information

MDPI

Review

Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management

Shahrukh Mushtaq * and Mahmood Shah

Newcastle Business School, University of Northumbria at Newcastle, Newcastle upon Tyne NE1 8ST, UK; mahmood.shah@northumbria.ac.uk
* Correspondence: shahrukh.mushtaq@northumbria.ac.uk

Abstract: This review addresses the fragmented literature on administrative interventions for cybercrime mitigation within e-government services, which often prioritise technological aspects over a unified theoretical framework. By analysing 32 peer-reviewed articles from the Web of Science (WoS) and Scopus databases, supplemented by additional sources located through Google Scholar, this study synthesises factors within the technical, managerial and behavioural domains using the Theory, Context and Method (TCM) framework. The findings reveal a predominant focus on managerial and technical factors, with behavioural aspects frequently overlooked. Cybercrime mitigation is often treated as a procedural step rather than a holistic process. This study advocates a well-established, context-specific mitigation plan, integrating regional factors through the Human–Organisation–Technology (HOT) framework to develop a comprehensive model for effective cybercrime mitigation in e-government services. This research has practical, theoretical and policy implications, offering actionable insights for improving operational practices, advancing theoretical frameworks and guiding policymakers in formulating effective cybercrime mitigation strategies.

Keywords: cybercrimes; mitigation; TCM framework; HOT framework; public services

Citation: Mushtaq, S.; Shah, M. Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. *Information* **2024**, *15*, 619. https://doi.org/10.3390/info15100619

Academic Editors: Dongkyoo Shin and Dongil Shin

Received: 22 August 2024
Revised: 28 September 2024
Accepted: 8 October 2024
Published: 10 October 2024

1. Introduction

Government institutions, eager to enhance connectivity, have increasingly offered online services to the public. These digital offerings have made services more accessible; at the same time, they have also left users' security vulnerable. Institutional management strives to protect user information, but as users willingly share their data with online services, the threat landscape grows more complex. With cyberthreats becoming more sophisticated, it is crucial for management to proactively strengthen their defences. Neglecting these measures risks damaging their reputation and compromising user data, causing distrust in services [1]. Therefore, effective institutional information security management (ISM) practices are essential for promising cybercrime prevention [2,3]. So far, the academic literature has not established a definitive relationship between both in the public sector context.

Amidst the COVID-19 pandemic in 2020, the global lockdowns compelled individuals to remain confined to their homes, precipitating a marked increase in online activity. The rise of cyberspace has posed new security challenges for governments. Its low entry cost, anonymity, geographical ambiguity and lack of transparency have attracted a range of actors. These include state entities, organised crime groups, terrorists and individuals, leading to threats such as cyberwarfare, cybercrime, cyberterrorism and cyberespionage. Unlike traditional national security threats, which are usually transparent and linked to identifiable governments and specific regions, these cyberthreats are markedly different. As a result, conventional national security measures have proven inadequate in mitigating cybercrimes [4]. Therefore, institutional management has more of a responsibility to protect their own and their users' data.

1.1. Critical Factors and Management Practices

Each successive advancement in information security introduces novel challenges that necessitate effective cybercrime mitigation strategies [5]. Management within organisations adopts a multifaceted role in the prevention of cybercrime. However, it is not clear which policies and practices work and which do not [6]. The evolution of cybercrime mitigation research requires a shift towards a more comprehensive approach, integrating managerial practices and new empirical insights [7] and identifying the critical factors responsible for effective mitigation, as well as incident management practices to reduce the prevalence of future events and identify practices commonly used in public sector institutions [8]. Moreover, given the multifaceted nature of cybercrime, understanding the efficacy of various policy interventions is also crucial [9]. Given that e-government intersects multidisciplinary research fields, such as computer science, information systems, public administration and political science [10], there is a significant variation in research streams within the literature regarding cybercrime mitigation in public services [11].

1.2. Public Service Management

In public service management, previous research has predominantly concentrated on either a techno-centric perspective or a service-centric approach to understanding citizens' service utilisation [12]. However, limited attention has been paid to explaining the managerial aspect of cybercrime mitigation in e-government services. The existing literature recognises policies' role in shaping institutional practices for cybercrime prevention [6]; however, a critical gap exists regarding the specific identification of management practices in mitigating cybercrime within e-government services. Moreover, limited research has comprehensively reported data breach incidents by integrating both the prevention and recovery perspectives [13]. The complexity in information security topics requires reporting the context in which the study is conducted [14].

Consequently, a crucial research imperative lies in clarifying the critical factors and management practices that demonstrably contribute to effectively mitigating cybercrime in this domain. This review aims to comprehensively analyse the scholarship on cybercrime mitigation in e-government services to answer the following research questions.

RQ 1. What are the current management practices for cybercrime mitigation?

RQ 2. What knowledge gaps exist?

RQ 3. What challenges are hindering progress in researching the topic?

To set the scene, it is important to discuss the context, namely, what we mean by "management". Studies either discuss individual managers or different levels of management, their style of leadership, etc. However, this review considers management primarily through the lens of practices and operations involving the procedures adopted for mitigating cybercrime in institutional settings. Depending on the diversity of available information, research articles recommending possible managerial practices for cybercrime prevention are also included.

2. Materials and Methods

Rapid reviews have emerged as a valuable tool to navigate the ever-expanding scientific literature. In contrast to traditional systematic reviews, which necessitate a meticulous and time-consuming approach, rapid reviews prioritise efficiency while synthesising the existing evidence. This streamlined methodology allows for the swift dissemination of pertinent information [15–17]. Nevertheless, meticulous integration of the search and selection elements within the search process is imperative to ensure accurate and comprehensive information retrieval. Therefore, the identification of relevant studies was completed manually, using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guide for protocol development and tracking the overall process and information flow [18]. Compliance with the PRISMA checklist improves the systematic reporting of review results [19]. Therefore, a PRISMA based approach was used, as presented in Figure 1.

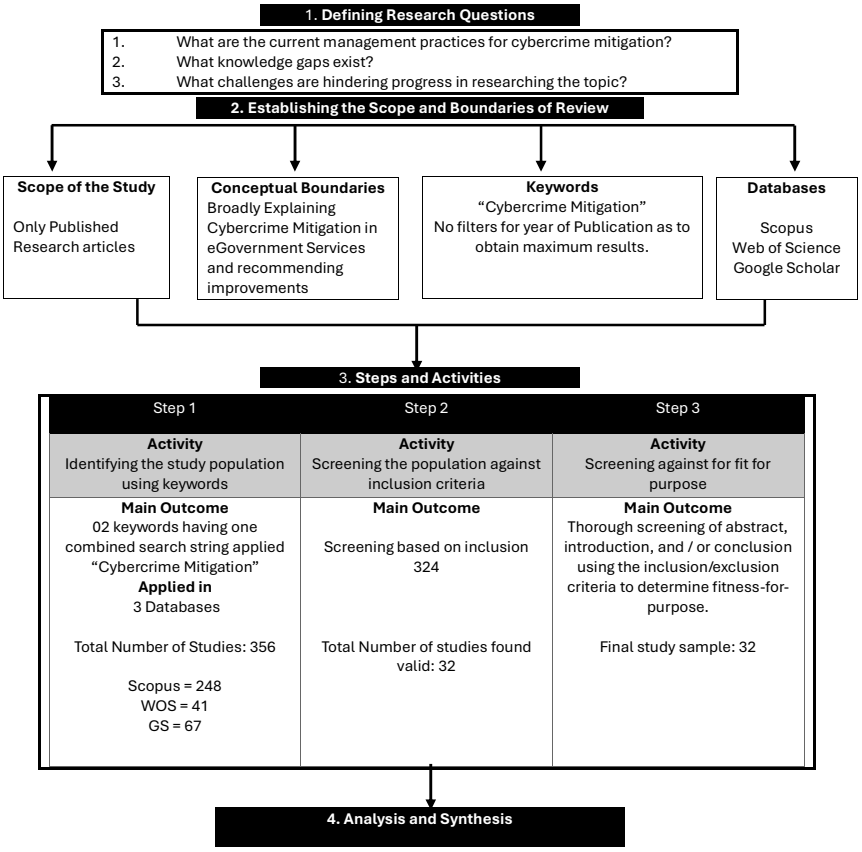

Figure 1. PRISMA. (Source: authors).

2.1. Inclusion and Exclusion Criteria

In the preliminary stages of the exploration of databases, scant literature was identified, prompting consideration of alternative sources. Simultaneous searches were conducted across the Web of Science and Scopus databases using the query "mitigating cybercrimes". Only peer-reviewed journal articles in the English language were included in the review process. The search was performed in the second week of July 2024. A total of 248 results from the Scopus database and 41 results from the WoS database were returned in the first hit. Moreover, Google Scholar was used for a context check of the relevant literature, finding 67 articles.

To cover a broad scale of disciplines, the search keywords were not limited to a timeframe filter. All results obtained from the three databases were considered one by one before identifying the final sample. The Theory, Context and Method (TCM) framework was adopted to summarise the suitable studies due to its efficiency in identifying the theory, context and method adopted by the result studies. It enables a swift synthesis based on cross comparisons of included text.

