information

Article

Countermeasure Strategies to Address Cybersecurity Challenges Amidst Major Crises in the Higher Education and Research Sector: An Organisational Learning Perspective

Samreen Mahmood *, Mehmood Chadhar and Selena Firmin

Centre for Smart Analytics (CSA), Federation University, MT Helen Campus, Ballarat 3350, Australia; m.chadhar@federation.edu.au (M.C.); s.firmin@federation.edu.au (S.F.)
* Correspondence: samreen.mahmood@federation.edu.au

Abstract: Purpose: The purpose of this research paper was to analyse the counterstrategies to mitigate cybersecurity challenges using organisational learning loops amidst major crises in the Higher Education and Research Sector (HERS). The authors proposed the learning loop framework revealing several counterstrategies to mitigate cybersecurity issues in HERS. The counterstrategies are explored, and their implications for research and practice are discussed. Methodology: The qualitative methodology was adopted, and semi-structured interviews with cybersecurity experts and top managers were conducted. Results: This exploratory paper proposed the learning loop framework revealing introducing new policies and procedures, changing existing systems, partnership with other companies, integrating new software, improving employee learning, enhancing security, and monitoring and evaluating security measures as significant counterstrategies to ensure the cyber-safe working environment in HERS. These counterstrategies will help to tackle cybersecurity in HERS, not only during the current major crisis but also in the future. Implications: The outcomes provide insightful implications for both theory and practice. This study proposes a learning framework that prioritises counterstrategies to mitigate cybersecurity challenges in HERS amidst a major crisis. The proposed model can help HERS be more efficient in mitigating cybersecurity issues in future crises. The counterstrategies can also be tested, adopted, and implemented by practitioners working in other sectors to mitigate cybersecurity issues during and after major crises. Future research can focus on addressing the shortcomings and limitations of the proposed learning framework adopted by HERS.

Keywords: organisational learning; cybersecurity; counterstrategies; learning loops; crisis

check for updates

Citation: 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. https://doi.org/10.3390/info15020106

Academic Editor: Theodora Tsikrika

Received: 16 December 2023
Revised: 21 January 2024
Accepted: 25 January 2024
Published: 9 February 2024

1. Introduction

Cybersecurity challenges have increased exponentially in recent years with major crises and remote work. The rapid increase in cybersecurity challenges has posed a heavy burden on businesses across the globe. Recent literature has highlighted an immense increase in cybersecurity challenges during the COVID-19 crisis [1–4]. Although every significant sector is facing cybersecurity challenges, the Higher Education and Research Sector is particularly vulnerable to these issues [5]. Especially, in Australia, the Australian Cybersecurity Centre (ACSC) reports HERS as the second-largest sector to suffer from cybersecurity vulnerabilities during a major crisis [6].

To survive, organisations have adapted and implemented different counterstrategies to mitigate these emerging cybersecurity challenges in HERS amidst the major crisis. HERS is defined as universities, tech colleges, and other institutions providing tertiary education curriculums [7]. Prior literature has identified the issue of increasing cybersecurity challenges during major crises [1,2,8]. However, most of the research studies are conceptual, literature review papers and do not focus on any sector, particularly HERS [3,8–11]. Also, few research studies have explored strategies to tackle cybersecurity issues [9,12]. For instance, a recent study gave recommendations to avoid cybersecurity issues [13]. Yet, the study recommendations are based on already published literature including WHO, Interpol, and Kaspersky reports and lack empirical exploration of these counterstrategies in HERS.

Previous cybersecurity studies focusing on Higher Education Institutions (HEIs) have mostly included students as their unit of analysis for the research study [14–16]. The unit of analysis for the current research study is cybersecurity experts and top managers employed and working in HERS.

The research paper aims to examine counterstrategies adopted and implemented in HERS exclusively in Australia to mitigate cybersecurity challenges amidst major crises using the Organizational Learning (OL) theory. Prior studies have used the Organisational Learning (OL) theory to explore cybersecurity incidents [8,17–19]. For instance, a recent research study [17] has used the double-loop learning approach from OL theory proposed by Argyris and Schon [20,21]. However, the study is a systematic literature review and has recommended that more research is needed to understand the right learning practices required because of reported cybersecurity incidents. Similarly, a research study has used single- and double-loop learning and proposed a comprehensive framework for the management of specific cyber resources [18]. However, the findings are based on prior literature, and the study itself outlines that there is a need to empirically test the proposed conceptual model in organisational settings. A research study suggested that future incident response research must incorporate a learning focus and facilitate double-loop learning [19]. Yet, the study is a literature review paper. Hence, the current study aims to bridge the abovementioned research gaps. The study will empirically investigate counterstrategies to mitigate these emerging issues during and after the major crisis in HERS in Australia and will reveal new theoretical and practical insights for scholars and practitioners, respectively. The guiding research question for this study is:

How do organisations learn and develop counterstrategies to address cybersecurity challenges in a major crisis?

The contribution of the current research to the literature on counterstrategies to enhance cybersecurity in organizations amidst major crises is manifold. Firstly, the study proposes a learning framework demonstrating multiple counterstrategies to minimise cybersecurity challenges during and after a major crisis. The study presents an improved learning method by empirically exploring several counterstrategies in response to emerging cybersecurity challenges amidst a major crisis in HERS. Secondly, the study uses OL theory and classifies these counterstrategies following literature definitions of single-, double-, and triple-loop learning. Thirdly, the study is the first to reveal these counterstrategies by empirically exploring the viewpoints of cybersecurity experts and top managers employed and working in HERS during and after the major crisis. Finally, the study proposed counterstrategies that can help other HEIs in efficiently responding to cybersecurity challenges in future crises. Also, practitioners working in other sectors can adopt and implement these strategies to minimise various cybersecurity challenges that emerged amidst major crises and ensure a secure working environment in their organisations.

The paper is structured as follows: in Section 2, we have discussed the literature review. Section 3 explains the methodology and Section 4 represents the results and findings of our research. The final section includes theoretical and practical contributions, conclusions, and future recommendations.

2. Literature Review

This section reviews the main areas of the literature that are relevant to the current research study. The literature review continues with an investigation of cybersecurity challenges and organisational learning theories.

2.1. Cybersecurity

Cybersecurity is defined as assembling organisational resources, processes, and structures to defend cyberspace and cyberspace-enabled systems from external threats [22].

Furthermore, cybersecurity issues are also defined as protecting the use of electronic data in an organisation from criminal or unauthorised external parties [23]. In the COVID-19 crisis, these various types of cybersecurity challenges increased tremendously. Recent studies claim that remote work practices in the COVID-19 crisis have tremendously increased cybersecurity attacks [1,2]. Cybercrimes significantly increased in 2020 because employees were working away from the central office location during the COVID-19 pandemic worldwide, including in Australia [2]. Moreover, the Australian Cyber Security Centre (ACSC) has stated that it has received more than 45 pandemic-themed cybercrime and cybersecurity incident reports [24]. Research studies by Aljohani [3] and ACSC [6] have pointed out an immense increase in cybersecurity challenges and their associated costs for organisations. The most common attacks reported in the COVID-19 pandemic include Phishing Attacks, Malware Attacks, Ransomware Attacks, and Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks [1,2,4,12,25].

Based on the above discussion, it can be argued that the literature has reported an immense increase in cybersecurity challenges during the major crisis worldwide, including in Australia. However, to the best of our knowledge, there is a lack of research studies that have empirically investigated the OL process that proceeds to the development of counterstrategies to mitigate these issues amidst the major crisis.

2.2. Organisational Learning

OL is the process of detecting and rectifying errors [20]. In OL, the implementation of new knowledge results in strategic changes based on experiences. This new information implementation helps improve organisational performance [21,26]. This novel information can bring changes to organisational counterstrategies, ultimately leading to improved organisational performance.

The three theoretical classes of OL consist of several common factors and assumptions, including the organisational adaptation perspective, collective learning perspective, and learning as a business. From the organisational adaptation perspective, an organisation is considered the unit of analysis. How organisations learn to change and adapt is observed [27]. This change and adaptation can be the consequence of entity-level cognitive learning capacities [28] or any change in these entity systems, daily practices, structures, and processes [29,30]. For this study, an organisational adaptation perspective is adopted because the study will be investigating changes in organisational strategies and structures to mitigate cybersecurity issues.

The OL model consists of three loops, as shown in Figure 1 [21,31]: (1) single-loop learning, (2) double-loop learning, and (3) triple-loop learning. Changes in organisational behaviour link to the nature and extent of each of these loops. Single-loop learning refers to the adaptive response of an organisation to varying circumstances. It helps in enhancing organisational knowledge and expertise without changing predefined goals and objectives. Double-loop learning includes evaluating and redefining the organisational goals, strategies, and mental maps. Double-loop learning is adopted when current business goals and strategies are inadequate [32]. Triple-loop learning, also known as deuteron learning, happens when current organisation models are no longer sufficient [32]. In triple-loop learning, new processes or strategies are implemented to reframe organisation mental maps, as shown in Figure 2 [31]. For this study, to analyse the data, all single-, double-, and triple-loop learning approaches were considered.

