7-8-2023

Seizing new possibilities for expanding the scope of Cybersecurity Research in Information Systems

Asaf Dori
University of Sydney, asaf.dori@sydney.edu.au

Cheuk Hang Au
National Chung Cheng University, allenau@ccu.edu.tw

Manoj A. Thomas
University of Sydney Business School, manoj.thomas@sydney.edu.au

Seizing New Possibilities for Expanding the Scope of Cybersecurity Research in Information Systems

Completed Research Paper

Asaf U. Dori
The University of Sydney
Business School, H70,
Darlington, NSW 2006, Australia
AUDori@outlook.com

Cheuk Hang Au
National Chung Cheng University
No.168, Sec. 1, University Rd.,
Minhsiung, Chiayi, Taiwan
allenau@ccu.edu.tw

Manoj A. Thomas
The University of Sydney
Business School, H70,
Darlington, NSW 2006, Australia
Manoj.Thomas@sydney.edu.au

Abstract

As Cybersecurity continues to have a significant impact on modern society, there is a pressing need for a more comprehensive research agenda in Information Systems (IS). In this study, we conducted a thorough literature review of prominent IS journals to identify gaps in Cybersecurity research practices. Our findings indicate that there is a significant gap between research and practice, particularly in terms of focus on Cybersecurity behavioural factors in the past decade. To address this gap, we recommend that future Cybersecurity research in IS should adopt a broader perspective that incorporates relevant sociotechnical knowledge areas and theories. We provide an example of Cybersecurity research topics that go beyond behavioural aspects and suggest mapping of Cybersecurity sociotechnical research knowledge areas in Information Systems to guide future research efforts. This study highlights the importance of broadening the scope of Cybersecurity research in IS to address the complex Cybersecurity challenges in contemporary practice.

Keywords: Cybersecurity Research, Information Security Research, Information Systems Security Research, Sociotechnical research, Literature review.

Introduction

Business opportunities brought by emerging technologies, such as FinTech and Internet-of-Things (IoT), have made Cybersecurity increasingly important since an essential prerequisite of their success and adoption is reliable and secure Information Systems (IS). Given the complexity of the topic and broad scope of reach of Cybersecurity in modern business and social contexts, Cybersecurity research can be considered multi-disciplinary in nature and covers a range of areas such as Computer Science, IS, Psychology, Criminology, and more recently, Business Law (Di Lernia et al. 2020). In addition, as emerging evidence points out, the recent global pandemic has exuberated Cybersecurity risks (World Economic Forum 2020), and the relevance of Cybersecurity research has become more pertinent. The multi-disciplinary nature of IS research (Sarker et al. 2019; Soper et al. 2014) suggests that valuable insights from holistic and diverse perspectives can potentially be generated through Cybersecurity research in this field.

In this paper, we present the results of a comprehensive literature review of leading IS journals that explored how practitioners-based Cybersecurity knowledge areas are applied in Cybersecurity research in IS. Our findings serve as an objective basis upon which further exploration and future directions of Cybersecurity research in the IS discipline can develop. We provide examples of Cybersecurity research topics that extends the scope of research beyond behavioural aspects and recommend a mapping of Cybersecurity sociotechnical research knowledge areas in Information Systems.

In more specific terms, this research investigates the contemporary basis of Cybersecurity research in IS. We seek to address two research questions: first, how do normative Cybersecurity knowledge areas align with the scope of Cybersecurity research in IS? And second, what is the nature of Cybersecurity research within the IS discipline? The contributions of this research are threefold. First, we intend to develop an understanding of current Cybersecurity research within the IS discipline. Second, we aim to identify the prevailing pattern of research in this sociotechnical area of study. Third, we offer recommendations for widening the scope of future Cybersecurity research in IS to improve currency, inclusivity, theoretical development and relevance.

The paper is organised as follows: the background and methodology of the research are presented first. Then, key findings from the data analysis are highlighted. Finally, we discuss the findings and their implications based on the emerging insights from the analysis, as well as provide recommendations for future research in Cybersecurity within the field of Information Systems.

Background

The global trend of accelerating digital transformation due to the COVID-19 pandemic since 2020 has increased the magnitude of Cybersecurity challenges (Amankwah-Amoah et al. 2021) and Cybersecurity related threats (Naidoo 2020; World Economic Forum 2020). The impact of cyberthreats may not be only measurable financial loss, but also paralysis of work progress or even business operations (Furnell and Shah 2020). Thus, the need for a critical perspective on the Cybersecurity research agenda in IS literature is more urgent than ever before. This motivates our study to conduct a literature review and examine Cybersecurity research in IS literature based on a normative framework for Cybersecurity. In turn, we seek to inform the development of future Cybersecurity research in IS literature.

While Cybersecurity scholarship is not uncommon in IS literature, literature reviews in this area are uncommon or have a limited focus. A recent literature review by Dhillon et al. (2021) acknowledged three previous reviews in 1993, 2001 and 2005 and established that other Cybersecurity literature reviews in IS have a narrow focus primarily on behavioural aspects. This is further demonstrated by examining the scope of other recent literature studies e.g., (Balozian and Leidner 2017; D'Arcy and Herath 2011; Guo 2013). Behavioural Information System security research is considered a key area in Information Systems security research with a focus on understanding how individuals and groups within an organisation behave in relation to security policies and practices (Boss et al. 2015; Haag et al. 2020). Focusing primarily on the behavioural aspects of Cybersecurity research in Information Systems studies may not suffice anymore, as it neglects other crucial dimensions of Cybersecurity. While behavioural Cybersecurity research can help us understand how humans interact with technology and how they can be vulnerable to cyber-attacks, it may not address other critical issues, such as process management, risk management, technical vulnerabilities economic implications, and others. Cybersecurity is a multi-disciplinary field that requires a comprehensive approach that involves not only behavioural but also technical and organisational aspects (Tatar et al. 2017). For instance, organisational vulnerabilities can stem from the lack of proper security policies and inadequate governance, while technical vulnerabilities can stem from inadequate development processes, design flaws, or lack of proper system controls. Furthermore, cybersecurity threats are constantly evolving and becoming more sophisticated (World Economic Forum 2023). Therefore, focusing only on behavioural aspects may not be enough to keep up with the ever-changing threat landscape. It is important to address broader aspects of Cybersecurity, including technical and organisational considerations, to better align the scope of Cybersecurity research in Information Systems with challenges based on contemporary business environments. Therefore, a holistic approach encompassing all aspects of cybersecurity is necessary to effectively combat cyber threats.

The study in this paper further extends on recent work by Dhillon et al. (2021) and distinguishes itself in several areas with its research approach. The differentiation is in five different areas, namely literature

analysis, literature scope, literature temporal boundaries, terminology, and the empirical foundation. These areas are further detailed in Appendix 1.