2.2. Data Extraction

Reviewers are advised to structure their narrative synthesis according to the Population, Intervention, Comparison and Outcomes (PICO) framework. However, the framework is directed more towards the medical sciences [16]. In order to grasp the detailed output from the identified sources, a Theory, Context and Method (TCM) framework was used to identify the research gaps and provide future directions for novel approaches [20]. This framework focuses on theoretical underpinnings in different contexts using various methods. Thus, it accommodates a comparison and evaluation of literature gaps. Figure 1 provides a snippet of the review process conducted for the data extraction.

3. Results

In the realm of government services, cybercrimes pose significant threats to system confidentiality, availability and integrity. The information security literature has traditionally focused heavily on technological dimensions, and an extensive literature search revealed noteworthy recommendations for managerial interventions for cybercrime mitigation within public sector settings. Upon reviewing all 356 results from the databases, 32 papers were deemed suitable for the study's objectives. Over the last two decades, there has been a significant increase in the number of studies on information and cybersecurity management as presented in Figure 2. This trend reflects growing concern within the academic community to protect the ever-changing digital market from cyberattacks.

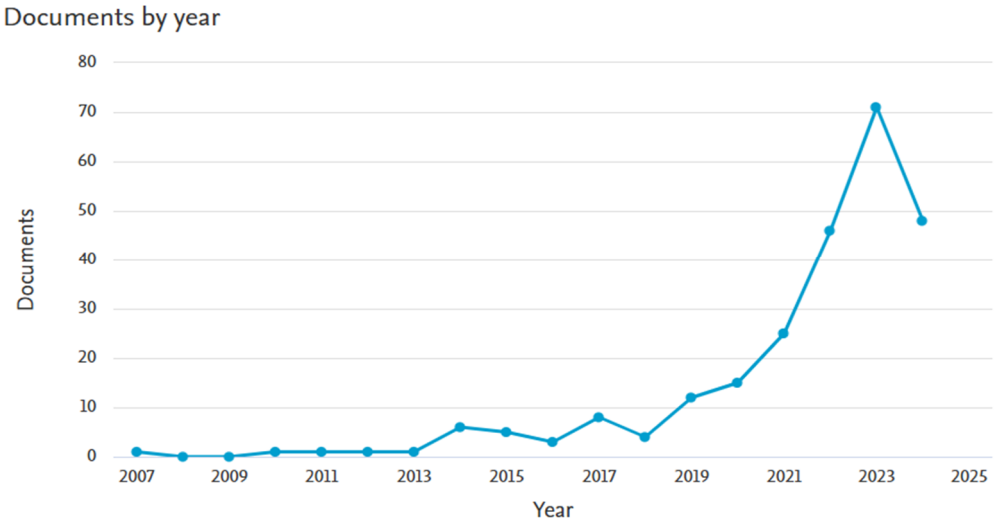

Figure 2. Publication trend in Scopus.

According to the United Nations report on the geographical distribution of countries based on the E-Government Development Index (EGDI) [21], certain nations continue to exhibit lower than average levels of e-government development. This disparity may stem from a lack of interest in digital transformation or insufficient resources necessary to implement and sustain e-government initiatives effectively.

The report provides a comprehensive analysis of global data on e-government development across various countries. Figure 3 highlights significant progress in e-government development worldwide, although lower development indices persist in certain regions, particularly in parts of Asia, Africa and the Middle East. One critical measure for mitigating cybercrime risks is cyber insurance. However, paradoxically, cyber insurance has intensified the issue. During the COVID-19 pandemic, companies with extortion insurance became prime targets for cybercriminals due to their insurance coverage. A supplementary report revealed that in 2021, 66% of organisations across 31 countries were subjected to ransomware attacks [22]. These attacks exploited technological weaknesses in systems, calling for management to level up their defences against cyberattacks.

Figure 3, indicates the UN report on e-government development index globally, representing lower developing index in regions highlighted in brown. Government institutions serve as intermediaries between individuals and society by providing employment and essential services, such as power, water, food, healthcare, communication, finance and transportation. These entities also collaborate to develop strategies for disaster mitigation and response [23]. Many scholars and practitioners contend that transferring private sector strategic management principles to the public sector is challenging due to fundamental differences in institutional goals. While the private sector prioritises competition and profit, the public sector focuses on efficiency and outcomes [24]. Therefore, the public sector has to devise solutions of its own for better cybercrime mitigation.

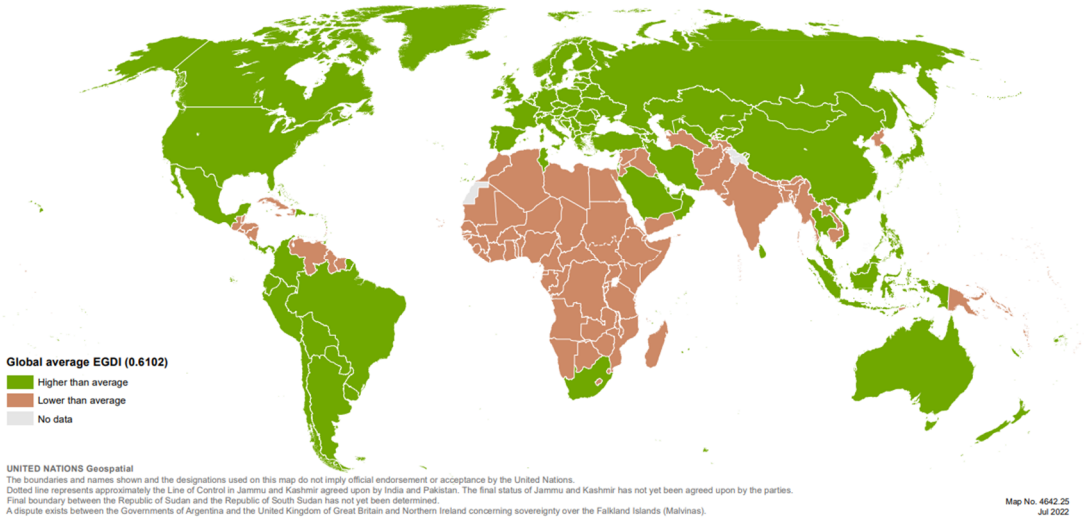

Figure 3. Geographical distribution of countries with EGDI values above and below the global average EGDI value; United Nations [21].

3.1. Extracting Factors

Cybercrimes have become a major risk to the world over time [25], and addressing cybercrimes in a rapidly evolving environment requires strategic, tactical and operational management approaches. Utilising the standard approaches—including detecting, assessing, analysing, evaluating and responding, along with their subphases—is essential to reduce the vulnerability to cyberattacks effectively [26].

This review identified critical factors and managerial practices in three research streams: technical, managerial and behavioural, as elaborated in Table 1. Therefore, considering the findings shown in Table 1, critical factors in the three research streams are reported in Figure 4. These critical factors identified for cybercrime mitigation are essential for an effective strategy to mitigate a cyber incident and provide an effective response.

According to Wall's (2001) classification mentioned in [27], cybercrimes can be categorised into four primary groups. Firstly, cyber trespass involves unauthorised entry into computer systems, typically executed by hackers employing malicious software to compromise security measures. Secondly, cyber deception and theft encompass fraudulent activities, such as spamming, online scams and theft of intellectual property. Thirdly, cyber porn and cyber obscenity pertain to the distribution of sexually explicit content online, including child pornography and instances of sexual exploitation enabled by digital platforms. Lastly, cyber violence entails the use of the internet for harassment, cyberbullying and threats directed at individuals or groups based on various personal characteristics.

Regardless of the method employed to breach or access data, the preparedness and responsiveness of the institution significantly determines the effectiveness of its response [28]. A checklist of the availability of all these factors informs the readiness of an institute for cyber incidents.

In comparison with the United Nations report on the geographical distribution of the E-Government Development Index (EGDI), presented in Figure 3, most of the research included in this review has concentrated on regions with lower e-government development indices, such as Nigeria, Pakistan, India, Zimbabwe and Saudi Arabia. Some studies have drawn comparisons with developed nations, where significantly higher e-government indices are reported. Although this was not the inclusion criteria for the research, still it is important to note that such outcomes from the included research are healthy in terms of the global attention of research on different regions with low EGDI index.