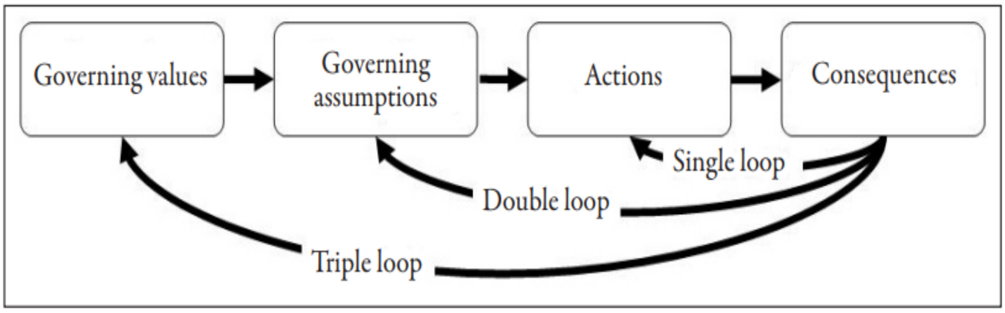

Figure 1. Organisational Learning [21].

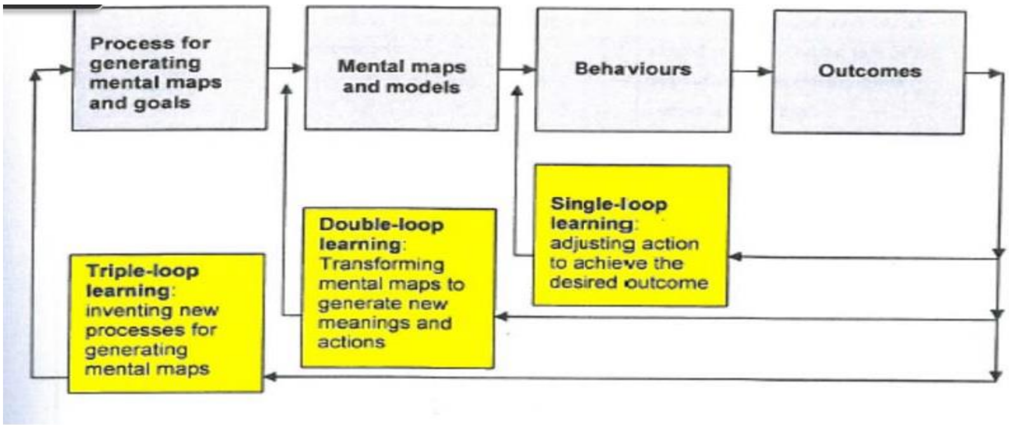
Process for generating mental maps and goals
Mental maps and models
Behaviours
Outcomes
Single-loop learning: adjusting action to achieve the desired outcome
Double-loop learning: Transforming mental maps to generate new meanings and actions
Triple-loop learning: inventing new processes for generating mental maps

Figure 2. Single-, Double- and Triple-Loop Learning [31].

2.3. Cybersecurity and Organisational Learning

Multiple studies are using various learning frameworks to report cybersecurity instances in different sectors. One of the recent research studies has transformed the incident response framework into a hybrid mode [33]. The framework's key focus is preparation, detection, analysis, and recovery from the incident. However, the framework does not cover the OL aspect in responding to the incident. Similarly, another survey study has investigated the cybersecurity learning experience during remote working practice [16]. The study has used the NIST NICE cybersecurity framework for analysing the data. The NICE framework involves analysing, collecting, investigating, and protecting against the incident. Although, the framework is widely used in the literature; however, the current study focuses on the OL aspect in responding to the cybersecurity challenge, which is lacking in this framework. Furthermore, a research paper has proposed the novel HEART of Information Security (HEART-IS) technique to assess human-error-related security incidents [34]. The framework's primary attention is limited to human-error-related cybersecurity incidents. Whereas, the current study has a broader perspective and covers the counterstrategies to cybersecurity issues reported exclusively during and after the major crisis using the OL process.

Apart from the abovementioned literature, few studies have used OL loops to report various cybersecurity incidents. For instance, a recent research study [17] used the double learning approach from the OL theory proposed by Argyris and Schon [20,21]. The study has reported various cybersecurity incidents based on the OL theoretical lens. However, the study is a systematic literature review and has recommended that more research is needed to understand the right learning practices required because of reported cybersecurity incidents. Similarly, a research study has used single- and double-loop learning and proposed a comprehensive framework for the management of specific cyber resources [18]. However, the study is conceptual in nature. The findings are based on prior literature, and the study itself outlines that there is a need to empirically test the proposed conceptual model in organisational settings, and it has not focused on any sector to test this integration.

Besides this, a research study has found that integrating information security management and incident response can lead to better security through learning [8]. However, the study emphasized improving incident response capabilities in any organisation rather than the current counterstrategies. Similarly, a research study suggested that future incident response research must incorporate a learning focus and facilitate double-loop learning [19]. Yet, the study is a literature review paper.

Another significant research gap identified from the literature is the type of industry chosen in these research studies. Most of the prior research studies exploring cybersecurity challenges using various frameworks have been conducted in the study of the healthcare sector [33,35]. Some have focused on financial organisations [36,37], while another research paper reports the findings from the petroleum industry [38]. However, HERS is the industry that does not attract much attention from researchers when exploring counterstrategies to mitigate cybersecurity challenges. The literature reports an immense increase in cybersecurity issues in HERS during this major COVID-19 crisis [6,39,40]. Therefore, the current study has exclusively focused on HERS to explore counterstrategies to mitigate cybersecurity challenges that emerged amidst major crises using learning loops.

Also, the unit of analysis is of primary importance when conducting a research study. Prior research studies proposing a framework for security incidents have focused on general employees, students, IT professionals, and healthcare professionals as participants for their research study [16,34,35]. Whereas, few studies have involved network response, incident response, security, and risk managers, IS policy managers, and senior managers as primary participants [36,37]. However, both studies' industry sector is different (financial organisation), and both studies were conducted before the major COVID-19 crisis happened in 2019. Table 1 elaborates further on the frameworks, industry type, participants, and methodology used in the literature.

The existing literature on investigating counterstrategies to minimise cybersecurity challenges through the OL process amidst the major crisis in HERS has some limitations. Firstly, most of the research has highlighted an increase in cybersecurity challenges during the COVID-19 crisis [1–4] but does not involve empirical exploration of counterstrategies to minimise these challenges during and after major crises. Secondly, prior literature has not used OL theory to explore counterstrategies exclusively developed to tackle cybersecurity issues that emerged in HERS amidst a major crisis [16,33,34]. As mentioned above, the studies using OL loops about cybersecurity are conceptual, literature reviews, and lack empirical evidence [17,18], Moreover, the studies have different units of analysis [16] and have focused on different sectors [33,35–37]. The current study aims to fill all these identified research gaps.

Table 1. Summary of Prior Research Studies.

Reference	Framework/Model/Theory	Elements in Framework	Industry	Methodology	Publication Year	Participants	Type of Paper
[33]	Incident Response Framework	Preparation, Detection and Analysis, Containment, Eradicate and Recover, Post Incident activities	healthcare in the UK	case study	2022	not specified	case study
[8]	Organisational learning theory to integrate information security management and incident responses	Single-loop learning and double-loop learning	not specified	not specified	2020	not specified	Conceptual paper
[34]	Create the novel HEART of Information Security (HEART-IS) technique to assess human-error-related security incidents and Reduction Technique (HEART-IS)	HEART Generic Task Types (GTT) and Error-Producing Conditions (EPC).	service industry	case study (one service industry organisation)	2019	all employees	empirical paper using security incidents reports
[35]	Security Assurance Model to link lesson learned from security incidents	1. Violated security requirements and objectives 2. Causes and solutions of security lessons learned	healthcare in China	case study	2017	IT professionals and healthcare professionals	empirical study using interviews
[37]	Proposed dynamic security process model based on the 4I model of organisational learning	Intuiting, Interpreting, Integrating, Institutionalizing	the financial organisation in Australia	case study	2015	Incident report team, Security, and Senior Managers	Empirical study using interviews
[36]	The proposed revised incident learning system	Response, identification, investigation, reporting, causal analysis, single-loop learning, double-loop learning, incident response process	global financial organisation	case study	2012	Network response, incident response, security and risk, and IS policy managers	Exploratory
[19]	Future incident response research must incorporate a learning focus and facilitate double-loop learning.	Double-loop learning	not specified	not specified	2010	secondary data	conceptual literature review paper
[38]	Incident Response Management (IRMA) method	proactive learning and sociotechnical actors	petroleum Industry	case study	2009	not specified	accident analysis

3. Methodology

This section introduces, justifies, and details the research methodology used in the current research study.

3.1. Research Design

The qualitative research method will be used for this research study. Qualitative research emphasises meanings in context [41] and is typically used for the investigation of complex phenomena. Exploring counterstrategies to address cybersecurity issues is complicated because (1) the literature points out that exploring counterstrategies to cybercrimes is a complex phenomenon [42], (2) cybersecurity is a manifold challenge for organisations [43], and (3) investigating counterstrategies for cybersecurity challenges requires a wide-ranging knowledge of cybersecurity challenges in the organisation [44]. Therefore, the qualitative research method will be more appropriate as it is most suitable when exploring a complex phenomenon and investigating how people interpret their experiences [45,46].

Other key features that led to choosing a qualitative methodology for this study are the nature of the research problem, existing knowledge of the phenomenon, and the research question under investigation. The first key feature is the nature of the research problem under investigation [47]. In this research study, exploring counterstrategies to cybersecurity issues that emerged exclusively during the major crisis in HERS is under investigation, and the literature suggests that when exploring and interpreting the nature of changing experiences about organisational processes, qualitative types of research are more preferable [47].