With regards to the terminology used, inconsistencies with conceptualisation of Cybersecurity, and the interchangeable use of alternative terms like Information Security is widely acknowledged in literature (Althonayan and Andronache 2018; Dori and Thomas 2021; Von Solms and Von Solms 2018). While several attempts have been made to develop better cogency with the term and definition, this remains a recurring issue in research and practice (Von Solms and Von Solms 2018). In this literature review, we consider Cybersecurity as an umbrella term, consistent with the ubiquitous use of the term (Althonayan and Andronache 2018) and encompassing the broader set of related concerns (Whitman and Mattord 2019).

For the categorisation of Cybersecurity domains, the research was looking to adopt an established and proven practice-oriented categorisation scheme as an additional analytical lens. After examining the available literature, two options were identified. First is the CISSP book of knowledge (Gordon 2015) and second is the Cybersecurity Body of Knowledge (CyBok 2019). Further analysis of the potential categorisations determined that categorisation in the Cybersecurity Body of Knowledge (CyBok 2019) is more fit for purpose as it addresses the IS areas more specifically. The Cybersecurity Body of Knowledge (CyBok 2019) is funded by the National Cybersecurity Programme (UK) and aims to shape Cybersecurity knowledge areas ("CyBOK: More Knowledge Areas for Review - NCSC.GOV.UK" 2019). The Cybersecurity Body of Knowledge (CyBok 2019) identified nineteen top-level areas of knowledge in the Cybersecurity domain and provided the analytical lens for exploring the scope of Cybersecurity research in IS publications. These nineteen knowledge areas guided the analysis with the addition of the area 'Cybersecurity economics'. This area was added owing to the following consideration. First, 'Security Economics' is included as a 'crosscutting theme' in Cybok (CyBok 2019) that impacts multiple knowledge areas. Second, Cybersecurity publications in the literature corpus were found to address this specific area e.g., (Benaroch 2018). Last, recent developments in Cybersecurity practices include 'Cyber Risk Quantification' (Gartner 2021) which is the process of assessing and measuring potential risks and impacts in monitory terms.

Research approach

The research process involved multiple stages, as presented in Figure 1. Initially, the scope of the terminology was identified as the first step, followed by defining the literature corpus and search parameters as the second step. The third step involved a coding analysis, where an organising framework was developed, and selected research publications were analysed. The final step involved interpreting the results based on the categorisation of knowledge areas and a frequency analysis of the theories and methodologies used.

As mentioned in the introduction, the terminology in the Cybersecurity domain is inconsistent. While several attempts by scholars and practitioners were made to progress the terminological discussion (Althonayan and Andronache 2018; Gartner 2018; Guerra and Kim 2020; Von Solms and Van Niekerk 2013), terms like Cybersecurity and Information Security are nevertheless used interchangeability. To include an adequate representation of Cybersecurity research in IS journals, a wide range of terms were used in the search processes, which included "Cybersecurity", "Cybersecurity", "Information Security", "IT Security" and "Computer Security". The search was limited to articles from the last decade and within 2010 to July 2020 to represent the state of contemporary research in the domain.

The literature review process selected A and A-STAR IS journals[1] (ABDC 2019) as a representative set of top-quality international IS journals for this review (Boell and Blair 2019). As we intended to examine the representation of Cybersecurity in IS, the journal Computers and Security (A ranking on the ABDC list), which specialised in Security topics, was excluded from the review. An inclusion of specialised journal in this review would have skewed the results of the review and will impact the ability to provide a representative overview of Cybersecurity research in IS. All the articles were meticulously reviewed to

[1] The journal's list as per the Australian Business Deans Council (ABDC) Journal Quality List is available at: https://abdc.edu.au/abdc-journal-quality-list/

confirm that they dealt with Cybersecurity research topics and the detailed review enabled us to develop an in-depth understanding of the Cybersecurity body of research in IS journals.

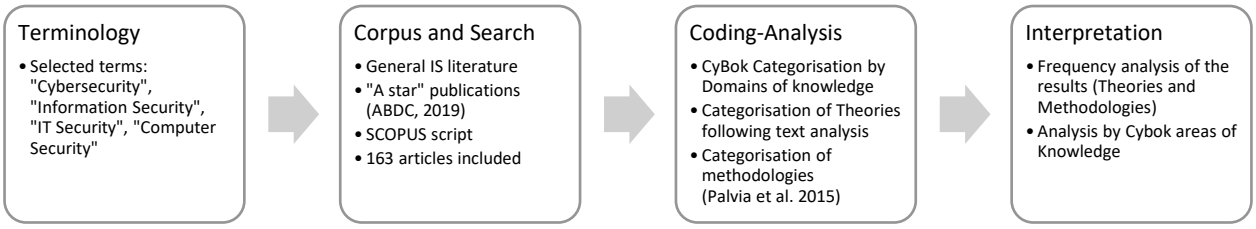

Figure 1 - Research Process

The coding process was performed with a team of two researchers (including a subject matter expert) with oversight from a third researcher (senior IS scholar). To improve the uniformity of coding and to reduce the ambiguity with the categorisation, the coding process was done iteratively with regular meetings to discuss the emerging findings and to make adaptations in the categories as necessary. The primary aspect that is included in the coding is the Cybersecurity domain of knowledge. In this assessment, we have used the CyBOK domains of knowledge (CyBok 2019) to code the different publications based on the area of knowledge that is addressed. To increase the rigor of the review process, following the initial review, a sample-based (>60%) second review of the coding was performed for additional validation. The categorisation of around 10% of the papers had the potential for ambiguity. To resolve this, the three-member team reviewed and discussed these papers to arrive at the final classification.

Data Analysis

The analysis of the data produced outcomes in three distinct domains. Firstly, it entailed the examination of the literature categorised by the knowledge domains. Secondly, it involved appraising the theories that are used in the literature corpus. Lastly, it encompassed the evaluation of the methodologies employed.

Research by knowledge areas

Table 1 presents the results of the analysis by the Cybersecurity domains as categorised by the Cybersecurity Body of Knowledge (CyBok 2019) and the mapping of the sociotechnical scope of the knowledge areas. The Cybok nineteen areas of knowledge are divided under five top labels (CyBok 2019): (1) Human, Organisational and regulatory aspect, (2) Attacks and defence, (3) System security, (4) Software and Platform Security and (5) Infrastructure Security. The category of Human Factors, as per its definition (CyBok 2019), captured literature that examines primarily behavioural factors, while the category of Adversarial Behaviours captured literature that examine research into behavioural aspects of attackers. Hence, these two categories were classified as behavioural research. By using this categorisation as a part of the analysis, we intended to provide a perspective on the scope of Cybersecurity research found in IS literature.