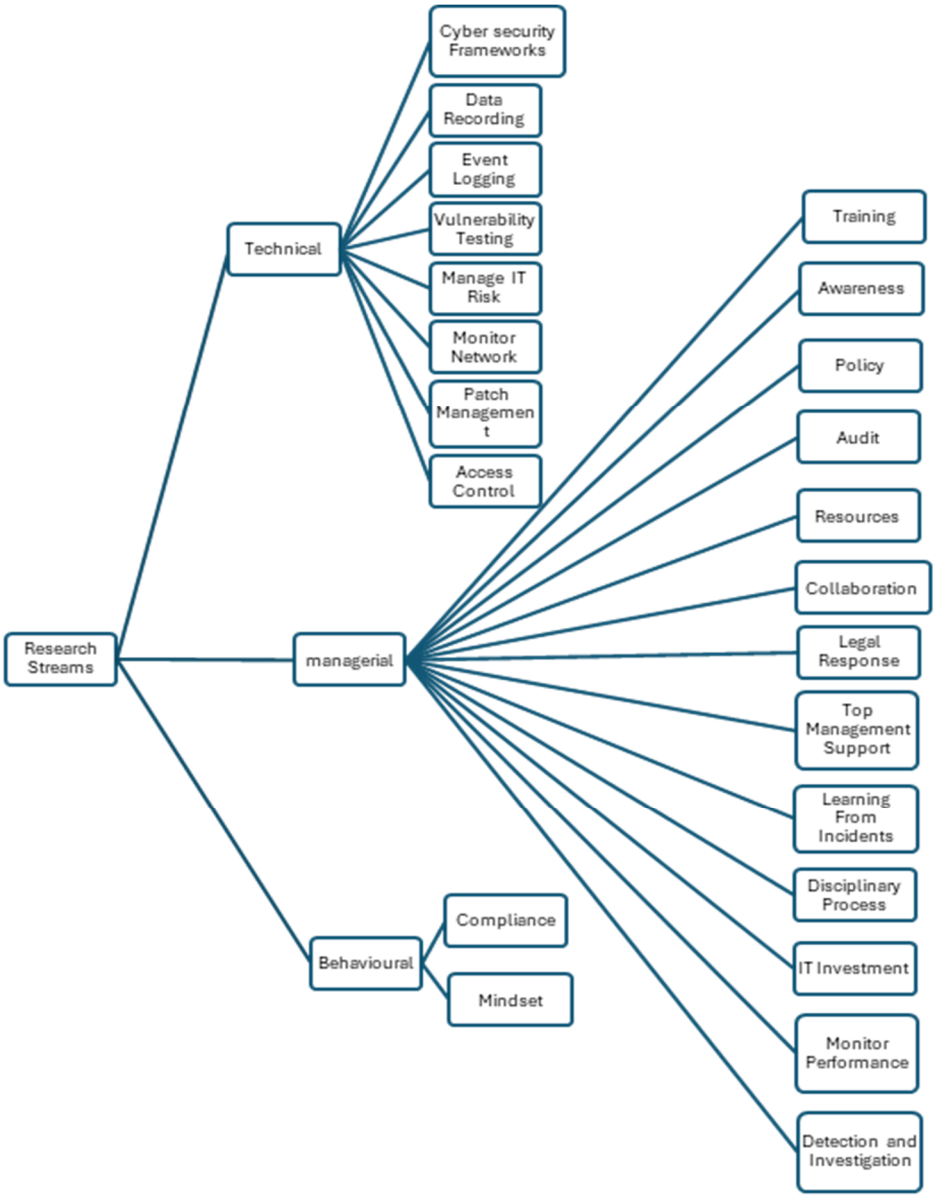

Figure 4. Critical factors of identified three research streams (Source: authors).

Table 1. Synthesis of critical factors and the three research streams identified.

		Technical											Managerial							Behavioural	
S. No	Source	Cybersecurity Frameworks	Data Recording	Event Logging	Manage IT Risk	Monitor Network	Access Control	Centralise Cyberse-curity	Training	Awareness	Policy	Audit	Resources	Collaboration	Legal Response	Top Man-agement Support	Learning from Incidents	Monitoring Perfor-mance	Cyber Insurance	Compliance	Criminal Behaviour
1	[29]								✔												
2	[2]									✔	✔	✔				✔				✔	
3	[30]								✔	✔	✔	✔								✔	
4	[27]													✔							
5	[31]							✔					✔	✔							
6	[32]									✔					✔						
7	[33]											✔		✔							
8	[34]																		✔		
9	[35]	✔	✔	✔												✔					
10	[36]																✔				
11	[37]												✔	✔		✔					
12	[38]	✔																			
13	[39]	✔			✔		✔			✔	✔		✔							✔	
14	[40]	✔			✔					✔	✔		✔		✔					✔	
15	[41]																				
16	[42]												✔								
17	[43]	✔				✔				✔											
18	[44]	✔	✔	✔		✔	✔		✔	✔							✔			✔	
19	[45]													✔							
20	[46]				✔					✔											
21	[47]	✔	✔	✔					✔					✔		✔					
22	[48]									✔											
23	[49]	✔	✔	✔	✔		✔														
24	[50]								✔	✔					✔						
25	[51]								✔												
26	[52]														✔						
27	[4]				✔								✔	✔				✔			
28	[53]								✔					✔							
29	[54]									✔	✔										
30	[55]					✔			✔		✔										
31	[56]	✔	✔	✔							✔										
32	[57]																✔				✔

Source: Author-Generated. Moreover, the data presented in this paper are also globally well-distributed. The studies referenced in Appendix A encompass a broad range of geographical locations, as illustrated in Figure 5.

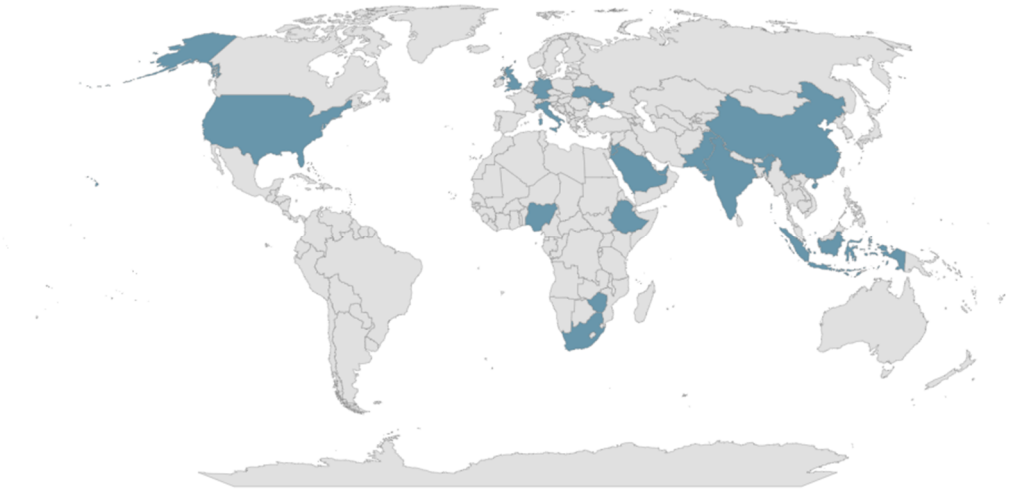

Figure 5. Global population report of included studies, blue highlighted regions represent the geographical location of studies included in review (author-generated).

3.2. Extracting Theoretical Models

The TCM framework assisted in identifying the theoretical underpinning of the identified studies, finding that e-government lacks a theory of its own. The literature indicates an exploration of the theoretical foundation within e-government services [58], concluding that e-government research exploits multidisciplinary theories while inherently lacking a theory of e-government itself.

However, later, Malodia, Dhir [7] compiled a theory including managerial capabilities and critical factors involved in e-government services. Nonetheless, their theory does not focus specifically on cybercrime mitigation. The domain of cybercrime prevention has been actively explored through multidisciplinary theoretical lenses. Although not all the research articles explicitly adopted a specific theoretical framework, Table 2 presents a comprehensive overview of the theories utilised in the studies reported in this review.

Table 2. Theoretical underpinning of studies.

Theories or Models	Context	Source
UTAUT Model	Smart Cities	[32]
Anti-Money Laundry Model	Global Regulatory System	[45]
Fraud Management Life Cycle	Banking Sector	[56]
Protection Motivation Theory	Banking Sector	[51]
Deterrence Theory	Laws in Global Context	[52]
Routine Activity Theory	General Population, Developing World	[53,54]
Learning Loop Framework	Higher Education	[55]
Risk Management Theories	Reviewers Collaboration	[34]
Socio-Technical Analysis	E-Government Public Value	[31]
NIST Cybersecurity Framework	Public Sector Cyber Resilience	[44]
Human-Organisation-Technology (HOT) Framework	Public Sector Organisations	[47]
Institutional Theory	Public Sector Organisations	[47]
Critical Success Factor	E-Government Sector	[37]
Socio-Technical STS Theory	E-Government Services	[40]

Source: Authors' own.

4. Discussion

This review utilised the prominent WoS and Scopus databases, further harnessing the Google Scholar search engine, and consolidated information from 32 published studies. It introduces three research streams and highlights major recommendations for public sector institutions. The scarcity of the literature on mitigating cybercrimes and the uniqueness of the technically multifaceted research area in e-government services stimulated this review to identify factors and research gaps to propose a future research agenda.

4.1. Research Stream I (Technical)

The expansive literature search followed by careful extraction of information from within these research papers led to three different research streams. The factors distributed across the articles fall into three categories: (I) technical, (II) managerial and (III) behavioural. These factors are often examined separately across various studies and are rarely consolidated into a single study. Moreover, they are not consistently addressed within the context of e-government services, despite recommendations that government institutions offering digital services should consider them comprehensively.

- Cybersecurity Frameworks

Since e-government has an inheritance from both public administration and infused technology, services are offered through digital channels. According to [35,38–40,43,44,47,49,56], cybersecurity frameworks are an important constituent for mitigating cybercrimes. The authors either utilised or recommend international cybersecurity frameworks. These frameworks include the National Institute of Standards and Technology (NIST) cybersecurity framework, the International Organisation for Standardisation (ISO) frameworks and the Control Objective for Business and Related Technologies (COBIT).