The second key feature of choosing a qualitative methodology for this study is the knowledge of the phenomenon being investigated [47]. Previous research papers have highlighted cybersecurity challenges faced during the major crisis, and few of the documents have provided recommendations based on their subjective viewpoints [1,2,9,12,48]. However, the topic of this research is new. To the best of our knowledge, no previous in-depth exploratory study has been conducted on exploring an organisational learning process that initiates counterstrategies to these cybersecurity challenges considering a particular sector amidst major crises. Previous research studies highlight that qualitative methodology is best to use when little knowledge exists about the research problem being investigated [47,49].

The third key feature is the type of research questions. In this study, the focus is to explore counterstrategies in response to emerging cybersecurity challenges during and after the major crisis. The literature depicts that deciding the methodology for a research study depends upon the research question being asked [50]. Furthermore, the qualitative method is preferred when asking how, what, and why questions [50,51]. Also, the qualitative method is desirable when looking for exploration rather than numerical answers [50].

3.2. Context

The current study examines the phenomenon of OL that triggers strategic changes in response to increasing cybersecurity challenges in HERS. The study explores OL processes in the context of HEIs operating in Australia during and after major crises. At the time of the interviews, it was ensured that all HEIs were operating and working amidst a major crisis. Also, all the participants were employed and actively participated in devising, adopting, and implementing organisational strategic changes to minimize cybersecurity challenges in HERS.

3.3. Data Collection

All three researchers were involved in the interviews. Cybersecurity experts and top managers directly involved in the organisational strategic learning process to tackle cybersecurity challenges were selected as participants for this study. A snowball sampling technique was used as prior literature suggests that personal contacts can be used to select the appropriate cases. The snowball sampling method is defined as accessing informants through the contact information provided by other informants, usually via social networks and personal contacts [52,53]. Various HR and top management individuals in HERS were contacted through emails and social networks, and an overview of the research study, the reason their participation is valuable for this research study, and the involvement that would be required if they chose to participate was included in the email. However, participation by the case organisation was voluntary. Table 2 provides further information about the interviewees. In total, 23 interviews were conducted between September 2022 and May 2023. All the interviews were audiotaped and then transcribed by the first author after obtaining permission from the participant. The final transcription of the interview was shared by the relevant interviewee to read and amend anything. After receiving a positive response from the interviewee, the final transcription was used for further analysis. Interview questions focused on various types of cybersecurity challenges that emerged amidst major crises, what strategical changes the organisations came up with to tackle these issues, and how the organisations' learning process was triggered because of increasing cybersecurity issues. Probing questions like elaborating on specific examples and strategies were asked to acquire an in-depth knowledge of various strategies that are used in HERS.

Table 2. Interview Description Table.

Code Assigned	Role	Experience
C001	Chief Security Officer (CSO)	11 years
C002	Information Security Manager (ISM)	3 years
C003	Senior IT Manager	5 years
C004	Cybersecurity Analyst	9 years
C005	CSO	9 years
C006	Strategic Manager	6 years
C007	Cybersecurity Lead	10 years
C008	Data security Analyst	4 years
C009	Security Testing Manager	5 years
C010	Information Security Officer (ISO)	9 years
C011	CSO	13 years
C012	ISM	7 years
C013	Senior IT Manager	9 years
C014	Security Engineer	4 years
C015	ISO	3 years
C016	Senior Executive Officer	7 years
C017	Senior IT Officer	4 years
C018	Senior Security Officer	6 years
C019	Head of Change Management	6 years
C020	Information Security Assistant	4 years
C021	Development Manager	8 years
C022	ISO	5 years
C023	Senior Manager	4 years

4. Data Analysis

The data analysis as shown in Table 3 was performed in two steps. Throughout the iterative analysis, we adopted the principle of theoretical engagement in analysing the data. Theoretical engagement refers to using the theoretical lens from literature in various stages of qualitative data analysis [54]. Firstly, open coding was done. Open coding is described by Strauss and Corbin [47] as the part of the analysis in which data are closely examined to name and categorise. Further, themes were developed as the literature points out that thematic analysis is preferable to content analysis because, in thematic analysis, categories are not decided before data coding [55]. Instead, in thematic analysis, categories are designed from data. Open coding helps to document various themes that will appear during the process. In the second step, theoretical coding was performed. Walsham [56] refers to analysing research data through underpinning theories being used for the research study. For the current study, a theoretical lens of OL theory by Argyris [21] and Snell and Chak [31] is used to guide further data analysis. In other words, we drew on the conceptual foundation of single-, double-, and triple-loop learning initiated by Argyris [21] and Snell and Chak [31]. These learning loops were used to evaluate the organisational strategy process to mitigate cybersecurity challenges in HERS during and post major crisis.

Table 3. Content and Thematic Analysis.

Participant Quotes	Open Coding	Theoretical Coding	Core Themes
The trainings were helpful. Our cloud partners not only verbally discussed but they showed us all by demonstrating each feature in front of us through video meetings in teams.	Cloud service trainings	Improved employee learning	Single-loop learning
We've got cyber security awareness training portal as well. On this portal, our employees can access range of training cybersecurity courses and workshops anytime.	Awareness training portals		
a cybersecurity training awareness program in which every week we were arranging a meeting and discussing various cybersecurity issues which could occur due to remote working. However, that was more like a discussion rather than formal training.	Cybersecurity programs		
one to one online sessions for employees to help them secure office desktops and work in a safe environment	Online sessions		
Non-technical employees were taught to reset and gain temporary password in case of password breaches	Learning password resets		
Every month phishing email campaigns and trainings were sent to all staff members. Simulated phishing emails training were given every week	Phishing email campaigns		
Short videos and quizzes are sent to employee regarding their cybersecurity trainings to keep up to date	Video content		
learning material and exams in a way that it can be conducted online without any issue. So, yes multiple virtual handling skills were developed.	Virtual handling skills		
All employees' mobile devices have a secure check app installed, which is based on the multi-factor authentication technique. As a second authentication, the login is confirmed via our mobile phone app.	Secure check application	Improved security	
There is a security posture document that I personally have been a part of. The document maps what we're going to go with the products that we already had and having to utilize those going forward.	Security posture document		
To stay safe, we then introduced and bounded our staff and employees to use emails, teams associated with their Microsoft institution accounts.	Official email and OneDrive		
We have implemented stronger 'Sensitivity Labels' in Microsoft (Office 365) using the sensitivity option in Microsoft O365 to help you protect your emails and documents. With data constantly being created, edited, stored, and shared within and outside organisation, it is essential to embrace security features like this	Using sensitivity labels		
To avoid such situation to repeat in future, we started using VPN, firewalls	Utilising firewalls		
Even though sharing passwords is strongly discouraged, use LastPass when you need to do so with your team.	Utilising LastPass		
We are doing a Cyber Security Risk Factor analysis across all of the departments and sending information to all departments to save them from the cybersecurity challenges which we have faced or can face during the hybrid work	Incident and risk analysis	Monitoring and evaluating security	
we also employed penetration security testing on schedule to see if they can find any gaps	Security testing		
to deal with these issues, we already have a aim to review through different cybersecurity frameworks and initiate a quarterly report based on that review. The review involves doing security check based on cybersecurity famous frameworks.	Review security		

Table 3. *Cont.*

Participant Quotes	Open Coding	Theoretical Coding	Core Themes
we relocated several of our services to the cloud, we do have agreements where the client supplier is in charge of maintaining the security of the infrastructure.	Adopting cloud computing	Strategic—Integrating other software	Double-loop learning
Windows Defender was made mandatory in order to prevent such malware attacks	Adopting Windows Defender		
We implemented MFA to prevent hackers from accessing our official portals	Implementing multifactor authentication		
our next move is to search for a managed service provider for the system you have been using as an example, which is undoubtedly one of the best management systems. We employ various software that has been outsourced from third parties to provide the 24/7 monitoring systems that we need.	Introducing 24/7 monitoring systems	Strategic thinking—Partnering with other companies	
our crowdstrike falcon endpoint security solution rapidly identified the threat, protecting our data.	partnerships with CrowdStrike Falcon		
we approach that with a better Technology we use mimecast to filter those emails to got a rejection	Partnerships with Mimecast		
Activtrak collaboration was introduced. Activtrak company help us secure and aids in monitoring and analysis	Partnerships with Activtrak		
we have got Cybereason Defense Platform which is our endpiont	Partnerships with Cybereason Defence Platform		
just one final thing to finish, the major change was rearrangement of the whole management and reporting structure in the organisation. Now, the employees were directly reporting to the chief security officers in the cybersecurtiy department unlike before when they were reporting their immediate supervisors only. Remote working and increased cyber issues has proven to be a significant push towards changing of organisational management structures in terms of performing daily tasks and reporting to the heads	Changes in management structures	Strategic learning—Changing the existing systems	
Now its mandatory to include cyber awareness, zero trust in the core values of the organisation to avoid these cyber incident situation in future, now the values of better communication, helping and supporting eachother, listening and acquiring new skills are encouraged to deal with the cyber risks during the hybrid mode of work and make hybrid work a success.	Changes in core organisational values		
Cybersecurity policy was introduced. Cybersecurity policy outlines the uses of systems in a protected way and how to safe yourselves from outer world attacks while working from home.	Cybersecurity policy	Strategic information—Introducing new policies and procedures	Triple-loop learning
So the first one device usage, obviously now the staff is said to use only officially provided laptops, desktops and mobile phones for work no personal devices usage	Device usage policy		
using chatbot app for official conversations	Introducing chatbot app		
Other one I talked about is data access. In this policy, staff is now restricted to reach all data. Security managers has designed the software in this way that only eligible people are able to reach the data they need and no one can change it except the privileged accounts. Privileged accounts are the top people who have authority to manipulate, delete, and add new data.	Introducing access management policy		
The policy key points include presence of all employees, actively participating and sharing their issues and challenges with top management in the mandatory onliny weekly meeting.	Meet-and-greet policy		
Zero trust policy, which we have now implemented, has greatly aided us in preventing and reducing cybersecurity assaults.	Introducing zero trust policy		

5. Results and Findings

All the counterstrategies revealed by the participants were characterised according to single-loop learning, double-loop learning, and triple-loop learning [21,31]. The key findings are summarised in Table 4.