Cybok Category	Cybok knowledge area	Scope	Number of research items
Human, Organisational and Regulatory Aspects	Risk Management & Governance	Sociotechnical scope	33
	Law & Regulation	Sociotechnical scope	4
	Privacy & Online Rights	Sociotechnical scope	5
	Human Factors	Sociotechnical scope	88
Attacks and Defences	Malware & Attack Technologies	Primarily Technical	Nil
	Adversarial Behaviours	Sociotechnical scope	7
	Security Operations & Incident Management	Sociotechnical scope	21
	Forensics	Sociotechnical scope	Nil
Systems Security	Operating Systems & Virtualisation Security	Primarily Technical	Nil
	Cryptography	Primarily Technical	Nil
	Distributed Systems Security	Primarily Technical	1
	Authentication, Authorisation & Accountability	Primarily Technical	Nil
Software and Platform Security	Software Security	Primarily Technical	Nil
	Web & Mobile Security	Primarily Technical	Nil
	Secure Software Lifecycle	Primarily Technical	Nil
Infrastructure Security	Cyber-Physical Systems Security	Primarily Technical	Nil
	Hardware Security	Primarily Technical	Nil
	Network Security	Primarily Technical	Nil
	Physical Layer & Telecommunications Security	Primarily Technical	Nil

Table 1 - Cybersecurity Knowledge areas (CyBok 2019) by sociotechnical research scope and number of publications

The mapping of the knowledge areas to sociotechnical scope was done to identify the Cybersecurity knowledge areas that are suitable for IS research in contrast to other knowledge areas that are primarily technical and are likely to be better suited for research in Computer Science. As a discipline, Information Systems is characterised by having a sociotechnical focus which consists of human participants that perform activities using Information Systems (Alter 2018). The distinction with the identification of a sociotechnical scope was made with the purpose of identifying the Cybersecurity knowledge areas relevant to Information Systems and for the analysis of the coverage of the existing research by knowledge areas. The results demonstrate that the majority of the publication covered behavioural aspects of Cybersecurity (95 out of 163) followed by research in the area of Risk Management and Governance (33 out of 163) and Security Operations and Incident Management (21 out of 163). Other areas like Privacy and Online rights are represented by less than ten publications each. The observations on research by knowledge area demonstrated that the majority (59%) of Cybersecurity publications in Information Systems, as represented by the literature corpus, aimed at exploring behavioural aspects of Cybersecurity.

Observations about the use of theories

The coding for the identification and classification of the theories used in research is more complex primarily due to the number of theories identified and the initial classification in free text format. To address this issue, an additional manual review was undertaken to further improve the coding of data for this part of the analysis. In this instance, semantic differences were addressed to improve the uniformity of the results (e.g., different use of acronyms and spelling versions used to represent the same theoretical framework). In addition, for the same reasons of consistency, the classification treated different versions of the same theories similarly. For instance, general deterrence theory was classified as deterrence theory. The coding process included theories that were used as a primary theory in the article or where they influenced the research outcome (e.g., theory led to the formation of a model). The content analysis of our Cybersecurity corpus identified a set of 85 theories (including models and frameworks).

Top 10 Theories in IS Cybersecurity literature	Theory[2] originating area
Protection Motivation Theory	Psychology
Deterrence Theory	Criminology
Rational Choice Theory	Psychology
Technology Acceptance Model	Psychology
Routine Activity Theory	Psychology
Theory of Planned Behaviour	Psychology
Institutional Theory	Sociology
Theory of Reasoned Action	Psychology
Neutralization	Psychology
Game Theory	Mathematics

Table 2. Top Ten Theories in IS Cybersecurity Research

Table 2 lists the top ten used theories (by ranking) found in the research publications. We observed that Protection Motivation Theory was the most commonly used theory, followed by Deterrence theory, Rational choice theory, Technology Acceptance Model and Routine Activity Theory. Other theories listed in Table 2 are less represented and are ranked lower in the list. The detailed data that underpin these observations are provided in Appendix 2. The analysis in this area, demonstrates that the great majority of the theories used in Cybersecurity research found in the literature body have a background in Psychology and related disciplines (e.g., Criminology).

Observations about the use of methodologies

To develop an understanding of another dimension of Cybersecurity research in Information Systems literature, we also examined the use of methodology in the publications. Table 3 presents the observations regarding the use of methodologies in the literature. The classification of the methodologies adapted the classification scheme proposed by Palvia et al. (2015) in their review of Methodologies in Information Systems research.

Methodology – Categorisation by Palvia et al. (2015)	Percentage of Cybersecurity publications
Survey	31%
Mathematical Model	18%
Secondary Data	12%
Laboratory Experiment	10%
Case Study	8%
Qualitative Research	6%
Design Science	4%
Library Research	3%
Speculation/commentary	2%
Field Experiment	2%
Framework and Conceptual Model	2%
Content Analysis	2%

Table 3. Representation of methodologies in Cybersecurity research (n=167).

The data shows that the leading methodology used in Cybersecurity research is Surveys with 31% of the publications followed by Mathematical Model with 18%, Secondary Data with 12%, Laboratory Experiment

[2] The "Theory originating area" is derived from on *Theories Used in IS Research* website (Larsen, K. R., Eargle 2015).

with 10%, Case Study with 8%, Qualitative Research with 6%, Design Science with 4%, Library Research with 3% and Speculation/commentary, Field Experiment, Framework and Conceptual Model and Content Analysis with 2% each. The data demonstrates that the research in this field applies quantitative methods to a great extent. This observation is further confirmed by the classification of the research publications by the type of research that demonstrates that the majority of the papers applied quantitative methods equating to 75% of the papers (121 out of 163). Qualitative research was used in 18% of the papers (29 out of 163), and pluralistic research methods were applied in five percent (11 out of 163) of the studies. The detailed data that underpin these observations are provided in Appendix 2.

To sum up, the analysis demonstrates the following observations. Research by knowledge areas (CyBok, 2019) indicates that most publications were focused on behavioural aspects of Cybersecurity, followed by research in the knowledge areas risk management, governance, and security operations. Theories used in the research publications were primarily from the Psychology and Criminology disciplines, with Protection Motivation Theory being the most commonly used. Quantitative methods, such as surveys and mathematical modelling, were predominantly used in the research publications, with only a smaller percentage of studies utilising qualitative or pluralistic research methods.

Discussion and Implications

The discussion section explores the findings from several perspectives. First, we will discuss the implications of the orientation of Cybersecurity research in Information Systems towards studying behavioural aspects. Second, we suggest an approach to widen the scope of sociotechnical Cybersecurity research in Information Systems and discuss the theoretical and methodological implications of doing that. Last, we provide an example of topics and suggestions about how to explore broader sociotechnical Cybersecurity knowledge areas with the use of increasingly diverse theories and methods.