Topa and Karyda [35] suggested ISO framework practices for better information security management. Similarly Benz and Chatterjee [38] used the NIST framework for risk evaluation in the SME sector, recommending it where the burden of risk evaluation is divided between governments and institutions. According to Diesch, Pfaff [39] the information and security practices mentioned in the NIST framework are important for cybersecurity within institutes. Annarelli, Clemente [44] extracted the managerial practices in the NIST framework, recommended their usage in public sector organisations and further suggested their usage in the financial sector [49,56].

Malatji, Marnewick [40] opined that a socio-technical framework should be used for effective cybersecurity. The authors consolidated a social, technical and environmental framework for corporate governance. Similarly, Al-ma'aitah [47] considered the Human—Organisation—Technology framework for enhancing the effectiveness of cybersecurity within e-government services. The authors reported that the adopted strategies did not have a significant impact on cybersecurity effectiveness. According to Mishra, Alowaidi [43], one of the reasons for cybersecurity failure in e-government services is non-adherence to international security standards. Moreover, the authors inferred that a lack of trust in e-government services is due to users' belief in the lack of privacy in the sector.

- Data recording and event logging

The recording of data and systematic event logging are crucial for understanding the occurrence of specific incidents. The ISO framework provides guidelines for data recording and logging [35]. These practices are instrumental in facilitating the analysis and interpretation of such events, thereby enabling the derivation of valuable insights [44]. Effective learning and improvement are also contingent upon the accurate identification and documentation of events or errors. The comprehensive data collected and subsequently reviewed serve as a diagnostic tool to identify anomalies and irregularities, thereby guiding necessary modifications and interventions [47,49,56].

- Manage IT Risk

Online activities that deliver services via the internet are inherently vulnerable to both technical failures and external threats, such as cyberattacks. However, not all risk can be mitigated, such as a potential impact that would arise in the case of a cyberattack [39]. Moreover, the external and internal risk environment is ever changing [40]. Consequently, it is imperative for management to anticipate the potential risks associated with cyberthreats and system failures and to proactively develop strategies and preparedness measures to mitigate these risks [4,46,49].

- Network Monitoring

Continuous network monitoring enhances an institution's capacity to detect anomalies in real time. This capability facilitates the prompt implementation of effective measures in response to incidents. Additionally, such vigilant monitoring enables the identification of any atypical changes, thereby supporting early intervention and resolution. However, in the-government sector, mostly non-adherence to international security frameworks causes issues [44,55].

- Access Control

This means "to ensure that access to assets is authorised and restricted based on business and security requirements" [39]. The concept also extends to both physical and digital controls. Management must implement a tiered approach to security and access, ensuring that not all personnel within the organisation have proximity to critical physical systems integral to infrastructure. Similarly, digital access should be restricted based on role-specific requirements, such that only authorised individuals are granted access to sensitive resources. This stratified approach to security helps safeguard critical assets by enforcing appropriate access controls at both the physical and digital levels [44,49].

- Centralised Cybersecurity

Although this attribute was noted in only one of the research articles, it is included here due to its compelling recommendations. The authors propose the establishment of a centralised national cybersecurity framework designed to coordinate with local e-government service offices. This centralised approach would allow for a comprehensive evaluation and assessment of the cyberspace environment on a broad scale, facilitating recommendations for enhancements across all peripheral outlets and tailored local services. Such a structure aims to improve the overall cybersecurity posture by ensuring cohesive and standardised practices at both the national and local levels [31].

4.2. Research Stream II (Managerial)

- Training

The recommendation of continuous employee training emerged as the second most prevalent theme across the identified research studies. The ISO protocols recommend this training to be conducted at least twice a year [44]. Such ongoing training is essential for equipping employees with the knowledge and skills necessary to enhance their practices in both improving interventions and preventing cybercrimes. Given the rapid evolution of digital technologies, regular and effective training is crucial to ensure that staff remain current with the latest advancements. This training should encompass all organisational levels, from lower management interacting directly with systems to ensure engagement and information sharing to top management, thereby securing comprehensive support and commitment [29,30,44,47,50,51,53,55].

- Awareness

One of the fundamental aspects of technology use is awareness, not just to use the technology but to be aware of potential vulnerabilities that might arise due to its use. Therefore policy awareness is essential for employees to ensure compliance [2]. A large

volume of studies emphasised training and awareness; this establishes their important role in public service institutions [2,30,32,39,40,43,44,46,48,50,54].

- Policy

Policy serves as a basic framework to be followed for routine operations. Moreover, it informs operations in certain situations. However, a policy is of no specific use unless compliance is observed [2]; therefore, a definitive policy is important to direct staff and employees in understanding what needs to be done in various situations [2,30,39,40,54–56].

- Audit

Audit refers to the inquiry into any potential anomalies in information and cybersecurity practices. This includes the audit of information and communication between departments and customers. In most cases, this refers to the audit of online systems and their effectiveness [2,30,33]. Auditing the privacy, digital assets and processes of e-government services provides critical insights into the system's overall efficiency and effectiveness. This assessment helps identify strengths and weaknesses, highlighting areas where further improvements are needed to enhance service delivery, ensure data protection and optimise digital operations.

- Resources

Some authors emphasise suitable resources. Reference can be made to the context of public sector institutions where either resources are not well shared or they are abused for other purposes rather than focusing on cybersecurity [4,31,37,39,40,42]. Public sector institutions, especially in developing countries, are newly established and require extensive infrastructural investment.

- Collaboration

Collaboration pertains to the integration of multiple departments in securing cyberspace. According to the literature, the most highly recommended form of institutional collaboration is collaboration with law enforcement agencies. This partnership is deemed essential for enhancing the effectiveness of cybersecurity measures through coordinated efforts and shared expertise [4,31,32,34,37,45,47,53].

- Legal Response

There are distinct formats of response to cybersecurity issues: one involves addressing the incident directly, while the other pertains to potential legal proceedings, including investigation and prosecution. Both formats are crucial for comprehensive cybersecurity management. Nonetheless, it is imperative to ensure that a legal response framework is readily accessible to address and resolve issues through formal judicial channels when necessary [32,40,50,52].

- Top Management Support

Management support is essential across all facets of an institution, but the absence of backing from top management can render any activity untenable. Thus, it is crucial for top management to recognise the significance of these aspects and to prioritise the support and well-being of staff. Without the endorsement and commitment of senior leadership, the successful implementation and sustainability of various initiatives are severely compromised, especially in improving cybersecurity within the organisation [2,4,35,37,45,47,53].

- Learning from Incidents

Institutions are more effectively equipped when they learn from the experiences and solutions of others who have faced similar challenges. Instead of waiting for incidents to occur within their own organisation, it is advisable for institutions to proactively prepare by studying how others have addressed and resolved issues [36]. Organisations typically document their incidents and conduct monthly meetings to review the interventions employed to address these situations, with these discussions being grounded in the initial

reporting of incidents [44]. Furthermore, institutions can leverage extensive research in specific domains to gain insights into past incidents, criminal behaviours and other relevant factors, thus enhancing their preparedness and response strategies [57].

- Monitoring Performance

A significant portion of the management literature focuses on employee performance and production efficiency. However, institutional managers must also prioritise the assessment of their cybersecurity performance. This involves evaluating metrics such as the frequency of incidents, the efficacy of their resolution and the most effective methods for neutralising cyberthreats. To achieve this, it is essential to develop and consider key performance indicators (KPIs) that specifically measure the effectiveness of cybersecurity controls. Such evaluations help ensure that cybersecurity measures are both robust and responsive to emerging threats [4].

- Cyber Insurance

Although not a frequently emphasised concept in the reviewed research, cyber insurance represents a viable strategy for mitigating institutional losses. This protection can be structured as either collective insurance for the entire organisation or individual insurance for employees. Both approaches serve to safeguard against financial repercussions stemming from cyber incidents [34], at least covering financial loss in case of a cyber breach.

4.3. Research Stream III (Behavioural)

- Compliance

A mandatory task for all employees working within an institution is to comply with the set policy. The management must ensure that compliance is observed, as the formation of a policy does not guarantee cybercrime mitigation unless full compliance is achieved [2,30]. Achieving 100% compliance does not equate to achieving 100% security. While full compliance is essential for enabling audits and implementing security measures, it alone does not guarantee complete protection against all security threats [39]. However, an integrated framework that considers governance and compliance must be incorporated [40]. Thus, while compliance is a critical component of a robust security framework, it must be complemented by other proactive measures, e.g. effective governance, to ensure comprehensive security.

- Criminal Mindset

This concept pertains to the mindset and behaviour of individuals perpetrating cybercrimes, who may operate from diverse settings and localities. Understanding criminal behaviour is crucial for effectively managing cyberthreats, as it enables institutions to anticipate the tactics and motivations of cybercriminals. By gaining insights into these behavioural patterns, organisations can develop targeted mechanisms and strategies to address potential vulnerabilities and enhance their overall cybersecurity posture.

4.4. Theoretical Underpinning of Studies

Apart from not employing theory at all, a fundamental distinction in the application of theories across the identified studies lies in their mode of the use or unit of analysis. Figure 6 provides an illustration of the theoretical frameworks adopted. For instance, studies that focus on the individual level, whether examining users or managers, tend to utilise theories that explore behaviour and personal experiences. Conversely, those adopting an institutional or organisational perspective are more inclined to apply theories that are specifically tailored to analyse institutional dynamics and structures.