Table 4. Key Findings.

Summary of Key Findings	
Recommended Counterstrategies	**Key Points**
Cybersecurity awareness and training support	One-to-one personalised training programs, introducing cybersecurity awareness training through portals, exclusive cloud service training by cloud providers
Phishing campaign	Training to deal with phishing attacks, introducing simulated phishing emails training sessions, showing phishing content in training to recognise phishing emails
Video learning materials and virtual handling skills	Introducing short videos and quiz activities to test training outcomes, improving virtual handling skills to ensure a smooth transition of activities online
Installing secure check applications in mobile devices, and MFA implementation	Installation of a secure check application in all employees' mobile phones to improve security and avoid password breaches: The secure check app uses the MFA technique.
Developing security posture documents	The document outlines the security status of networks, information, and systems based on information security resources and capabilities in place to manage the defence. It highlights how we would be reacting to external environment changes like in pandemics, disasters.
Using official email and OneDrive for storage purposes	Official documents will only be accessed, sent, and stored in official emails and OneDrive only, saving and access to data through personal emails is prohibited.
Utilising sensitivity labels in Microsoft, and installing firewalls	Stronger "Sensitivity Labels" in Microsoft (Office 365) using the sensitivity option in Microsoft O365 have been implemented to help protect emails and documents. Installation of firewalls in all workstations is ensured.
Using lastpass for password sharing.	Password sharing is discouraged except for in urgent cases. LastPass must be adopted to share passwords.
Adopting cloud computing	Relocation of services to the cloud, agreements where the client–supplier cloud partner oversees ensuring the security
Windows Defender	Adoption of using Windows Defender to avoid certain malware attacks
Activtrak, Cybereason Defence Platform, Mimecast, Falcon CrowdStrike, and other 24/7 security services	Partnerships with certain external entities including ActivTrak, Cybereason Defence Platform, Mimecast, Falcon CrowdStrike, and other 24/7 security services providers to ensure and enhance security and avoid cybersecurity attacks
Incident and risk analysis	Monitoring and evaluation through Cyber Security Risk Factor analysis across all the departments to improve security features
Security testing	Schedule penetration security testing is carried out across the department.
Review security	A security review is carried out quarterly using different cybersecurity frameworks, and the report is shared and discussed to improve security across the organisation.
Changes in management structures	Rearrangement of the whole management and reporting structure, employees directly report to the CSOs in the cybersecurity department
Changes in organisational values	Changes in organisational culture, values of better communication, introducing better support systems, and acquiring new skills are all new values.
Cybersecurity policy	Outlines the uses of systems in a protected way and how to save yourself from outer-world attacks while working from home.
Device usage policy	Use only officially provided laptops, desktops, and mobile phones for work, no personal device usage
Chatbot application	Developed a chatbot app for communication with colleagues and other employees within the department during remote working
Access management policy	Introducing new data restriction rules according to the job titles, guidelines to request any inaccessible data, and instructions for the access and use of data securely
Meet-and-greet policy	The mandatory presence of all employees, actively participating and sharing their issues and challenges with top management, and exchanging ideas with colleagues, and management
Zero-trust policy	No one is trusted, verification is required for everyone who wants to gain access to the system

5.1. Single-Loop Learning

The single-loop learning theme describes all the counterstrategies that result in the modifications of organisational actions. Single-loop learning is defined as modifying the actions to accomplish a desired consequence [21,31]. The single-loop learning contains three primary sub-themes: (1) Improved Employee Learning, (2) Improved Security, and (3) Monitoring and Evaluating.

Analysing this theme outlines all adapted counterstrategies that simulated learning by action, leading to single-loop learning.

5.1.1. Improved Employee Learning

Becoming more skillful and adjusting individual actions to achieve overall organisational goals is studied under the single-loop learning in the literature [31]. In the current study, single-loop learning was enabled in HERS to mitigate cybersecurity challenges by improving employee learning abilities. Cloud service training, arranging cybersecurity awareness programs, running phishing email campaigns, online learning sessions, improving virtual handling skills, developing video learning content, and learning how to improve password security are all counterstrategies to enhance employee skills and abilities and meet the goal of mitigating cybersecurity issues amidst major crises in HERS.

A recent study has highlighted that cybersecurity awareness and training support are beneficial in overcoming cybersecurity challenges during the pandemic [57]. Our findings are consistent with the literature; C012 quoted that “the trainings we provided them has made them even aware of resolving and reporting these incidents quickly as compare to before. All employees now know what the worth is of the cyber department and have expertise in cybersecurity. The future is for only those employees who have knowledge of technology and cybersecurity”.

Furthermore, a research study found that individual education level has a major impact on phishing attacks during the pandemic [58]. C010 mentioned that “we introduce a phishing campaign for everyone and in that I as a expert explain them by examples and screenshots, picture and other images that how a fake URL, scam email will look. We trained our employees to report them and then how they can block those emails. I believe after this campaign, more than 100 ko phishing emails were being reported to us on a daily basis by our employees”. The study extends the current literature by revealing phishing campaigns, video learning materials, and virtual handling skills as significant steps to improve employee education levels and mitigate cybersecurity challenges, including phishing attacks.

5.1.2. Improved Security

Improving the organisational expertise and competency base without modifying existing objectives is termed single-loop learning in the literature [31]. Security features were enhanced to tackle cybersecurity challenges, and this improvement in existing security features is directly related to single-loop learning in organizational learning theory. The counterstrategies to enhance existing organisation security features in HERS include installing secure check applications in mobile devices, developing security posture documents, using official email and OneDrive for storage purposes, utilising sensitivity labels in Microsoft, installing firewalls, and using LastPass for password sharing.

Prior literature has highlighted the use of various Internet of Things applications and the introduction of various security measures in HEIs, respectively [59,60]. However, Adil et al.’s [59] study focus is on smart cities, and Wang et al.’s [60] study is a systematic review. The current study extends the literature by empirically exploring and reporting installing secure check applications in mobile devices as key counterstrategies in HERS during and after a major crisis. C016 quoted that “if they have changed their network or even working stations when they sign in, they have to go to their secure app to approve the sign-in request from their mobile devices. This was to tackle password breach issues”.

Furthermore, a research study has talked about security posture in relation to supply chain capabilities [61]. However, the study is one of the first to report security posture documents as key counterstrategies in improving security in HERS amidst major crises to mitigate cybersecurity issues exclusively. C019 talked about "we have a document called security posture and we actually consulted it several times during cyber risks issues. The document outlines us the security status of our networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defence of our company and it also highlights us how we would be reacting as the situation changes like in pandemics, disasters".

Besides this, prior research studies have highlighted the storing of information in official cloud storage, the use of LastPass as a cybersecurity tool, sensitivity labels for data security, and the use of firewalls and VPNs to ensure a secure environment, respectively [62,63]. The current study confirms the literature by revealing using the official cloud drive for storage, utilising LastPass, sensitivity labels, and installation of firewalls and VPNs as essential counterstrategies in HERS to mitigate cybersecurity issues amidst major crises. C002 mentioned "Implementation of stronger 'Sensitivity Labels' in Microsoft (Office 365) to help protect all personal work documents from hackers and external attackers".

5.1.3. Monitoring and Evaluating Security

According to the literature, examining current organisational capabilities without altering basic activities is studied with single-loop learning in the OL process [31]. Participants highlighted that all the existing security measures were being monitored and evaluated due to increased cybersecurity challenges during the major crisis in HERS. Some of the security testing methods revealed by the participants include incident and risk analysis, security penetration testing, and reviewing security through cybersecurity frameworks.

Prior literature highlights the importance of incident risk analysis for cybersecurity protection [64]. However, the study does not solely focus on using incident and risk analysis as a counterstrategy amidst a major crisis in higher education. Also, another research study summarises the data analysis of 550 security incidents in HEIs [65]. However, the study is a systematic review paper and lacks empirical evidence. Therefore, the current study is significant in empirically confirming the literature for mitigating cybersecurity issues in HERS amidst major crises. C002 revealed that "in 2021, we did a cybersecurity check again by deeply going through the incident and risk analysis".

Previous studies have emphasized the use of penetration testing techniques to overcome cybersecurity challenges during the pandemic [3,66]. However, the study by Abukari and Bankas [66] focuses on teleworkers, and the paper by Aljohani [3] is a conceptual review paper. Yet, the current study empirically revealed penetration testing as one of the significant counterstrategies, as C009 quoted that "penetration security testing was used to monitor our systems. It is also a tool we have been using. It is also known as ethical hacking".