Information Systems as a research community has been identified "..as a scholarly community derives partly from our study of the first-order, second-order, and third-order effects of IT that span multiple functional areas and business processes." (Agarwal and Lucas 2005). This multi-disciplinary character arguably positions Information Systems as a discipline to offer unique comprehensive insights into the practice of Cybersecurity that spans across organisational and disciplinary boundaries. Soomro et al. (2016) calls for more complete approaches for information security management and highlight shortcomings in the exploration of the management role in information security management. As outlined in the findings (Table 1), we demonstrate that in leading Information Systems publications, Cybersecurity behavioural factors is an overrepresented knowledge area as represented by the literature corpus. Considering these observations, the multi-disciplinary character of the Information Systems discipline can drive wider consideration of knowledge areas for scoping Cybersecurity research. In Table 4 we provide a sample from our literature corpus that demonstrate the potential broader multi-disciplinary application of Cybersecurity research in Information Systems. The table shows five knowledge areas, details the research context, and provides two examples of Information Systems publications that explore these areas.

With regard to sociotechnical research, Sarker et al. (2019) raised concerns regarding the diminishing sociotechnical focus in the Information Systems discipline. Our analysis of the Cybersecurity papers in Information Systems research also supports this premise by demonstrating the dominance of Behavioural Security studies, which is largely consist of Type I 'Predominantly Social' research (Sarker et al. 2019). Type I research is "…where the investigation focuses almost exclusively on the social (including psychological, sociological, economic, or philosophical) aspects related to the phenomenon of interest, with technological or informational considerations serving as the context." (Sarker et al. 2019). Reflecting on this work by Sarker et al. (2019), Cybersecurity research in Information Systems shares the concerns that are raised regarding the lack of cohesion and informed consideration of broad social and technical aspects. Failing to thoroughly consider the role of technology in comprehending or clarifying a particular Cybersecurity phenomenon poses a potential threat to the field of research and the development of a unique and cohesive research characteristics in Information Systems research. Assertions about the limited breath and scope of contributions of Cybersecurity research in IS were previously made by (Lowry et al. 2017). We echo their recommendation that broader sociotechnical Cybersecurity research in specific technology context is essential.

Cybersecurity research areas in IS[3]	**Context**	**Examples of IS research**[4]
Cybersecurity Governance and risk management	Risk, policies, audit, governance	(De Gusmão et al. 2016) (Cram et al. 2017)
Cybersecurity Behavioural factors	Compliance, acceptance, conformance, perceptions	(Samonas et al. 2020) (Donalds and Osei-Bryson 2020)
Cybersecurity Privacy and Legal	Contractual, Liability, Information Privacy	(Lee et al. 2013) (Hui et al. 2019)
Security Operations and Incident Management	Process, operations, incidents	(Hui et al. 2012) (Ahmad et al. 2015)
Cybersecurity Economics	Investment optimisation	(Chun et al. 2016) (Benaroch 2018)

Table 4 – Example of Cybersecurity Research in diverse knowledge areas in IS

Seminal work by Benbasat and Zmud (2003) examines the identity of the Information Systems discipline and can also benefit from reflection in the context of our Cybersecurity related findings. Benbasat and Zmud (2003) identify the concept of 'Error of Inclusion' in IS research meaning "…when IS research models involve the examination of constructs best left to scholars in other disciplines." (Benbasat and Zmud 2003, p. 190). The dominance behavioural studies and the influence of Psychology as the origination area of theories in Cybersecurity research, is an indication that 'Error of inclusion' is potentially endemic in Cybersecurity research in Information Systems as some of the constructs being investigated may be more appropriate for research by other disciplines (e.g., Psychology, Criminology).

Theories provide a framework for understanding and explaining various phenomena that occur in the field. They support researchers and practitioners in organising their knowledge and observations, make predictions, and develop potential solutions to problems (Gregor 2016). The findings highlight the limited breadth and scope of theories used in Cybersecurity research in Information Systems and support similar findings by Lowry et al. (2017) that also highlight limitations in theoretical and methodological contributions of Cybersecurity research in Information Systems. Compared to overall IS research (Soper et al. 2014), the majority of theories used in Cybersecurity research originate from Psychology, while theories originated in other disciplines such as Management and Economics are underrepresented and not represented at all in the Top ten list (Table 2). Building upon the previous points regarding the limited multi-disciplinary and sociotechnical scope of Cybersecurity research in Information Systems, the limited scope of theories is impeding the development of theoretical contributions in a wider range of relevant Information Systems theories.

Selecting the appropriate research methodology ensures that the study is conducted in a rigorous and systematic manner, following established principles and guidelines. This helps to ensure that the data collected is reliable and valid and that the results can lead to the development of relevant theoretical and practical implications (Sarker et al. 2013). As the discourse about methodologies in the Information Systems discipline is extended and ongoing e.g., (Monteiro et al. 2022), it is beneficial to reflect on the use of methodologies in Cybersecurity studies. In our observations, we found a potential misalignment between the dominance of quantitative methodologies used in Cybersecurity research and the influential sociocentric approach. Schultze and Avital (2011) argue that using only quantitative methods in socially rich data situations may not be effective and that qualitative methods such as interviews are likely to be more beneficial in addressing socially rich data. Data that is complex and multifaceted, involving multiple perspectives, contexts, and meanings is typical context that is highly applicable in behavioural Cybersecurity studies. The limitations of quantitative methods in socially rich data situations include the inability to capture the nuances of social contexts, the potential for oversimplification of complex social

[3] Adapted based on the Cybok knowledge areas (CyBok 2019)

[4] Examples are from the literature corpus.

phenomena, and the reliance on pre-determined categories and measures that may not fully capture the diversity of social experiences. Qualitative methods such as interviews, on the other hand, allow for a more in-depth exploration of social phenomena, as they are flexible, open-ended, and focused on understanding the meanings and experiences of individuals within their social contexts (Myers and Newman 2007). Another observation with regard to methodology is related to the low percentage (2%) of publications that develop Frameworks and Conceptual models. This could be seen as further evidence that research on Cybersecurity in Information Systems has its limitations when it comes to practical applications. Cybersecurity practice is, to a large extent, driven by normative frameworks (e.g., NIST[5]), standards and government strategies (Dori and Thomas 2021; Rebollo 2013; Von Solms 2005) and yet in our exploration of the literature, research that addresses the development of frameworks and models was minimal. Extending methodological approaches in Cybersecurity research in Information Systems can enhance the understanding of complex phenomena, increase the validity and reliability of research findings, and address research questions that are not amenable to traditional methods (Orlikowski and Jack J. Baroudi 1991).