- Individual-level theories

The Routine Activity Theory (RAT) highlights three critical factors that contribute to the occurrence of a crime: opportunity, the presence of a suitable target and the absence of a capable guardian. This theory underscores the importance of modifying individuals'

routines to enhance precautionary measures and reduce their vulnerability to criminal activities. Additionally, the Protection Motivation Theory (PMT) explores how individuals' perceptions and assessments of threats influence their protective behaviours, emphasising the psychological processes that drive people to adopt safety measures.

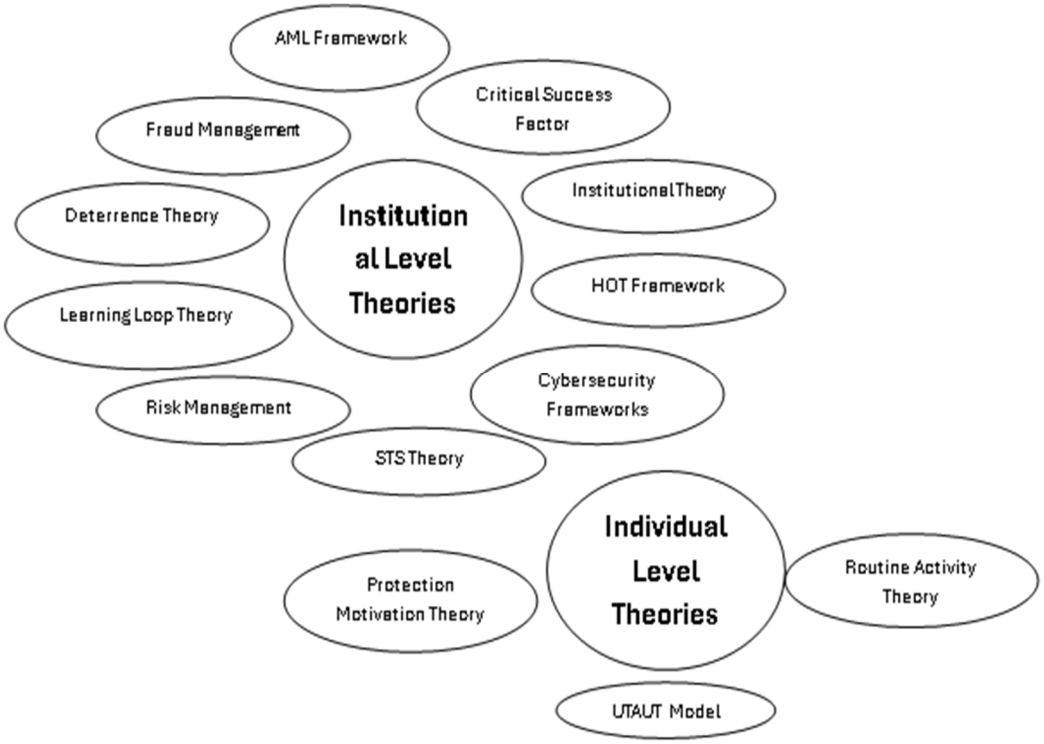

Figure 6. Theoretical perspectives adopted in identified studies (Source: authors).

The Routine Activity Theory was found to be widely used in understanding cybercrimes, especially phishing attacks [59–66]. RAT was also applied in a study related to target hardening, thus complementing the use of RAT and Situational Crime Prevention in preventive measures [65]. However, the RAT focuses on events rather than criminal activities, following the crime triangle, target, offender and absence of a guardian. However, the theory has received criticism with respect to the presence of the victim and the offender in the same space [67], since in the online world, it may be impossible to derive the necessity for the co-presence of the offender and the victim in real time. The criticism was addressed by changing "physical space" in the crime triangle to "network" [68,69], bringing it back into the realm of network and security.

Since these online spaces are managed by institutions offering electronic services, it is expected to be the responsibility of service providers. However, from the theoretical perspective, a possible extension can be made by considering the compromised guardian or inside job in the Routine Activity Theory [70], as the majority of criminology theories refer to the roles of individuals like those of employees and managers of the electronic service provision. The UTAUT model explains technology utilisation. Moreover, one study adapted the model by incorporating an array of factors pertinent to awareness in cybercrime prevention, thereby enhancing its applicability through the integration of technological use [32].

- Institutional-Level Theories

Some authors have employed risk management and compliance models, advocating for coordination between anti-money-laundering (AML) models and stakeholders. While risk assessment is a crucial component of operations, governments must evaluate and

determine the level of risk they are prepared to assume. This necessitates an assessment of their risk tolerance and the resources they can offer to the general public [45].

The fraud management life cycle (FMLC) is characterised by its extensive scope, integrating a series of interconnected processes. The cycle encompasses critical stages, including deterrence, prevention, detection, mitigation, analysis, policy formulation, investigation and prosecution. While each of these stages is indispensable for effective fraud prevention, the successful implementation of all stages requires the incorporation of additional processes. For example, deterrence is identified as a proactive strategy in mitigating cybercrimes [52], emphasising the imposition of sanctions as a response to employees' illicit activities.

Similarly, the prevention of cybercrime is broadly approached through initiatives such as awareness, education and training [32]. Effective detection, on the other hand, is associated with the rigorous implementation of cybersecurity frameworks [44]. The process of analysis is often coupled with ongoing monitoring, which is guided by policy formulation [2]. However, some authors argue that policy formulation does not guarantee cybercrime prevention unless compliance is observed. Furthermore, investigations and prosecutions are conducted based on policies set at the organisational level, or, in the case of public sector institutions, aligned with global standards set at the national level [52].

Mitigation operates between the detection and recovery stages, serving as a critical response mechanism aimed at halting ongoing fraudulent activity. Although essential for interrupting fraud, it is often portrayed as an intermediate step rather than a fully developed process in the existing literature.

4.5. Knowledge Gaps and Challenges

The studies focused less on behavioural aspects, as mentioned in Figure 4. For instance, the fraud management life cycle focuses on management prevention and intervention in case of an incident, while the anti-money-laundering model promotes understanding the behaviour of individuals. Similarly, the learning loop theory recommends learning from incidents within institutions, while the deterrence theory focuses on punishment in case of non-compliance with policies. This study therefore identified the following research gaps presented in Table 3. The recommendations are twofold—for institutes to better their defence while at the same time understanding criminal behaviour for better protection.

Table 3. Gaps and Challenges.

Gaps	Details	Challenges
Sector-Specific Fragmentation	More attention towards monetary institutions than e-government services at large.	Interest in adapting behavioural models to the diverse needs of e-government services management throughout the landscape, not just financial institutions.
Regulatory and Policy Integration	Limited utilisation of cybersecurity models for governance.	Improve resilience in public sector digital services using international cybersecurity frameworks.
High Tech for High Ends	The technological recommendations do assist but are not affordable by third-world countries [21].	Limited resources in adoption of state-of-the-art technology hinder public sector resilience to cybercrimes in third-world countries.
Managerial Integration for Cybercrime Prevention	Lack of managerial perspective in cybercrime mitigation within e-government services due to privacy and security concerns.	Involvement of managers in recommending prevention techniques within e-government services research.

Source: Authors.

E-government services management is mostly focused on compliance with established policies and international regulations. However, in relation to the extent of this review,

it is also important to note that these services are not evaluated from the management perspective. More attention is paid to the user-driven adoption of services and prevention of cybercrimes. One reason for the lack of research from the management perspective may be the availability of data. For instance, in public sector institutions, it is not easy to seek approval and obtain access to internal documents or access to the administration or management, especially in countries where there are existing international conflicts. For example, Pakistan and India [21] have a dispute over the geographical borders of Kashmir. According to the UN report, they rank low in e-government development indexes; thus, due to their conflict, they might not be interested in exposing their internal working mechanisms.

4.6. Theoretical Contribution

Research in this domain has predominantly concentrated on technical and managerial factors, primarily more from an organisational perspective. Nevertheless, there has been more emphasis on the Protection Motivation Theory, with limited attention devoted to the aspect of policy compliance [71], while for policy compliance, concepts from social bonds and involvement theory have previously been employed to understand employee compliance behaviour based on factors like commitment and belief [72]. However, further investigations focused on insider threats are needed to better understand the factors influencing the information security misbehaviour of employees [73].

For policy compliance, including the PMT, around 11 other theories were unified to develop a model of information security policy compliance [74]. The model contributed to explaining and, to some extent, predicting employees' IS policy violations or associated intentions. Similarly, efforts have been made to devise an integrated system theory for information security management [75] combining multiple information system theories into a framework for information security management reflecting upon the organisational behaviour and attitude of employees towards security. Still, security awareness and training programmes are reported to increase compliance and majorly improve institutional security, which is attributed to the criminological literature [76].

However, effective training and guidance must be clearly stated in institutional guidelines and sanctions imposed in case of non-compliance [77], although sanctions are referred to as being ineffective because of the lack of violation detection by managers and IT staff [74]. Moreover, development of policy guidelines does not guarantee cybercrime prevention unless compliance is observed [2]. Additionally, there is no systematic process of tracking cybercrime preventive practices and policies [6]. Therefore the primary impact on information security is reintroduced within management through managerial effectiveness and practices. Historically, this association was linked to instances where managers were either unaware of the situation or found it challenging to address the issue [78]. Still, the need for research on information security is demanded from the management perspective [2,79].