Using different cybersecurity frameworks to overcome cybersecurity issues has been highlighted in prior literature [67,68]. The study confirms the literature, and C005 summarises that "the next security review will be run by Third parties. They will use a different framework. One of the frameworks is the NIST Cyber Security Framework and other I remember is The International Standards Organisation (ISO) frameworks ISO/IEC 27001 and 27002. These frameworks will help us in reality to test those individual areas that we don't consider to be ready worthwhile".

5.2. Double-Loop Learning

In the current study, to avoid cybersecurity issues in HERS, cybersecurity experts and top management revealed ideas of partnerships and outsourcing with other companies. The double-loop learning theme reveals key counterstrategies that resulted in changing or reshaping the existing management practices amidst major crises. Double-loop learning involves reshaping and transforming the existing patterns and mental maps to achieve new actions [31]. The double-loop learning theme contains three primary sub-themes: (1) Strategic—Integrating other software, (2) Strategic thinking—Partnering with other companies, and (3) Strategic learning—Changing the existing systems.

Analysing this theme provides information about changes that led to the abandoning of traditional views and the adoption of new beliefs, also known as changes in mental maps. The findings reveal that strategic integration of various software programs, changes in strategic thinking by partnering with other companies, strategic learning through changes in existing structures, and providing strategic information by introducing changes in policies and procedures were significant counterstrategies implemented in HERS to mitigate cybersecurity issues. These counterstrategies led to the reframing of organisational current structures and values, leading to double-loop learning.

5.2.1. Strategic—Integrating Other Software

Knowing that the current arrangements are inadequate and adopting new systems to achieve organisational goals are studied under double-loop learning [31]. The current study opts to use double-loop learning in HERS to minimise cybersecurity issues by strategically integrating other software in the organisation.

Adopting cloud computing has been highlighted in the literature to minimise cybersecurity issues in higher education, especially during distance learning [40,69]. The study aligns with the current literature; C020 mentioned, "We opted cloud computing, preventing data sharing from any other source other than cloud to tackle these cyber viruses".

Moreover, a recent research study summarises the effectiveness of using Windows Defender against certain ransomware attacks [70]. The study findings confirm the current literature. C011 quoted "Window Defender was also compulsory. Malware attacks were increasing and it was needed to stop them".

Also, in the literature, MFA implementation has been highlighted as a tool to avoid cybersecurity issues in the health and higher education sector during the COVID-19 pandemic [71]. The current study confirms the existing literature by revealing the adoption of MFA techniques in HERS to mitigate cybersecurity challenges during and after a major crisis. To avoid third-party interruptions and session hijacking attacks in HERS, MFA was adopted. C017 talked about it: "Later it was fixed once MFA was implemented. MFA for everyone who was part of that online meeting was ensured to avoid any third irrelevant party from entering in the meeting".

5.2.2. Strategic Thinking—Partnering with Other Companies

In prior studies, developing shared paradigms and transforming existing mental maps to achieve new actions are studied in double-loop learning in the OL literature [20,31]. Participants revealed that partnering and outsourcing with external firms with various expertise is being practiced in HERS to mitigate cybersecurity challenges amidst major crises. The interviewees summarised that their organisations are partnering with various companies including ActivTrak, Cybereason Defence Platform, Mimecast, Falcon CrowdStrike, and other 24/7 security services offering companies to minimise cybersecurity issues.

In the literature, 24/7 security monitoring systems have been discussed [2,72]. However, both research studies are conceptual and do not focus on any sector, particularly HERS. The study extends the prior literature by empirically exploring and revealing a 24/7 monitoring system as an essential counterstrategy adopted by HERS amidst a major crisis. C017 mentioned, "The other major transformation was outsourcing from major IT companies for ensuring continuous 24/7 secure environments by using different software".

Also, previous research studies focusing on HEIs have outlined the reports by Mimecast [73] that summarise that 74% of businesses suffered from various cybersecurity attacks, and the number of cyberattacks increased by 33% [74,75]. However, the study adds to the literature by revealing a partnership between Mimecast and HERS as a significant counterstrategy in Australia to mitigate cybersecurity issues during and after a major crisis. C006 talked about "Mimecast partnership was significant in reducing cyber issues in pandemic".

A recent survey study has discussed Falcon CrowdStrike to be used by different organisations for analysing data and detecting cyberattacks [76]. Yet, the current study revealed it as a transforming strategy adopted in HERS exclusively in Australia to mitigate cybersecurity issues that emerged amidst major crises. C012 mentioned, "partnership with falcon was an intelligent move by us to quickly tackle cybersecurity attacks".

Furthermore, the literature highlights that using the ActivTrak platform for direct supervision was being exercised during the COVID-19 pandemic, but the use of this platform was ineffective [77]. However, our study contradicts the literature, and it is revealed that ActivTrak helped in monitoring and analysing employee work during remote working and ultimately helping in implementing a cybersecure work environment. C004 quoted that "Partnerships proved to be very effective in our case with different security companies. Like collaborating with Mimecast and ActivTrak. ActivTrak, I know, during hybrid work helps us to get better productivity insights and monitor our staff".

Besides this, research studies have talked about various defence platforms to avoid cybersecurity issues during the COVID-19 pandemic [78,79]. However, both studies are systematic literature reviews and lack empirical investigation. The current study initiates to report the Cybereason Defense Platform partnership as a significant counterstrategy in HERS exclusively to tackle cybersecurity issues amidst the major crisis in Australia. C001 revealed, "To help with malware and ransomware attacks particularly, we use their services, we outsourced with a third party named as Cybereason Defense Platform".

5.2.3. Strategic Learning—Changing the Existing Systems

Altering the organisational current norms and values is studied in double-loop learning in the OL theory in the literature [20,31]. In the current study, existing management structures and current organisational values were modified to ensure a cyber-safe working environment in HERS in Australia. These modifications are directly related to the literature definition of double-loop learning [31].

A recent study has highlighted changes in structures in HEIs to manage cybersecurity [60]. The study has highlighted the use of Key Performance Indicators to monitor and assess cybersecurity. However, the current study has reported exclusively the management structural changes from a different perspective and adds to the current literature. The changes are highlighted in the reporting systems and direct communication between top management, the cybersecurity department, and employees. C016 quoted that "the management hierarchy is changed completely. The reporting of issues, resolving them, and communication barriers between top management and employees all have been changed after the pandemic crisis. You know cyber issues were rising day after day we must change our core structure to avoid them. I can tell you it helped really it did".

Prior literature has highlighted the changes in organisational culture and its norms during the pandemic due to digital transformation and managing cybersecurity in HEIs [80,81] The current study confirms the literature by empirically exploring and revealing changes in organisational values as one of the key counterstrategies to tackle cybersecurity issues during and after a major crisis in HERS in Australia. C023 mentioned "Opted for the MFA, Cybereason defence. Introducing zero trust strategy and making it a core value in the organisation structure. Acquiring cybersecurity skills, and flexible communication between employees and CSOs have all become core values in our organisation now".

5.3. Deutero or Triple-Loop Learning

The Triple-loop learning theme describes new organisational policies that were introduced amidst the major crisis in HERS to mitigate emerging cybersecurity challenges. Deutero or triple-loop learning is defined as the invention of new policies and processes in the OL process [31]. The theme contains one primary sub-theme: 1. Strategic information—Introducing new policies and procedures.

Investigating the theme revealed that improving the strategic information by introducing new organisational policies helped in ensuring a secure working environment in HERS amidst a major crisis.

Strategic Information—Introducing New Policies and Procedures

Formulating new strategic policies to improve OL is studied under triple-loop learning [31]. In the current study, triple-loop learning was enabled in HERS to mitigate cybersecurity challenges by introducing and implementing new organisational policies to enhance strategic information. Introducing a cybersecurity policy, device usage policy, chatbot application, access management policy, meet-and-greet policy, and zero-trust policy are all counterstrategies to mitigate cybersecurity issues amidst the major crisis.

Previous literature has generally outlined the changes in working routine policy during the pandemic [1,82]. Also, prior literature has highlighted changes in management policies due to cybersecurity threats in HEIs [83,84]. The paper by Ghavifekr and Fung [84] discussed that multiple short-term policies and tech policies were introduced during the pandemic. However, the current paper has specified the names of new policies and the characteristics of these policies according to the participant's explanations adopted in HERS to minimise cybersecurity issues amidst the major crisis.

The study revealed the meet-and-greet policy introduced in HERS. The main characteristics of the meet-and-greet policy include the mandatory presence of all employees, actively participating and sharing their issues and challenges with top management, and exchanging ideas with colleagues and management. C002 revealed "the meet and greet policy, yes every week for all staff members it was mandatory to attend this meet and greet online meeting with a cup of coffee and there they talk about their experiences of working from home and cybersecurity issues like phishing emails, spam messages about COVID-19 vaccine, etc. I think that was all".

Another significant new policy adopted was the data access policy. The key point in this policy was introducing new data restriction rules according to the job titles, guidelines to request any inaccessible data, and instructions to the access and use of data securely. C012 mentioned "Staff access to all data is now limited under this policy. The policy was created by security administrators so that only authorised users can access the data they require".