In Table 5 we provide several examples of research topics that extend the scope of Cybersecurity research in Information Systems in exploring sociotechnical knowledge areas that goes beyond behavioural topics and utilise a broader range of theories and methodologies. The first example is about exploring Cybersecurity Governance and Management challenges. This scope addresses the knowledge area 'Risk management and governance'. It can benefit from the application of theories from Strategic Management and Organisational Studies and use qualitative methods to support the exploration of the complex context of the phenomena. The second example is about investigating Cybersecurity Incident Management topics which includes several potential perspectives. Cybersecurity Incident Management can be explored in the context of process management, effective operations, economic considerations (e.g., ROI, Insurance) and others. In this example, potential applicable theories for exploration are from Operations Management and Economy and supporting methodologies can include Laboratory Experiments and Design Science. The third example proposes exploration of 'Improvements in the development life cycle' to address challenges in the knowledge area of 'Secure Software Lifecycle'. This area is also suitable for studying in the contest of process management, effective operations, economic considerations, and others. Potential applicable theories to support the exploration of this topic include Economics and Organisational Studies and applicable methodologies in this context can be qualitative methods and Design Science. The last example is about studying the management practices of Cybersecurity response capabilities. This area can be explored from the perspective of two knowledge areas. The first is 'Risk management and governance' with a focus on management practices and the second is 'Security Operations and risk management' with a focus on operational considerations. Theories that can support exploration in this area are from Sociology and Organisational Studies supported by the potential use of Field Experiment or Design Science methodologies. We offer multiple examples of research topics that broaden the scope of Cybersecurity research in Information Systems to be more inclusive in exploring sociotechnical knowledge areas and use broader range of theories and methodologies.

We extend on a recent empirical study by Dhillon et al. (2021) that identified the gaps between Cybersecurity research and practice in Information Systems by providing further support and details, applying a different research approach, discussing implications of the use of theories and methodologies, and by providing an additional level of details using a normative representation of practices as it is articulated by the Cybersecurity areas of knowledge (CyBok 2019).

[5] A framework published by the US National Institute of Standards and Technology

Research topic	**Knowledge areas** (CyBok 2019)	**Theories for consideration**	**Methodologies for consideration**
Cybersecurity Governance and Management Challenges	Risk management and governance	Dynamic capabilities Ambidexterity	Qualitative Research Case studies
Incident management	Security Operations and risk management	Theory of Constraints Activity-Based Costing	Laboratory Experiment Design Science
Improvements in the development life cycle	Secure Software Lifecycle	Transaction cost Adaptive structuration theory	Qualitative Research Design Science
Management of Cybersecurity response capabilities	Risk management and governance Security Operations and risk management	Resource dependency theory Institutional Theory	Field Experiment Design Science

Table 5 - Illustrations of Cybersecurity research topics that extends the scope of research beyond behavioural aspects

We call for more broadly applied Cybersecurity research in Information Systems research to further address the disparity between research and practice and to further support Information Systems researchers with the creation of impactful Cybersecurity research in society and business. A more holistic view that includes "technologies–policies–processes– people–society–economy–legislature" is also critically needed (Dori and Thomas 2021; Lowry et al. 2017) in Cybersecurity studies. A proposed improved scope coverage for Cybersecurity research in Information Systems is outlined in Figure 2. In this illustration, on the left side, we summarise the scope of Cybersecurity research in Information Systems as it was observed in the literature. On the right side of the figure, we provide a proposed redistribution of scope that offers a more balanced approach towards research of sociotechnical Cybersecurity knowledges areas. This proposed approach was developed based on a variety of sources e.g., (Australian Government 2023; CyBok 2019; World Economic Forum 2023) and is also in alignment with the recommendation by the aforementioned study by Dhillon et al. (2021).

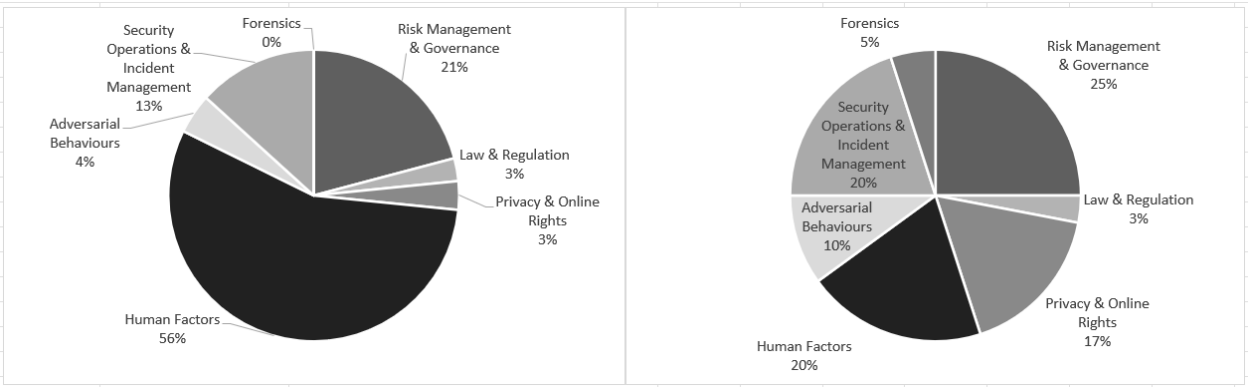

Figure 2 - Current (left) vs. proposed (right) mapping of Cybersecurity sociotechnical research knowledge areas in Information Systems

Considering recent call for emphasising significance in Information Systems research (Burton-jones et al. 2023), a more holistic view that considers various factors, including technologies, policies, processes,

people, society, economy, and legislature, is critical for enhancing the significance of Cybersecurity studies in Information Systems.

Implications to Research and Practice

We demonstrate that Cybersecurity research in leading Information Systems journals in the last decade have placed a significant emphasis on behavioural aspects in Cybersecurity and propose a broader focus of research to address relevant sociotechnical knowledge areas and improve the significance of research in this area. This study raises several implications for further development of Cybersecurity research in Information Systems. Our examples for extended research topics (Table 5), coupled with the appeal for a broader scope of Cybersecurity research in Information Systems, facilitate greater awareness of the sociotechnical knowledge areas to consider when conducting Cybersecurity research. Our mapping of the knowledge areas helps researchers assess the position of their own interests in the overall Cybersecurity domain and allows researchers to make necessary adjustments in their research portfolio to align with interests in current Cybersecurity practice. The mapping of the knowledge areas can also be used by early career researchers that are looking to initiate their Cybersecurity research portfolio in Information Systems. Extension of Cybersecurity research in Information Systems to deliberately includes the proposed knowledge areas can foster the development of applicable and impactful theories in this space.

This research has implications for practice as the relevance of Cybersecurity in Information Systems research and practice is growing (Dhillon et al. 2021). The discussion that addresses the knowledge areas, and the use of theories and methodologies enables researchers to close the gap with practice-oriented Cybersecurity research in Information Systems. A more balanced Cybersecurity research portfolio in Information Systems that is aligned with the key knowledge areas as identified by a key practitioner's book of knowledge can facilitate increasing alignment with key practice-oriented areas of interest. In turn, more informed Cybersecurity policies and practices may be formulated.