The three streams, technical, managerial and behavioural, propose multiple recommendation factors, as mentioned in Figure 4. However, each one of these factors can be observed from an individual and institutional perspective. For instance, the managerial aspects can be studied in institutions as a unit or through behavioural improvements in employees due to training programmes. It was also observed that while a reactive approach is incorporated in the management life cycle for effective cybercrime mitigation, the specific details of the mitigation process are not explicitly addressed. Additionally, the mitigation phase is often treated as a subsequent activity addressed later in the procedural framework. However, two of the theoretical frameworks, the Human–Organisation–Technology (HOT) and the NIST cybersecurity frameworks, if adopted together in a mixed method research setting, will assist in maintaining a balance of technological and managerial approaches towards cybercrime mitigation, encapsulating exploratory and explanatory research designs.

5. Conclusions

This review synthesises public sector recommendations for cybercrime mitigation, with a particular focus on critical factors for managerial practices within institutional settings. The review highlights key literature that intersects with managerial strategies, technical implementations and behavioural studies conducted in the realm of public administration. To answer the first research question, the study strived to identify the management factors mentioned in these studies for effective cybercrime mitigation. The study has found a predominant focus of research on technological and managerial factors compared to behavioural factors. Such a finding provides an indication that the lack of empirical data collection from institutional managements may be due to privacy concerns. For instance, most institutions have a strict policy of no data export, or they strictly limit their employees responding to any research groups.

Secondly, the study also sought to encapsulate the theoretical foundations employed in these investigations to identify the research gaps. It was revealed that e-government lacks a distinct theoretical framework of its own. Instead, interdisciplinary theories are frequently applied to e-government research, reflecting the inherently multidisciplinary nature of e-government services. This implies the need for exploratory research within the e-government domain to classify and identify the specific factors that contribute to effective cybercrime mitigation, particularly in the context of e-government services research. Notably, explicit references to cybercrime mitigation within this domain are scarce. Instead, some studies conceptualise it as a procedural element within broader frameworks for fraud mitigation in public sector institutions or as managerial practices geared toward addressing cybercrimes.

Lastly, the review reveals that e-government services lack a distinct theoretical foundation for cybercrime mitigation. Instead, the field draws upon criminological, managerial or behavioural theories, representing the multidisciplinary nature of investigation. While certain scholars have attempted to identify factors contributing to the successful operation of e-government services, their focus tends to be on successful adoption rather than on targeted cybercrime mitigation through managerial interventions. This challenge may be attributed to the lack of accessible data and the difficulty in retrieving records from the internal reports of institutions due to data privacy policies.

Future Research Recommendations

The research has found little evidence of cybercrime mitigation, apart from a procedural part of a fraud management life cycle. The recommendations for effective cybercrime mitigation are either proactive or reactive measures to mitigate cybercrimes or mitigate its effects after cyber incidents. The international cybersecurity standards are recommended to safeguard and protect national digital databases. However, they hinder the institutional implementation of mitigation unless managerial perspectives are valued.

To contribute to the literature, e-government services' cybercrime mitigation should be examined through the management perspective, as these are the individuals who deal with cybersecurity events in preventing the crime and limiting its effect firsthand. The Human–Organisation–Technology (HOT) framework offers a balanced approach by incorporating a comprehensive range of factors within a single study. However, to validate and contextualise these factors specifically within the e-government domain, an exploratory study would be beneficial. None of the studies considered the management perspective specifically directed to cybercrime mitigation within the sector. Therefore, the following future research recommendations are presented:

1. Management perspective studies in cybercrime mitigation within e-government services, provided the study is context-specific (regional, institutional or problem-oriented).
2. Development of a theory of cybercrime prevention within the e-government services domain or information system security domain, including human intervention.

3. Checking the feasibility of results from one study to other different contexts to understand their viability, especially in the lower development index of countries identified in the UN e-government survey [21].

6. Limitations

Our study is subject to certain limitations, particularly regarding the selection of databases. Additionally, broader collaboration with other experts in the domain could have potentially yielded more comprehensive results.

Author Contributions: Conceptualization: S.M.; methodology, M.S.; software, S.M.; validation, S.M.; investigation, S.M.; data curation, S.M.; writing—original draft preparation, S.M.; writing—review and editing, S.M. & M.S.; visualization, S.M.; supervision, M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. TCM Framework.

S. No	Source	Findings	Population	Theory	Context	Method
1	[57]	Expats collaborate with local accomplices to commit economic cybercrimes, particularly focusing on money laundering through false identification and sham companies to launder money.	Ghanaians in US	N/A	Economic cybercrime	Content Analysis
2	[48]	Increasing awareness in students can reduce cybercrimes.	Students in Jordan, higher education institutes	N/A	Impact of awareness	Quantitative
3	[46]	Awareness and data safety campaigns from governments must be initiated.	US, Singapore and India	N/A	Comparing essential elements to mitigate cybercrimes	Quantitative
4	[32]	Awareness is important to adopt technology; however, government initiatives and legal awareness have limited influence in adoption of preventive behaviour.	Smart city population in India	UTAT Model	Mitigate cybercriminal activities	Quantitative
5	[27]	It is crucial to identify and enhance cooperative relationships between state-based law enforcement and private sector initiatives in law enforcement.	Regulatory bodies and private industry	N/A	Law enforcement for prevention	Review
6	[45]	Despite existing anti-cybercrime and anti-money-laundering legislation, weaknesses of global regulations and state-level enforcement are issues.	Case laws and policy documents	AML Model	Cybercrime law and best practices to reduce weaknesses	Document Analysis

Table A1. *Cont.*

S. No	Source	Findings	Population	Theory	Context	Method
7	[50]	To cater for cybercrime challenges, the government should revise criminal and procedural laws, strengthen electronic device security measures and enhance training and awareness among law enforcement and administrative officials.	Indonesia	N/A	Legal framework of cybercrime prevention	Qualitative Descriptive
8	[49]	A decision support framework assists in understanding the impact of cyber fraud, which further assists in deciding the sector where prevention and mitigation can deliver most effect, for instance, on profitability, goodwill, customers' satisfaction or risk management.	17 licensed banks in South Africa	N/A	Adaptive response policy	Analytical Hierarchy Process
9	[56]	The study suggests an inclusive policy framework that incorporates legal, governance, internal control and regulatory elements aimed at strengthening cybersecurity within South African banks.	Professionals of South African banking sector	FMLC	Cyberfraud mitigation in banking	Mixed Method
10	[51]	Frequent training and government alerts may also be important for cyberattack prevention.	Financial executives from UAE banks	Protection Motivation Theory	Cyberattack prevention in UAE using leadership	Quantitative
11	[52]	The research underscores the importance of tailored punishments to deter cybercrimes and ensure fairness in legal responses to technology-related offences.	Laws of UK, USA, China, Ethiopia and Pakistan	Deterrence Theory	Punishment of cybercriminals	Review
12	[54]	Cybersecurity is the key element of mitigating the risk and incidents of cybercrime. Targeted educational initiatives and policy measures can enhance cybercrime prevention.	General population in USA	Routine Activity Theory	Cybersecurity knowledge and awareness	Quantitative
13	[55]	The strategies of policy updates, system modifications, partnerships, new software integration, enhanced training, security improvements and rigorous monitoring aim to ensure a cybersafe environment now and in future crises.	Cybersecurity experts and top managers in Australia	Learning Loop Framework	Cybersecurity challenges in higher education	Qualitative

Table A1. *Cont.*

S. No	Source	Findings	Population	Theory	Context	Method
14	[33]	Regulatory frameworks must be strengthened to enforce mandatory cybersecurity standards and regular audits across financial institutions, fostering collaborative efforts between banks, regulatory bodies and law enforcement agencies.	Administration-level employees inPakistan	N/A	Impact on performance of banking sector	Quantitative
15	[34]	Use of cyber insurance to manage financial risks associated with cyber incidents and collaborative efforts between public and private sectors can enhance national cybersecurity resilience.	Collaboration of reviewers from India and the USA	Risk Management Theories	Model selection for threat mitigation	Review
16	[31]	Resources for implementing cybersecurity measures in e-government portals. Collaboration to centralise cybersecurity in small cities.	China	Socio-Technical Analysis	E-Government development from public value perspective	Qualitative
17	[41]	The operational aspects of information security in e-government are inherently complex, which contributes to the limited amount of scientific research dedicated to this field.	Ukraine	N/A	Review of country's information legislation	Review
18	[42]	E-government has shown a notable correlation with increased commitments to cybersecurity and business utilisation.	127 countries			Quantitative
19	[43]	The standard operating procedures developed by NIST and ISO for cybersecurity are important. The major vulnerabilities are weak security systems, lack of awareness and enterprise failure.	Saudi Arabia	N/A	E-government cyberthreats and vulnerabilities	Mixed Method
20	[30]	Policy, training, audits and compliance are regarded to be the best management practices. Organisations must be up to date with industry standards and information security management.	India	N/A	Information security management practices	Case Study
21	[44]	NIST management practices are important, stressing thorough data recording and registration to reduce failure.	Italy	NIST Framework	Cyber resilience using managerial practices	Qualitative
22	[35]	ISO controls can be used as guidelines for managerial practices in information security management.	N/A	N/A	Guidelines for enhancing IS management	Review