Similarly, cybersecurity policy is also introduced, and the main topics covered under this policy are IT assets that need protection and the list of threats identified to these IT assets, rules and controls for protecting these assets from external attacks. C004 talked about "now I think all institutions have this cybersecurity policy that was actually introduced during COVID-19 pandemic".

Besides this, a chatbot application is introduced. The organisation has developed a chatbot app for communication with colleagues and other employees within the department during remote working. C017 said "we have a chatbot on our portals now, we can report cyber issues more quickly".

Lastly, a zero-trust policy is introduced. In simple words, C002 quoted "zero trust means No one trusts no one. So even though your password is correct, we still need, another ID. I mean your personal ID to confirm". It can be said here that after careful empirical investigation, the study is the first to initiate and report these policies as effective counterstrategies to mitigate increasing cybersecurity challenges in HERS in Australia amidst the major crisis.

6. Discussion

A framework classifying identified counterstrategies according to single-loop, double-loop, and triple-loop learning using OL theory has been formulated, as shown in Figure 3. The left side shows modified definitions of the learning loops framework proposed by Snell and Chak [31] according to the current study in HERS. The middle circles reveal the steps from process to outcome according to the learning framework [31], and the right side highlights the counterstrategies used in HERS under each learning loop to mitigate cybersecurity challenges amidst a major crisis in HERS.

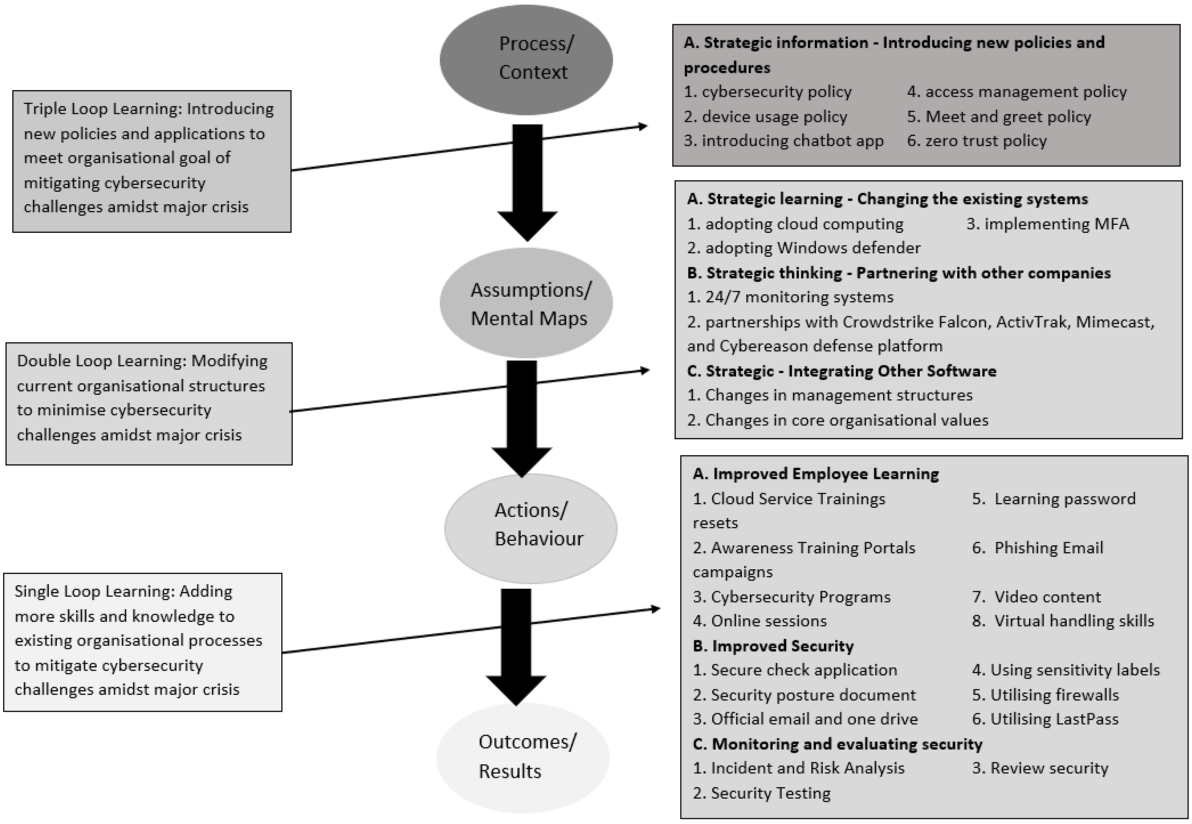
Process/ Context
Assumptions/ Mental Maps
Actions/ Behaviour
Outcomes/ Results
Triple Loop Learning: Introducing new policies and applications to meet organisational goal of mitigating cybersecurity challenges amidst major crisis
Double Loop Learning: Modifying current organisational structures to minimise cybersecurity challenges amidst major crisis
Single Loop Learning: Adding more skills and knowledge to existing organisational processes to mitigate cybersecurity challenges amidst major crisis
A. Strategic information - Introducing new policies and procedures
1. cybersecurity policy
2. device usage policy
3. introducing chatbot app
4. access management policy
5. Meet and greet policy
6. zero trust policy
A. Strategic learning - Changing the existing systems
1. adopting cloud computing
2. adopting Windows defender
3. implementing MFA
B. Strategic thinking - Partnering with other companies
1. 24/7 monitoring systems
2. partnerships with Crowdstrike Falcon, ActivTrak, Mimecast, and Cybereason defense platform
C. Strategic - Integrating Other Software
1. Changes in management structures
2. Changes in core organisational values
A. Improved Employee Learning
1. Cloud Service Trainings
2. Awareness Training Portals
3. Cybersecurity Programs
4. Online sessions
5. Learning password resets
6. Phishing Email campaigns
7. Video content
8. Virtual handling skills
B. Improved Security
1. Secure check application
2. Security posture document
3. Official email and one drive
4. Using sensitivity labels
5. Utilising firewalls
6. Utilising LastPass
C. Monitoring and evaluating security
1. Incident and Risk Analysis
2. Security Testing
3. Review security

Figure 3. Mapping of research study results in the learning framework [31].

The current study's findings have reported counterstrategies to emerging cybersecurity challenges in HERS amidst the major crisis. The study reveals that improved employee learning, improved security and monitoring, and evaluation of current security processes are adding knowledge to organisation current policies, objectives, and mental maps [31] and are studied under single-loop learning. Therefore, all counterstrategies under these themes are placed in single-loop learning in the above framework. In addition, the study found that changes in the existing systems, partnerships with other organisations, and integration of external software are all modifying current organisational policies, norms, and mental maps in HERS to mitigate cybersecurity challenges amidst major crises. These changes are studied in the double-loop learning level proposed by Snell and Chak [31], and therefore, all counterstrategies relevant to these modifications are placed under double-loop learning in the above framework. Finally, introducing new policies and procedures as a counterstrategy to deal with these emerging cybersecurity challenges in HERS amidst major crises is termed as introducing new structures and strategies for learning in an organisation. These new strategies are studied under the triple-loop learning level in the literature [31], and all relevant counterstrategies to these new policies are placed under triple-loop learning in the above framework.

7. Theoretical and Practical Contributions

The study has multiple contributions for scholars: (1) Research studies have given recommendations to avoid cybersecurity attacks during the COVID-19 crisis [9,13]. However, most of the studies have not used any theoretical framework to support their findings and are conceptual studies. Therefore, this study contributes to the body of knowledge by empirically exploring and mapping the counterstrategies to mitigate cybersecurity issues using the OL theoretical lens; (2) The study not only confirms prior literature by reporting various counterstrategies but also extends current literature by revealing phishing campaigns, video learning materials, and virtual handling skills as significant steps to improve employee education levels, installing secure check applications in mobile devices, reporting the management structural changes, and introducing new organisational policies as key counterstrategies to mitigate cybersecurity issues in HERS amidst the major crisis; (3) Most of the previous studies have not focused on any sector, particularly HERS, to report these challenges [1,4,9]. However, current study findings are exclusively from HERS in Australia during and post major crises; and (4) Unlike prior research studies, the study has taken cybersecurity experts' and top managers' perspectives to report the findings. Thus, this current study adds to the literature by empirically investigating counterstrategies to mitigate cybersecurity challenges amidst major crises in HERS.

This research also makes practical proposals by revealing counterstrategies that were adopted and implemented in HERS during and post major crises. Although the findings of this study are limited to HERS in Australia, the results can be used around the globe by experts working in HERS. The model proposed outlines counterstrategies to cybersecurity challenges amidst a major crisis. This model can make HERS more efficient in mitigating cybersecurity issues in future crises. The counterstrategies can also be tested, adopted, and implemented by practitioners working in other sectors to mitigate cybersecurity issues during and after major crises. Overall, this paper presents important contributions to the literature by revealing counterstrategies using single-loop, double-loop, and triple-loop classification being practiced in HERS in Australia to mitigate cybersecurity challenges.

8. Conclusions

Unlike earlier research studies on revealing strategies to mitigate cybersecurity challenges using conceptual theoretical literature, the research paper has explored various counterstrategies by interviewing cybersecurity experts and top managers working in HERS during and after the major crisis. The counterstrategies highlighted in our findings based on single-loop learning are improving employee learning abilities, improving organisational security, and monitoring and evaluating current security practices. Data analysis found that strategic integration of software, partnerships with other companies through strategic thinking, and using strategic learning to change the existing organisational structures are all counterstrategies studied under the double-loop learning definition in the literature. Finally, introducing new policies and procedures is also reported as a significant counterstrategy, and this dimension is directly related to triple-loop learning. The result of this research paper offers valuable insights into counterstrategies literature to ensure a secure working environment for both scholars and practitioners during and after a major crisis.