Conclusions, Recommendations and Limitations

In the context of Cybersecurity research, areas like economics (financial considerations), business (governance, management, processes), social (eco-systems), and technical (platforms) can benefit from further consideration in Information Systems research. Therefore, we call for renewed inquiries into practice aligned Cybersecurity research development in Information Systems. In these areas that are identified as highly relevant to practice, future work may explore potential application of new and extended theories to further contribute to a balanced sociotechnical focus, as well as apply a broader methodological approach that is fit for purpose in the specific research context of Cybersecurity.

The Information Systems research community has expertise in analysing the effects of IT on various functional areas and business processes. Due to its multi-disciplinary nature, the Information Systems discipline is uniquely positioned to offer comprehensive insights into Cybersecurity practices across diverse boundaries. However, behavioural studies dominate Cybersecurity research in Information Systems, with a focus on limited social aspects and a diminishing focus on technical aspects. The dominance of behavioural studies raises concerns about the lack of informed consideration of both social and technical aspects in Cybersecurity research. The dominance of behavioural studies also indicates the possibility of the 'Error of Inclusion' (Benbasat and Zmud 2003), where research models examine constructs that may be more suitable for other disciplines, such as Psychology and Criminology. This paper calls for further reflection on the scope of Cybersecurity research in Information Systems to promote improved significance of research in the field.

There are limitations to this study. The literature review primarily focused on analysing and manually coding large volumes of textual data. While we argue for the significance of our results given all the articles that we reviewed were published in leading academic journals and had undergone reasonable peer review (or similar processes that ensured research quality), we may have omitted some individuals' insights, merely due to the volume of information that required cognitive analysis. Therefore, we encourage future research that may focus on broader range of articles, such as opinion articles and research articles that comes from other journals that we did not cover but had demonstrated substantial quality.

References

ABDC. 2019. "ABDC Journal List." (https://abdc.edu.au/research/abdc-journal-list/, accessed September 1, 2020).

Agarwal, R., and Lucas, H. C. 2005. "The Information Systems Identity Crisis: Focusing on High-Visibility and High-Impact Research," *MISQ* (29:3), pp. 381–398.

Ahmad, A., Maynard, S. B., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," *International Journal of Information Management* (35:6), pp. 717–723. (https://doi.org/10.1016/j.ijinfomgt.2015.08.001).

Alter, S. 2018. "System Interaction Theory: Describing Interactions between Work Systems," *Communications of the Association for Information Systems* (42:1), pp. 233–267. (https://doi.org/10.17705/1CAIS.04209).

Althonayan, A., and Andronache, A. 2018. "Shifting from Information Security towards a Cybersecurity Paradigm," *Proceedings of the 2018 10th International Conference on Information Management and Engineering - ICIME 2018* (September 2018), pp. 68–79. (https://doi.org/10.1145/3285957.3285971).

Amankwah-Amoah, J., Khan, Z., Wood, G., and Knight, G. 2021. "COVID-19 and Digitalization: The Great Acceleration," *Journal of Business Research* (136:August), Elsevier Inc., pp. 602–611. (https://doi.org/10.1016/j.jbusres.2021.08.011).

Australian Government. 2023. "2023 - 2030 Australian Cyber Security Strategy." (https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf).

Balozian, P., and Leidner, D. 2017. "Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Asecurity Theory," *Data Base for Advances in Information Systems* (48:3), pp. 11–43. (https://doi.org/10.1145/3130515.3130518).

Benaroch, M. 2018. "Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision Making," *Information Systems Research* (29:2), pp. 315–340. (https://doi.org/10.1287/isre.2017.0714).

Benbasat, I., and Zmud, R. W. 2003. "The Identity Crisis within the Is Discipline: Defining and Communicating the Discipline's Core Properties," *MIS Quarterly* (27:2), pp. 183–194.

Boell, S. K., and Blair, W. 2019. "Www.Litbaskets.Io, an IT Artifact Supporting Exploratory Literature Searches for Information Systems Research," in *Australasian Conference on Information Systems*. (https://www.acis2019.org/Papers/ACIS2019_PaperFIN_141.pdf).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), JSTOR, pp. 837–864.

Burton-jones, A., Gray, P., Editor, S., Majchrzak, A., and Editor, S. 2023. "MISQ Editor's Comments: Producing Significant Research," *MIS Quarterly* (47:1).

Chartered Association of Business Schools. 2021. "Academic Journal Guide 2021." (https://charteredabs.org/academic-journal-guide-2021/, accessed June 3, 2022).

Chun, S. H., Cho, W., and Subramanyam, R. 2016. "Transaction Security Investments in Online Marketplaces: An Analytical Examination of Financial Liabilities," *Decision Support Systems* (92), Elsevier B.V., pp. 91–102. (https://doi.org/10.1016/j.dss.2016.09.015).

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2017. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), Palgrave Macmillan UK, pp. 605–641. (https://doi.org/10.1057/s41303-017-0059-9).

"CyBOK: More Knowledge Areas for Review - NCSC.GOV.UK." 2019. (https://www.ncsc.gov.uk/blog-post/cybok-more-knowledge-areas-review, accessed September 17, 2021).

CyBok. 2019. "The Cyber Security Body of Knowledge," in *CyBok*, A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin (eds.). (https://www.cybok.org/).

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643–658. (https://doi.org/10.1057/ejis.2011.23).

Dhillon, G., Smith, K., and Dissanayaka, I. 2021. "Information Systems Security Research Agenda:

Exploring the Gap between Research and Practice," *The Journal of Strategic Information Systems* (30:4), North-Holland, p. 101693. (https://doi.org/10.1016/J.JSIS.2021.101693).
Donalds, C., and Osei-Bryson, K. M. 2020. "Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents," *International Journal of Information Management* (51:November 2018), Elsevier, p. 102056. (https://doi.org/10.1016/j.ijinfomgt.2019.102056).
Dori, A. U., and Thomas, M. 2021. "A Comparative Analysis of Governance in Cyber Security Strategies of Australia and New Zealand," in *Pacific Asia Conference on Information Systems (PACIS)*. (https://aisel.aisnet.org/pacis2021/107/).
Furnell, S., and Shah, J. N. 2020. "Home Working and Cyber Security–an Outbreak of Unpreparedness?," *Computer Fraud & Security* (2020:8), Elsevier, pp. 6–12.
Gartner. 2018. "Cybersecurity Redefined for the Digital Era." (https://www.gartner.com/ngw/eventassets/en/conferences/sec24/documents/gartner-security-risk-management-summit-us-research-note-cybersecurity-redefined-digital-era-2018.pdf).
Gartner. 2021. "Benchmarking Cyber-Risk Quantification." (https://www.gartner.com/en/publications/benchmarking-cyber-risk-quantification, accessed May 15, 2023).
Gordon, A. 2015. *Official (ISC2) Guide to the CISSP CBK*, (4th ed.).
Gregor, S. 2016. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), pp. 611–642.
Guerra, K., and Kim, D. J. 2020. "Cybersecurity: A Definition across Europe and North America," in *AMCIS 2020 Proceedings*. (https://aisel.aisnet.org/icis2019/sustainable_is/sustainable_is/10).
Guo, K. H. 2013. "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis," *Computers and Security* (32:1), Elsevier Ltd, pp. 242–251. (https://doi.org/10.1016/j.cose.2012.10.003).
De Gusmão, A. P. H., E Silva, L. C., Silva, M. M., Poleto, T., and Costa, A. P. C. S. 2016. "Information Security Risk Analysis Model Using Fuzzy Decision Theory," *International Journal of Information Management* (36:1), pp. 25–34. (https://doi.org/10.1016/j.ijinfomgt.2015.09.003).
Haag, S., Siponen, M., and Liu, F. 2020. "Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future," *The Data Base for Advances in Information Systems* (52:2).
Hui, K. L., Hui, W., and Yue, W. 2012. "Information Security Outsourcing with System Interdependency and Mandatory Security Requirement," *Journal of Management Information Systems* (29:3), pp. 117–156. (https://doi.org/10.2753/MIS0742-1222290304).
Hui, K. L., Ke, P. F., Yao, Y., and Yue, W. T. 2019. "Bilateral Liability-Based Contracts in Information Security Outsourcing," *Information Systems Research* (30:2), pp. 411–429. (https://doi.org/10.1287/isre.2018.0812).
Larsen, K. R., Eargle, D. 2015. "Theories Used in IS Research Wiki." (https://is.theorizeit.org/wiki/Main_Page, accessed February 10, 2021).
Lee, C. H., Geng, X., and Raghunathan, S. 2013. "Contracting Information Security in the Presence of Double Moral Hazard," *Information Systems Research* (24:2), pp. 295–311. (https://doi.org/10.1287/isre.1120.0447).
Di Lernia, C., Hardy, C., and Dori, A. 2020. "Cyber-Related Risk Disclosure in Australia: Evidence from the ASX200," *Company and Securities Law Journal* (37:4).
Lowry, P. B., Dinev, T., and Willison, R. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26:6), Springer, pp. 546–563. (https://doi.org/10.1057/s41303-017-0066-x).
Monteiro, E., Constantinides, P., Scott, S., Shaikh, M., and Burton-Jones, A. 2022. "Qualitative Research Methods in Information Systems: A Call for Phenomenon-Focused Problematization," *MIS Quarterly* (46:4), iii–xix. (https://misq.umn.edu/awards-paper-year).
Myers, M. D., and Newman, M. 2007. "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization* (17:1), pp. 2–26. (https://doi.org/10.1016/j.infoandorg.2006.11.001).
Naidoo, R. 2020. "A Multi-Level Influence Model of COVID-19 Themed Cybercrime," *European Journal of Information Systems*, Taylor & Francis, pp. 1–16. (https://doi.org/10.1080/0960085X.2020.1771222).
Orlikowski, W. J., and Jack J. Baroudi. 1991. "Studying Information Technology in Organizations : Research Approaches and Assumptions," *Institute of Operations Research and the Management Science* (2:1), pp. 1–28.

Palvia, P., Kakhki, M. D., Ghoshal, T., Uppala, V., and Wang, W. 2015. "Methodological and Topic Trends in Information Systems Research: A Meta-Analysis of IS Journals," *Communications of AIS* (37), pp. 650–650.

Rebollo, O. 2013. "Overview of Key Information Security Governance Frameworks," in *IT Security Governance Innovations: Theory and Research*, E. FernáNdez-Medina, D. Mellado, and E. Fernández-Medina (eds.), IGI Global, pp. 1–12.

Samonas, S., Dhillon, G., and Almusharraf, A. 2020. "Stakeholder Perceptions of Information Security Policy: Analyzing Personal Constructs," *International Journal of Information Management* (50:April 2018), Elsevier, pp. 144–154. (https://doi.org/10.1016/j.ijinfomgt.2019.04.011).

Sarker, S., Chatterjee, S., Xiao, X., and Elbanna, A. 2019. "The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and Its Continued Relevance," *MIS Quarterly: Management Information Systems* (43:3), pp. 695–719. (https://doi.org/10.25300/MISQ/2019/13747).

Sarker, S., Xiao, X., and Beaulieu, T. 2013. "Qualitative Studies in Information Systems: A Critical Review and Some Guiding Principles," *MIS Quarterly: Management Information Systems* (37:4).

Von Solms, B., and Von Solms, R. 2018. "Cybersecurity and Information Security–What Goes Where?," *Information & Computer Security* (26:1), Emerald Publishing Limited, pp. 2–9.

Von Solms, R., and Van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), Elsevier, pp. 97–102. (https://doi.org/10.1016/j.cose.2013.04.004).

Von Solms, S. H. 2005. "Information Security Governance - Compliance Management vs Operational Management," *Computers and Security* (24:6), pp. 443–447. (https://doi.org/10.1016/j.cose.2005.07.003).

Soomro, Z. A., Shah, M. H., and Ahmed, J. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review," *International Journal of Information Management* (36:2), Elsevier Ltd, pp. 215–225. (https://doi.org/10.1016/j.ijinfomgt.2015.11.009).

Soper, D. S., Turel, O., and Geri, N. 2014. "The Intellectual Core of the IS Field: A Systematic Exploration of Theories in Our Top Journals," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 4629–4638. (https://doi.org/10.1109/HICSS.2014.569).

Tatar, U., Gokce, Y., and Gheorghe, A. V. 2017. *Strategic Cyber Defense: A Multidisciplinary Perspective*, IOS Press.

Whitman, M. E., and Mattord, H. J. 2019. "Management of Information Security . Cengage Learning," *Inc., Boston, MA* (2210).

World Economic Forum. 2020. "We Must Rethink and Repurpose Cybersecurity for the COVID-19 Era." (https://www.weforum.org/agenda/2020/06/we-must-rethink-and-repurpose-cybersecurity-for-the-covid-19-era/).

World Economic Forum. 2023. "Global Cybersecurity Outlook 2023 Contents." (https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf).

Appendix 1.

Comparison of research approach with Dhillon et al. (2021)

Comparison Criteria	Dhillon et al. (2021)	Research approach
Literature Analysis	LDA algorithm	In-depth content analysis
Scope of the literature	IS CABS 3 rating including specific IS Security Journals (Chartered Association of Business Schools 2021)	IS A* and A ratings excluding IS Security Journals (ABDC 2019)
Literature corpus temporal boundaries	1990-2020	2010-2020
Terminology	Limited to Information Systems Security	Cybersecurity as an umbrella term including common variants like Information Security
Empirical foundation	Delphi study	Coding and classification by Cybok knowledge area as a normative representation of practice

Table 6 - Comparison of research approach with Dhillon et al. (2021)

Appendix 2.

