encryption	Civil security	Western
Carvalho et al., 2021	High	C, G, O, R	Blockchain	General	Non-specified
Ciaian et al., 2021	High	B, G, R	Blockchain	Finance	Non-specified
Clohessy & Acton, 2019	High	B, G, O	Blockchain	General	Western
Donalds & Barclay, 2022	High	B, C, D, G, M, O, R	General	General	Jamaica
El Khoury et al., 2022	High	B	General	ICT	Various
Garg et al., 2021	High	B	Blockchain	Banking	India
Gokalp et al., 2022	High	B, C, D, G, O, R	Blockchain	E-commerce supply chains	Western / Turkey
Herath et al., 202o	High	B, G, O	General	General	Western
Higgs et al., 2016	High	C, G, O, R	General	General	Western
Jackson, 2016	High	B, C, D, R	General	Education	Western
Kefallinos et al., 2009	High	C, G, O, R	General	Government	Western

Khan et al., 2019	High	C, D, G. O. R	Cloud computing	General	UAE
Khayer et al., 2021	High	B, C, D, O, R	Cloud computing	General	Bangladesh
Krishna, 2021	High	B, C, G	General	Government	Various
Lee et al., 2016	High	C, D, R	General	Home security	Korea
Li, 2015	High	G, O	2-factor authentication	Finance	China
Luo & Choi, 2022	High	B, G, O, R	General	E-commerce supply chains	Non-specified
Qian et al., 2012	High	C, O, R	General	Oil and gas industry	Western
Rajan et al., 2021	High	G, O	General	General	India / UK / Turkey
Raut et al., 2018	High	B, C, D, O, R	Cloud computing	Various including manufacturing	India
Sivan-Sevilla, 2021	High	D, G, O, R	General	Various	Western
Wang et al., 2021	High	C, D, O	General	Hospitality & tourism	China
Wu & Saunders, 2011	High	D. O	General	General	Western
Al Hogail, 2015	Medium	G, O	General	General	Saudi Arabia
Al Ketbi et al., 2021	Medium	C, O, R	Blockchain	Various	UAE
Alassafi et al., 2016	Medium	B, D, R	Cloud computing	Government	Saudi Arabia
Alizadeh et al., 2020	Medium	B, D, G, O	Cloud computing	E-banking	Iran
Alqahtani & Erfani, 2021	Medium	D, G, O	General	General	Saudi Arabia
Anderson, 2010	Medium	D, O, R	General	General	Unclear
Bu et al., 2021	Medium	D, G, O	General	Various	China
Chehrehpak et al., 2014	Medium	B, C	Blockchain	Various	UAE

Damenu & Beaumont, 2017	Medium	G, R	General	Banking	‘Developing country’
Da Veiga & Eloff, 2007	Medium	G, O, R	General	General	Unclear
Fu et al., 2022	Medium	B, C, D, G, O	Mobile payment tools	Retail	Taiwan
Gangwar & Date, 2015	Medium	B, G, O, R	Cloud computing	Manufacturing	India
Goldman, 2012	Medium	D, G, O	General	General	Western
Ihmouda et al., 2016	Medium	D, O	General	Education	Malaysia
Kanger & Pruulmann-Vengerfeldt, 2015	Medium	B, G, O, R	Secure Multiparty Computation (SMC)	Banking	Various
Kitchin & Dodge, 2019	Medium	G, O, R	Smart city technology	Government	Western
Koskosas, 2011	Medium	G, O, R	General	Banking	Western
Laux et al., 2011	Medium	B, D, O	Biometric authentication	Finance	Western
Liu et al., 2020	Medium	G, O	General	Government	China
Park et al., 2016	Medium	C, R	Cloud computing	General	Korea & China
Pathari & Sonar, 2013	Medium	G, R	General	ICT	India
Priyadarshinee et al., 2017	Medium	B, C, D, O, R	Cloud computing	Various including manufacturing	India
Radu & Amon, 2021	Medium	G	5G	Various	Various
Schinagl & Shahim, 2020	Medium	B, G, R	General	General	Unclear
Sener et al., 2016	Medium	G, O	Cloud computing	General	Unclear
Skarzauskiene et al., 2021	Medium	C, G	General	General	Australia / Lithuania
Venkatraman & Delpachitra, 2008	Medium	B, G, O, R	Biometric authentication	Banking	Western

Al-Darwish & Choe, 2020	Low	O, R	General	Oil and gas sector	Qatar
Cannoy & Salam, 2010	Low	C, D, G, O, R	General	Health	Western
Chiniah et al., 2019	Low	B, D, G, O, R	Cloud computing	ICT	Mauritius
Dhillon et al., 2016	Low	C, G, O, R	General	ICT	Western
Golightly et al., 2022	Low	B, R	Cloud computing	General	Western
Groner & Brune, 2012	Low	R	General	General	Western
Hashemi et al., 2015	Low	B	Cloud computing	General	Unclear
Riley et al., 2009	Low	C, D, O, R	Biometric authentication	General	India / South Africa / UK
Swamy, 2013	Low	B, D, G, O, R	Cloud computing	General	Western
Tafokeng Talla & Kala Kamdjoug, 2019	Low	D, O	General	General	Unclear

*Topics covered = B – Benefits, C – Consequences, D = Decision-making processes, G – Regulations or other incentives, O – Organisational conditions, R – Risks.