During the exploration of counterstrategies to various cybersecurity challenges amidst the major crisis in HERS, some challenges were faced. Some of the CSOs and other cybersecurity experts were hesitant to reveal and explain counterstrategies in response to specific cybersecurity incidents in the interviews. Participants were cautious about revealing a vulnerable cybersecurity incident to be published with their organisation name. In such cases, the challenge was overcome by ensuring that organisation names would not be published anywhere in the research and remain anonymous. Also, another challenge was to gain access to official organisational policies that were changed to mitigate cybersecurity issues. In this scenario, only those details of the policies are explained that were shared and agreed upon by the participants to be published in the research paper.

The study has a few limitations, which can serve as future research directions. Firstly, the study unit of analysis is the cybersecurity experts and top managers. Future research studies can empirically explore these counterstrategies using other units of analysis, for example, students, administrators, and other stakeholders. Secondly, the study has solely explored counterstrategies in response to cybersecurity challenges amidst major crises. Future research studies can consider other organisational challenges faced during and after the major crisis and explore relevant counterstrategies. Thirdly, the study has only considered one major sector, which is HERS; however, future studies can replicate the study in other sectors, including health, sports, textile, etc. As the ACSC report [6] highlights, other sectors were also vulnerable to these challenges amidst a major crisis. Moreover, the study is conducted in Australia HERS. Future studies can consider and replicate the study in other geographical areas. Lastly, future researchers can focus on addressing the shortcomings and limitations of the proposed learning framework adopted by HERS.

Author Contributions: Data curation, S.M.; formal analysis, S.M.; investigation, S.M. and S.F.; methodology, S.M. and M.C.; resources, M.C. and S.F.; validation, M.C.; writing—original draft, S.M.; writing—review and editing, M.C. and S.F. All authors will be informed about each step of manuscript processing including submission, revision, revision reminder, etc., via emails from our system or assigned Assistant Editor. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Australian National Statement on Ethical Conduct in Human Research 2007 and approved by the Human Research Ethics Committee (HREC), Federation University Australia.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: All the relevant data have been included in this article. Additional information can be provided on request.

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

Abbreviations

Abbreviation	Full Form
ACSC	Australian Cybersecurity Centre
HERS	Higher Education and Research Sector
HEIs	Higher Education Institutions
MFA	Multi-Factor Authentication
OL	Organisational Learning
ISO	International Standards Organization
DoS	Denial of Service
DDoS	Distributed Denial of Service
CSO	Chief Security Officer
ISM	Information Security Manager

References

1. Pranggono, B.; Arabo, A. COVID-19 pandemic cybersecurity issues. *Internet Technol. Lett.* **2021**, *4*, e247. [CrossRef]
2. Eian, I.C.; Yong, L.K.; Li, M.Y.X.; Qi, Y.H.; Fatima, Z. Cyber attacks in the era of COVID-19 and possible solution domains. *Preprints* **2020**, 2020090630. [CrossRef]
3. Aljohani, H. Cyber security threats during the pandemic. *J. Contemp. Sci. Res.* **2020**, *5*. Available online: http://www.jcsronline.com/wp-content/uploads/2021/05/Volume5Issue1Paper1.pdf (accessed on 24 July 2023).
4. Khan, N.A.; Brohi, S.N.; Zaman, N. Ten deadly cyber security threats amid COVID-19 pandemic. *TechRxiv* **2020**. [CrossRef]
5. Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education. *Comput. Secur.* **2019**, *86*, 350–357. [CrossRef]
6. ACSC. *ACSC Annual Cyber Threat Report July 2019 to June 2020*; ACSC: Canberra, Australia, 2020.
7. UNESCO. Higher Education Sector (for R&D Data). Available online: https://uis.unesco.org/en/glossary-term/higher-education-sector-rd-data (accessed on 24 July 2023).
8. Ahmad, A.; Desouza, K.C.; Maynard, S.B.; Naseer, H.; Baskerville, R.L. How integration of cyber security management and incident response enables organizational learning. *J. Assoc. Inf. Sci. Technol.* **2020**, *71*, 939–953. [CrossRef]
9. Himdi, T.; Ishaque, M.; Ahmed, J. Cybersecurity challenges during pandemic in smart cities. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021; pp. 445–449.
10. Okereafor, K.; Manny, P. Understanding cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic. *Int. J. IT Eng.* **2020**, *8*. [CrossRef]
11. Williams, C.M.; Chaturvedi, R.; Chakravarthy, K. Cybersecurity risks in a pandemic. *J. Med. Internet Res.* **2020**, *22*, e23692. [CrossRef] [PubMed]
12. Ramadan, R.A.; Aboshosha, B.W.; Alshudukhi, J.S.; Alzahrani, A.J.; El-Sayed, A.; Dessouky, M.M. Cybersecurity and Countermeasures at the Time of Pandemic. *J. Adv. Transp.* **2021**, *2021*, 6627264. [CrossRef]

13. Saleous, H.; Ismail, M.; AlDaajeh, S.H.; Madathil, N.; Alrabaee, S.; Choo, K.-K.R.; Al-Qirim, N. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digit. Commun. Netw.* **2023**, *9*, 211–222. [CrossRef] [PubMed]
14. Raju, R.; Abd Rahman, N.H.; Ahmad, A. Cyber Security Awareness in Using Digital Platforms among Students in a Higher Learning Institution. *Asian J. Univ. Educ.* **2022**, *18*, 756–766.
15. Lourenço, J.; Morais, J.C.; Sá, S.; Neves, N.; Figueiredo, F.; Santos, M.C. Cybersecurity Concerns Under COVID-19: Representations on Increasing Digital Literacy in Higher Education. In *Perspectives and Trends in Education and Technology: Selected Papers from ICITED 2022*; Springer: Cham, Switzerland, 2023; pp. 739–748.
16. Karjalainen, M.; Kokkonen, T.; Taari, N. Key elements of on-line cyber security exercise and survey of learning during the on-line cyber security exercise. In *Cyber Security: Critical Infrastructure Protection*; Springer: Cham, Switzerland, 2022; pp. 43–57.
17. Patterson, C.M.; Nurse, J.R.; Franqueira, V.N. Learning from cyber security incidents: A systematic review and future research agenda. *Comput. Secur.* **2023**, *132*, 103309. [CrossRef]
18. Salimath, M.S.; Philip, J. Cyber management and value creation: An organisational learning-based approach. *Knowl. Manag. Res. Pract.* **2020**, *18*, 474–487. [CrossRef]
19. Shedden, P.; Ahmad, A.; Ruighaver, A. Organisational learning and incident response: Promoting effective learning through the incident response process. In Proceedings of the 8th Australian Information Security Mangement Conference, Perth, Australia, 30 November 2010.
20. Argyris, C.; Schön, D.A. *Organizational Learning: A Theory of Action Perspective*; 77/78; Centro de Investigaciones Sociológicas: Madrid, Spain, 1997; pp. 345–348.
21. Schön, D.; Argyris, C. *Organizational Learning II: Theory, Method and Practice*; Addison Wesley: Reading, MA, USA, 1996; 305p.
22. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]
23. Oxford University Press. Oxford Online Dictionary. Available online: http://www.oxforddictionaries.com/definition/english/Cybersecurity (accessed on 24 July 2023).
24. Abrahamsson, P.; Salo, O.; Ronkainen, J.; Warsta, J. Agile software development methods: Review and analysis. *arXiv* **2017**, arXiv:1709.08439.
25. He, Y.; Aliyu, A.; Evans, M.; Luo, C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *J. Med. Internet Res.* **2021**, *23*, e21747.
26. Chadhar, M.A.; Daneshgar, F. Organizational Learning and ERP Post-implementation Phase: A Situated Learning Perspective. *J. Inf. Technol. Theory Appl.* **2018**, *19*, 7.
27. Edmondson, A.C.; Kramer, R.M.; Cook, K.S. Psychological safety, trust, and learning in organizations: A group-level lens. In *Trust and Distrust in Organizations: Dilemmas and Approaches*; Russell Sage Foundation: Manhattan, NY, USA, 2004; Volume 12, pp. 239–272.
28. Friedman, V.J.; Antal, A.B. Negotiating reality: A theory of action approach to intercultural competence. *Manag. Learn.* **2005**, *36*, 69–86. [CrossRef]
29. Pentland, B.T.; Feldman, M.S. Organizational routines as a unit of analysis. *Ind. Corp. Chang.* **2005**, *14*, 793–815. [CrossRef]
30. Shrivastava, P. A typology of organizational learning systems. *J. Manag. Stud.* **1983**, *20*, 7–28. [CrossRef]
31. Snell, R.; Chak, A.M.-K. The learning organization: Learning and empowerment for whom? *Manag. Learn.* **1998**, *29*, 337–364. [CrossRef]
32. Cecez-Kecmanovic, D.; Janson, M.; Zupancic, J. Relationship between Information Systems and Organisational Learning-Lessons from the Field. *ACIS 2006 Proc.* **2006**, *58*.
33. He, Y.; Zamani, E.D.; Lloyd, S.; Luo, C. Agile incident response (AIR): Improving the incident response process in healthcare. *Int. J. Inf. Manag.* **2022**, *62*, 102435. [CrossRef]
34. Evans, M.; He, Y.; Maglaras, L.; Janicke, H. HEART-IS: A novel technique for evaluating human error-related information security incidents. *Comput. Secur.* **2019**, *80*, 74–89. [CrossRef]
35. He, Y.; Johnson, C. Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Inform. Health Soc. Care* **2017**, *42*, 393–408. [CrossRef] [PubMed]
36. Ahmad, A.; Hadgkiss, J.; Ruighaver, A.B. Incident response teams–Challenges in supporting the organisational security function. *Comput. Secur.* **2012**, *31*, 643–652. [CrossRef]
37. Ahmad, A.; Maynard, S.B.; Shanks, G. A case analysis of information systems and security incident responses. *Int. J. Inf. Manag.* **2015**, *35*, 717–723. [CrossRef]
38. Jaatun, M.G.; Albrechtsen, E.; Line, M.B.; Tøndel, I.A.; Longva, O.H. A framework for incident response management in the petroleum industry. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 26–37. [CrossRef]
39. Tick, A.; Cranfield, D.J.; Venter, I.M.; Renaud, K.V.; Blignaut, R.J. Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. *Electronics* **2021**, *10*, 2865. [CrossRef]
40. Alexei, L.A.; Alexei, A. Cyber security threat analysis in higher education institutions as a result of distance learning. *Int. J. Sci. Technol. Res.* **2021**, *10*, 128–133.
41. Anderson, J.; Poole, M. *Assignment and Thesis Writing*; Juta and Company Ltd.: Claremont, CA, USA, 2009.
42. Maleh, Y. *Security and Privacy Management, Techniques, and Protocols*; IGI Global: Hershey, PA, USA, 2018.
43. De Bruijn, H.; Janssen, M. Building cybersecurity awareness: The need for evidence-based framing strategies. *Gov. Inf. Q.* **2017**, *34*, 1–7. [CrossRef]