Table A1. *Cont.*

S. No	Source	Findings	Population	Theory	Context	Method
23	[40]	Importance of bridging socio-technical gaps in cybersecurity frameworks to achieve effectiveness. Recommendations include adopting integrated management processes, ensuring compliance with regulatory standards and fostering continuous improvement in cybersecurity practices across governmental and organisational levels.	Global context	Socio-Technical Systems	Optimising cybersecurity practices as a socio-technical management process	Mixed Method Research
24	[2]	The study suggests that information security should be considered the responsibility of management, and further notes that information security managers should consider a holistic approach.	N/A	N/A	Information security management practices	Review
25	[38]	The NIST framework can be used for cybersecurity self-evaluation within SMEs. Government can encourage SMEs to use the NIST framework and enhance national cyber resilience.	N/A	NIST Framework	Cybersecurity evaluation tool for SMEs	Quantitative
26	[39]	The NIST framework constitutes cybersecurity management practices which are important to structure the processes and information security of an organisation.	Cybersecurity experts in Germany	Conceptual	Information security factors	Qualitative
27	[47]	Implementing technical measures, senior management in cybersecurity governance, strengthening regulatory frameworks, conducting regular training programmes for employees, fostering collaboration among stakeholders, investing in cybersecurity infrastructure and integrating insights from institutional theory into cybersecurity strategies.	Technology department staff members and e-government officials in Jordanian ministries	HOT Framework, Institutional Theory	Cybersecurity enhancement in public sector organisations	Quantitative
28	[4]	Cybersecurity is a shared responsibility, involving not just governments but also organisations and individuals. A unified effort from all stakeholders can effectively combat cybercrime.	Global	N/A	Cybersecurity tactics in mitigating cybercrimes	Mixed Method

Table A1. *Cont.*

S. No	Source	Findings	Population	Theory	Context	Method
29	[36]	Lessons from advanced nations can help mitigate electronic tax cybercrimes. Nigeria, Kenya and South Africa should establish strong institutions to monitor and address cyber tax crimes effectively.	Nigeria and South Africa	N/A	Crime in electronic taxation	Review
30	[53]	The government needs to develop relevant anti-cybercrime laws with stringent penalties, as well as cybercrime policies tailored for the business sector. Additionally, law enforcement officers must be trained to bridge the skills gap currently hampering their response to cybercrime.	38 retail players in Zimbabwe	Routine Activity Theory	Cybercrimes in developing third world	Mixed Method
31	[37]	Particularly in the context of Pakistan, management and resources are deemed more important for the success of e-government services than social and economic factors.	Multiple agencies in Pakistan	Critical Success Factors	E-government Success in Pakistan	Mixed
32	[29]	Incident management trainings should be initiated by government.	N/A	N/A	Incident management practices	Review

References

1. Reddick, C.; Anthopoulos, L. Interactions with e-government, new digital media and traditional channel choices: Citizen-initiated factors. *Transform. Gov. People Process Policy* **2014**, *8*, 398–419. [CrossRef]
2. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [CrossRef]
3. Shah, M.H.; Jones, P.; Choudrie, J. Cybercrimes prevention: Promising organisational practices. *Inf. Technol. People* **2019**, *32*, 1125–1129. [CrossRef]
4. Phillips, A.; Ojelade, I.; Taiwo, E.; Obunadike, C.; Oloyede, K. Cyber-Security Tactics in Mitigating Cyber-Crimes: A Review and Proposal. *Int. J. Cryptogr. Inf. Secur. IJCIS* **2023**, *13*. Available online: https://airccse.org/journal/ijcis/current2023.html (accessed on 1 August 2024).
5. McLaughlin, M.D.; Gogan, J. Challenges and best practices in information security management. *MIS Q. Exec.* **2018**, *17*, 237–262.
6. Dupont, B. Enhancing the effectiveness of cybercrime prevention through policy monitoring. *J. Crime Justice* **2019**, *42*, 500–515. [CrossRef]
7. Malodia, S.; Dhir, A.; Mishra, M.; Bhatti, Z.A. Future of e-Government: An integrated conceptual framework. *Technol. Forecast. Soc. Change* **2021**, *173*, 121102. [CrossRef]
8. Patterson, C.M.; Nurse, J.R.C.; Franqueiraand, V.N.L. Learning from cyber security incidents: A systematic review and future research agenda. *Comput. Secur.* **2023**, *132*, 103309. [CrossRef]
9. Ganin, A.A.; Quach, P.; Panwar, M.; Collier, Z.A.; Keisler, J.M.; Marchese, D.; Linkov, I. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Anal.* **2020**, *40*, 183–199. [CrossRef]
10. Dias, G.P. Fifteen years of e-government research in Ibero-America: A bibliometric analysis. *Gov. Inf. Q.* **2019**, *36*, 400–411. [CrossRef]
11. Ramzy, M.; Ibrahim, B. The evolution of e-government research over two decades: Applying bibliometrics and science mapping analysis. *Libr. Hi Tech* **2022**, *42*, 227–260. [CrossRef]
12. Chan, F.K.; Thong, J.Y.; Brown, S.A.; Venkatesh, V. Design characteristics and service experience with e-government services: A public value perspective. *Int. J. Inf. Manag.* **2025**, *80*, 102834. [CrossRef]
13. Khan, F.; Kim, J.H.; Mathiassen, L.; Moore, R. DATA BREACH MANAGEMENT: AN INTEGRATED RISK MODEL. *Inf. Manag.* **2021**, *58*, 103392. [CrossRef]

14. Djotaroeno, M.; Beulen, E. Information Security Awareness in the Insurance Sector: Cognitive and Internal Factors and Combined Recommendations. *Information* **2024**, *15*, 505. [CrossRef]
15. Hobensack, M.; von Gerich, H.; Vyas, P.; Withall, J.; Peltonen, L.-M.; Block, L.J.; Davies, S.; Chan, R.; Van Bulck, L.; Cho, H.; et al. A rapid review on current and potential uses of large language models in nursing. *Int. J. Nurs. Stud.* **2024**, *154*, 104753. [CrossRef]
16. Garritty, C.; Gartlehner, G.; Nussbaumer-Streit, B.; King, V.J.; Hamel, C.; Kamel, C.; Affengruber, L.; Stevens, A. Cochrane Rapid Reviews Methods Group offers evidence-informed guidance to conduct rapid reviews. *J. Clin. Epidemiol.* **2021**, *130*, 13–22. [CrossRef]
17. Tricco, A.C.; Antony, J.; Zarin, W.; Strifler, L.; Ghassemi, M.; Ivory, J.; Perrier, L.; Hutton, B.; Moher, D.; Straus, S.E. A scoping review of rapid review methods. *BMC Med.* **2015**, *13*, 224. [CrossRef]
18. King, V.J.; Stevens, A.; Nussbaumer-Streit, B.; Kamel, C.; Garritty, C. Paper 2: Performing rapid reviews. *Syst. Rev.* **2022**, *11*, 151. [CrossRef]
19. E Kelly, S.; Moher, D.; Clifford, T.J. Quality of conduct and reporting in rapid reviews: An exploration of compliance with PRISMA and AMSTAR guidelines. *Syst. Rev.* **2016**, *5*, 79. [CrossRef]
20. Paul, J.; Khatri, P.; Duggal, H.K. Frameworks for developing impactful systematic literature reviews and theory building: What, Why and How? *J. Decis. Syst.* **2023**, *32*, 1–14. [CrossRef]
21. Affairs, U.N.D.o.E.a.S. United Nations E-Government Survey 2022. 2022. Available online: https://www.un-ilibrary.org/content/books/9789210019446 (accessed on 1 August 2024).
22. Basu, S. Cybercrime Insurance is Making the Ransomware Problem Worse. 2022. Available online: https://theconversation.com/cybercrime-insurance-is-making-the-ransomware-problem-worse-189842 (accessed on 10 August 2024).
23. van der Vegt, G.S.; Essens, P.; Wahlström, M.; George, G. Managing Risk and Resilience. *Acad. Manag. J.* **2015**, *58*, 971–980. [CrossRef]
24. Safi, A.J.; Mahmood, S.M.J. Strategic Management Practices in the Public Sector: A literature review–Descriptive. *Int. J. Adv. Multidiscip. Res.* **2021**, *9*, 88–104. [CrossRef]
25. Kassa, Y.W.; James, J.I.; Belay, E.G. Cybercrime Intention Recognition: A Systematic Literature Review. *Information* **2024**, *15*, 263. [CrossRef]
26. Yeboah-Ofori, A.; Opoku-Boateng, F.A. Mitigating cybercrimes in an evolving organizational landscape. *Contin. Amp. Resil. Rev.* **2023**, *5*, 53–78. [CrossRef]
27. Holt, T.J. Regulating Cybercrime through Law Enforcement and Industry Mechanisms. *Ann. Am. Acad. Political Soc. Sci.* **2018**, *679*, 140–157. [CrossRef]
28. Enigbokan, O.K.; Ajayi, N. Managing Cybercrimes Through the Implementation of Security Measures. *J. Inf. Warf.* **2017**, *16*, 112–129.
29. Tøndel, I.A.; Line, M.B.; Jaatun, M.G. Information security incident management: Current practice as reported in the literature. *Comput. Secur.* **2014**, *45*, 42–57. [CrossRef]
30. Singh, A.N.; Gupta, M. Information Security Management Practices: Case Studies from India. *Glob. Bus. Rev.* **2017**, *20*, 253–271. [CrossRef]
31. Zhang, H.; Tang, Z.; Jayakar, K. A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommun. Policy* **2018**, *42*, 409–420. [CrossRef]
32. Chatterjee, S.; Kar, A.K.; Dwivedi, Y.K.; Kizgin, H. Prevention of cybercrimes in smart cities of India: From a citizen's perspective. *Inf. Technol. People* **2019**, *32*, 1153–1183. [CrossRef]
33. Malik, M.S.; Islam, U. Cybercrime: An emerging threat to the banking sector of Pakistan. *J. Financ. Crime* **2019**, *26*, 50–60. [CrossRef]
34. Mukhopadhyay, A.; Chatterjee, S.; Bagchi, K.K.; Kirs, P.J.; Shukla, G.K. Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Inf. Syst. Front.* **2019**, *21*, 997–1018. [CrossRef]
35. Topa, I.; Karyda, M. From theory to practice: Guidelines for enhancing information security management. *Inf. Comput. Secur.* **2019**, *27*, 326–342. [CrossRef]
36. Eboibi, F.E.; Richards, N.U. Electronic taxation and cybercrimes in Nigeria, Kenya and South Africa: Lessons from Europe and the United States of America. *Commonw. Law Bull.* **2019**, *45*, 716–741. [CrossRef]
37. Hassan, M.H.; Lee, J. Policymakers' perspective about e-Government success using AHP approach: Policy implications towards entrenching Good Governance in Pakistan. *Transform. Gov. People Process Policy* **2019**, *13*, 93–118. [CrossRef]
38. Benz, M.; Chatterjee, D. Calculated risk? *A cybersecurity evaluation tool for SMEs. Bus. Horiz.* **2020**, *63*, 531–540. [CrossRef]
39. Diesch, R.; Pfaff, M.; Krcmar, H. A comprehensive model of information security factors for decision-makers. *Comput. Secur.* **2020**, *92*, 101747. [CrossRef]
40. Malatji, M.; Marnewick, A.; von Solms, S. Validation of a socio-technical management process for optimising cybersecurity practices. *Comput. Secur.* **2020**, *95*, 101846. [CrossRef]
41. Politanskyi, V.; Lukianov, D.; Ponomarova, H.; Gyliaka, O. Information Security in E-Government: Legal Aspects. *Cuest. Politicas* **2021**, *39*, 361–372. [CrossRef]
42. Krishna, B.; Sebastian, M.P. Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: A cross-country analysis. *Inf. Comput. Secur.* **2021**, *29*, 737–760. [CrossRef]