Detailed data charts

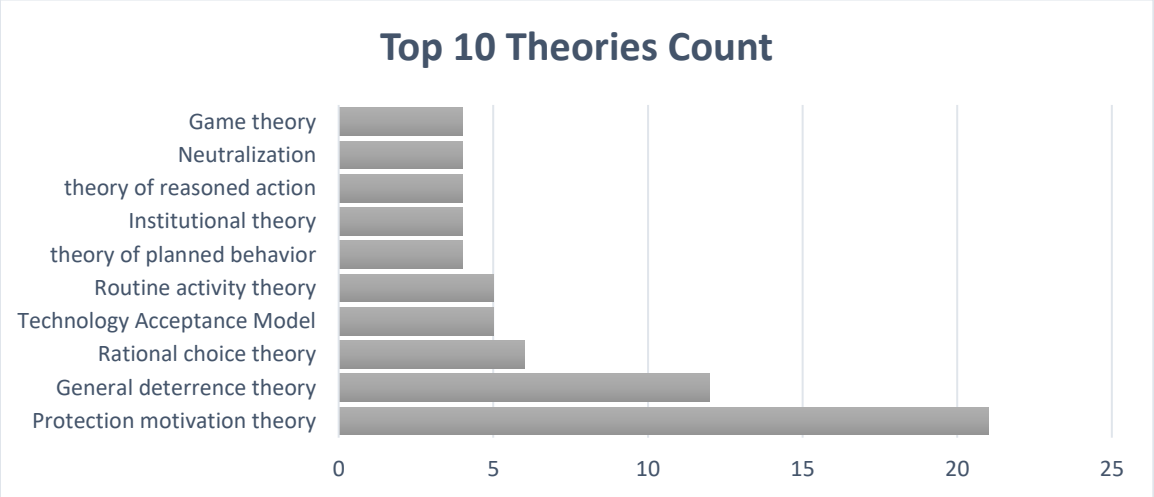

Figure 3 - Top ten theories in Cybersecurity research

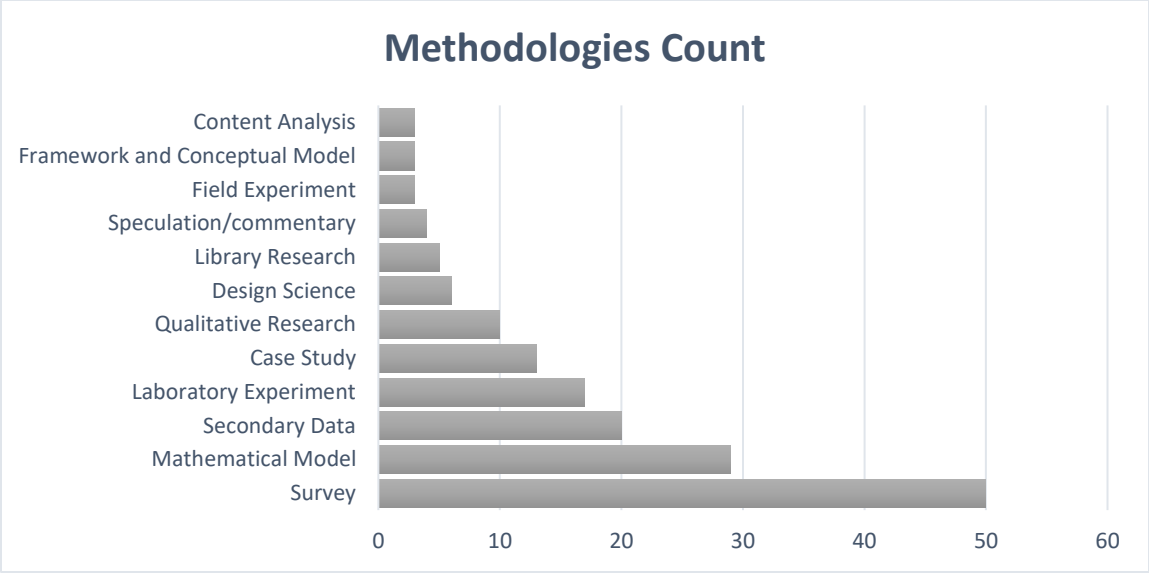

Figure 4. Overview of Methodologies in Cybersecurity Research

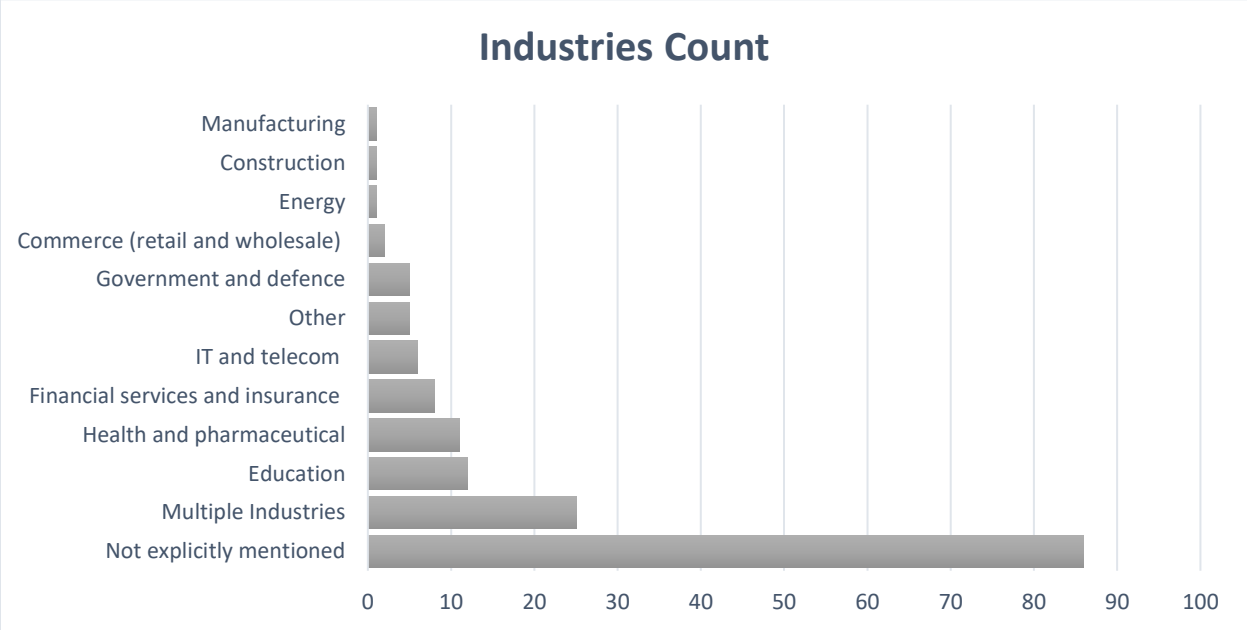

Figure 5 - Overview of Industries in Cybersecurity Research