44. Tagarev, T.; Sharkov, G.; Stoianov, N. Cyber security and resilience of modern societies: A research management architecture. *Inf. Secur.* **2017**, *38*, 93–108. [CrossRef]
45. Alvesson, M. Beyond neopositivists, romantics, and localists: A reflexive approach to interviews in organizational research. *Acad. Manag. Rev.* **2003**, *28*, 13–33. [CrossRef]
46. Denzin, N.K. *Collecting and Interpreting Qualitative Materials*; Sage: Thousand Oaks, CA, USA, 2008; Volume 3.
47. Strauss, A.; Corbin, J. *Basics of Qualitative Research*; Sage Publication: Thousand Oaks, CA, USA, 1990.
48. Ahmad, T. Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *SSRN Electron. J.* **2020**. [CrossRef]
49. Hoepfl, M.C. Choosing qualitative research: A primer for technology education researchers. *J. Techonl. Educ.* **1997**, *9*, 47–63. [CrossRef]
50. Patton, M. *Qualitative Research and Evaluation Methods*, 3rd ed.; Sage: Thousand Oaks, CA, USA, 2002.
51. Bogdan, R.; Biklen, S.K. *Qualitative Research for Education*; Allyn & Bacon: Boston, MA, USA, 1997.
52. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
53. Noy, C. Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *Int. J. Soc. Res. Methodol.* **2008**, *11*, 327–344. [CrossRef]
54. Stumpf, T.; Califf, C. On the use of meta-theory in grounded investigations: In principle and practice in hospitality and tourism research. In *Handbook of Research Methods in Tourism and Hospitality Management*; Edward Elgar: Northhampton, UK, 2018; pp. 123–135.
55. Ezzy, D. *Qualitative Analysis*; Routledge: London, UK, 2013.
56. Walsham, G. Interpretive case studies in IS research: Nature and method. *Eur. J. Inf. Syst.* **1995**, *4*, 74–81. [CrossRef]
57. Hijji, M.; Alam, G. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors* **2022**, *22*, 8663. [CrossRef] [PubMed]
58. Abroshan, H.; Devos, J.; Poels, G.; Laermans, E. COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access* **2021**, *9*, 121916–121929. [CrossRef]
59. Adil, M.; Khan, M.K. Emerging iot applications in sustainable smart cities for COVID-19: Network security and data preservation challenges with future directions. *Sustain. Cities Soc.* **2021**, *75*, 103311. [CrossRef] [PubMed]
60. Cheng, E.C.; Wang, T. Institutional strategies for cybersecurity in higher education institutions. *Information* **2022**, *13*, 192. [CrossRef]
61. Wong, L.-W.; Lee, V.-H.; Tan, G.W.-H.; Ooi, K.-B.; Sohal, A. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *Int. J. Inf. Manag.* **2022**, *66*, 102520. [CrossRef]
62. Hui, S.C.; Kwok, M.Y.; Kong, E.W.; Chiu, D.K. Information security and technical issues of cloud storage services: A qualitative study on university students in Hong Kong. *Libr. Hi Tech* **2023**. *ahead of print*. [CrossRef]
63. Khatri, S.; Cherukuri, A.K.; Kamalov, F. Global Pandemics Influence on Cyber Security and Cyber Crimes. *arXiv* **2023**, arXiv:2302.12462.
64. Zhang, Q.; Zhou, C.; Xiong, N.; Qin, Y.; Li, X.; Huang, S. Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2015**, *46*, 1429–1444. [CrossRef]
65. Ulven, J.B.; Wangen, G. A systematic review of cybersecurity risks in higher education. *Future Internet* **2021**, *13*, 39. [CrossRef]
66. Abukari, A.M.; Bankas, E.K. Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *Int. J. Sci. Eng. Res.* **2020**, *11*, 1401–1407.
67. Garba, A.A.; Bade, A.M. An investigation on recent cyber security frameworks as guidelines for organizations adoption. *Int. J. Innov. Sci. Res. Technol.* **2021**, *6*, 103–110.
68. Kumar, S.; Biswas, B.; Bhatia, M.S.; Dora, M. Antecedents for enhanced level of cyber-security in organisations. *J. Enterp. Inf. Manag.* **2021**, *34*, 1597–1629. [CrossRef]
69. Najm, Y.; Alsamaraee, S.; Jalal, A.A. Cloud computing security for e-learning during COVID-19 pandemic. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *27*, 1610–1618. [CrossRef]
70. Beaman, C.; Barkworth, A.; Akande, T.D.; Hakak, S.; Khan, M.K. Ransomware: Recent advances, analysis, challenges and future research directions. *Comput. Secur.* **2021**, *111*, 102490. [CrossRef]
71. Alghamdi, A. Cybersecurity threats to Healthcare Sectors during COVID-19. In Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 25–27 January 2022; pp. 87–92.
72. Goniewicz, K.; Khorram-Manesh, A.; Hertelendy, A.J.; Goniewicz, M.; Naylor, K.; Burkle, F.M., Jr. Current response and management decisions of the European Union to the COVID-19 outbreak: A review. *Sustainability* **2020**, *12*, 3838. [CrossRef]
73. Mimecast. *The State of Email Security Report*; CrowdStrike: Austin, TX, USA, 2020.
74. Aljumah, Y.; Ahmed, S.S. A novel approach to get awareness in Saudi Arabia regarding phishing attacks. In Proceedings of the 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia, 12–13 June 2021; pp. 1–5.
75. Eltahir, M.; Ahmed, O. Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan. *Inf. Sci. Lett.* **2023**, *12*, 13.

76. Nour, B.; Pourzandi, M.; Debbabi, M. A Survey on Threat Hunting in Enterprise Networks. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 2299–2324. [CrossRef]
77. Pokojski, Z.; Kister, A.; Lipowski, M. Remote work efficiency from the employers' perspective—What's next? *Sustainability* **2022**, *14*, 4220. [CrossRef]
78. Einler Larsson, L.; Qollakaj, K. Cybersecurity of Remote Work Migration: A Study on the VPN Security Landscape Post COVID-19 Outbreak. 2023. Available online: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1778036&dswid=-6273 (accessed on 15 December 2023).
79. Perwej, Y.; Abbas, S.Q.; Dixit, J.P.; Akhtar, N.; Jaiswal, A.K. A systematic literature review on the cyber security. *Int. J. Sci. Res. Manag.* **2021**, *9*, 669–710. [CrossRef]
80. Pavlova, E. Enhancing the organisational culture related to cyber security during the university digital transformation. *Inf. Secur.* **2020**, *46*, 239–249. [CrossRef]
81. Trumbach, C.C.; Payne, D.M.; Walsh, K. Cybersecurity in business education: The 'how to'in incorporating education into practice. *Ind. High. Educ.* **2023**, *37*, 35–45. [CrossRef]
82. Al Shammari, A.; Maiti, R.R.; Hammer, B. Organizational security policy and management during COVID-19. In Proceedings of the SoutheastCon 2021, Virtual, 10–13 March 2021; pp. 1–4.
83. Fouad, N.S. Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. *J. Cyber Policy* **2021**, *6*, 137–154. [CrossRef]
84. Ghavifekr, S.; Fung, H.Y. Change management in digital environment amid the COVID-19 pandemic: A scenario from Malaysian higher education institutions. In *Pandemic, Lockdown, and Digital Transformation: Challenges and Opportunities for Public Administration, NGOs, and Businesses*; Springer: Cham, Switzerland, 2021; pp. 129–158.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.