43. Mishra, S.; Alowaidi, M.A.; Sharma, S.K. Impact of security standards and policies on the credibility of e-government. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 1–15. [CrossRef]
44. Annarelli, A.; Clemente, S.; Nonino, F.; Palombi, G. *Effectiveness and Adoption of NIST Managerial Practices for Cyber Resilience in Italy*; Springer: Cham, Switzerland, 2021.
45. Mugarura, N.; Ssali, E. Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *J. Money Laund. Control.* **2021**, *24*, 10–28. [CrossRef]
46. Alhalafi, N.; Veeraraghavan, P. Self-sufficiencies in Cyber Technologies: A requirement study on Saudi Arabia. *Int. J. Comput. Sci. Netw. Secur.* **2022**, *22*, 204–214. [CrossRef]
47. Al-Ma'Aitah, M.A. Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *Electron. J. Inf. Syst. Dev. Ctries.* **2022**, *88*, e12223. [CrossRef]
48. Alhadidi, I.; Nweiran, A.; Hilal, G. The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon* **2024**, *10*, e32371. [CrossRef]
49. Akinbowale, O.E.; Klingelhöfer, H.E.; Zerihun, M.F. Analytical hierarchy processes and Pareto analysis for mitigating cybercrime in the financial sector. *J. Financ. Crime* **2021**, *29*, 984–1008. [CrossRef]
50. Anwary, I. Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach. *Int. J. Cyber Criminol.* **2023**, *17*, 12–22. [CrossRef]
51. Al-Kumaim, N.H.; Alshamsi, S.K. Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership. *Appl. Sci.* **2023**, *13*, 5839. [CrossRef]
52. Khadam, N.; Anjum, N.; Alam, A.; Mirza, Q.A.; Assam, M.; Ismail, E.A.; Abonazel, M.R. How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. *Heliyon* **2023**, *9*, e22823. [CrossRef]
53. Mugari, I.; Kunambura, M.; Obioha, E.E.; Gopo, N.R. Trends, impacts and responses to cybercrime in the Zimbabwean retail sector. *Safer Communities* **2023**, *22*, 254–265. [CrossRef]
54. Lee, C.S.; Chua, Y.T. The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime Delinq.* **2024**, *70*, 2250–2277. [CrossRef]
55. Mahmood, S.; Chadhar, M.; Firmin, S. Countermeasure Strategies to Address Cybersecurity Challenges Amidst Major Crises in the Higher Education and Research Sector: An Organisational Learning Perspective. *Information* **2024**, *15*, 106. [CrossRef]
56. Akinbowale, O.E.; Klingelhöfer, H.E.; Zerihun, M.F.; Mashigo, P. Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon* **2024**, *10*, e23491. [CrossRef] [PubMed]
57. Abubakari, Y.; Amponsah, A.A. Amponsah, Economic cybercrime in the diaspora: Case of Ghanaian nationals in the USA. *J. Money Laund. Control.* **2024**, *27*, 1–20. [CrossRef]
58. Bannister, F.; Connolly, R. The great theory hunt: Does e-government really have a problem? *Gov. Inf. Q.* **2015**, *32*, 1–11. [CrossRef]
59. Leukfeldt, E.R. Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behav. Soc. Netw.* **2014**, *17*, 551–555. [CrossRef]
60. Jansen, J.; Leukfeldt, R. Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *Int. J. Cyber Criminol.* **2016**, *10*, 79.
61. Leukfeldt, E.R.; Yar, M. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behav.* **2016**, *37*, 263–280. [CrossRef]
62. Graham, R.; Triplett, R. Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behav.* **2017**, *38*, 1371–1382. [CrossRef]
63. Akdemir, N.; Lawless, C.J. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Res.* **2020**, *30*, 1665–1687. [CrossRef]
64. Ghazi-Tehrani, A.K.; Pontell, H.N. Phishing evolves: Analyzing the enduring cybercrime. *Vict. Offenders* **2021**, *16*, 316–342. [CrossRef]
65. Ireland, L. Predicting online target hardening behaviors: An extension of routine activity theory for privacy-enhancing technologies and techniques. *Deviant Behav.* **2021**, *42*, 1532–1548. [CrossRef]
66. Lee, Y.Y.; Gan, C.L.; Liew, T.W. Phishing victimization among Malaysian young adults: Cyber routine activities theory and attitude in information sharing online. *J. Adult Prot.* **2022**, *24*, 179–194. [CrossRef]
67. Williams, M.L. Guardians upon high: An application of routine activities theory to online identity theft in europe at the country and individual level. *Br. J. Criminol.* **2015**, *56*, 21–48. [CrossRef]
68. Eck, J.E. Examining routine activity theory: A review of two books. *Justice Q.* **1995**, *12*, 783–797. [CrossRef]
69. Eck, J.E.; Clarke, R.V. Situational Crime Prevention: Theory, Practice and Evidence. In *Handbook on Crime and Deviance*; Krohn, M., Hendrix, N., Penly Hall, G., Lizotte, A., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 355–376.
70. Wang, J.; Gupta, M.; Rao, H.R. Insider threats in a financial institution. *MIS Q.* **2015**, *39*, 91–112. [CrossRef]
71. Almansoori, A.; Al-Emran, M.; Shaalan, K. Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Appl. Sci.* **2023**, *13*, 5700. [CrossRef]
72. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* **2016**, *56*, 70–82. [CrossRef]

73. Safa, N.S.; Maple, C.; Furnell, S.; Azad, M.A.; Perera, C.; Dabbagh, M.; Sookhak, M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Gener. Comput. Syst.* **2019**, *97*, 587–597. [CrossRef]
74. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q.* **2018**, *42*, 285–311. [CrossRef]
75. Hong, K.; Chi, Y.; Chao, L.R.; Tang, J. An integrated system theory of information security management. *Inf. Manag. Comput. Secur.* **2003**, *11*, 243–248. [CrossRef]
76. Trang, S.; Brendel, B. A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Inf. Syst. Front.* **2019**, *21*, 1265–1284. [CrossRef]
77. Holt, T.J. Understanding the state of criminological scholarship on cybercrimes. *Comput. Hum. Behav.* **2023**, *139*, 107493. [CrossRef]
78. Straub, D.W.; Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Q.* **1998**, *22*, 441. [CrossRef]
79. Lohrke, F.T.; Frownfelter-Lohrke, C. Cybersecurity research from a management perspective: A systematic literature review and future research agenda. *J. Gen. Manag.* **2023**, *48*, 1–25. [CrossRef]