information

*Article*

# Institutional Strategies for Cybersecurity in Higher Education Institutions

**Eric C. K. Cheng * and Tianchong Wang ***

Department of Curriculum and Instruction, Faculty of Education and Human Development, The Education University of Hong Kong, Hong Kong, China
* Correspondence: eckcheng@eduhk.hk (E.C.K.C.); twang@eduhk.hk (T.W.)

**Abstract:** Cybersecurity threats have grown exponentially, posing a heavy burden on organisations. Higher Education Institutions (HEIs) are particularly vulnerable, and their cybersecurity issues are receiving greater attention. However, existing research on cybersecurity has limited referencing value for HEI leaders and policy-makers because they are usually technology-focused. Publications that showcase best practices often lack system-wide perspectives towards cybersecurity in HEIs. Our paper, therefore, aims to bridge this literature gap and generate institutional cybersecurity strategies for HEI leaders and policy-makers from a system perspective. We first review how the cybersecurity landscape has evolved over the last few decades and its latest trends and projections for the next decade. By analysing these historical developments and new changes, we further illuminate the importance of strengthening HEI cybersecurity capacities. As we explore why HEIs face severe challenges to tackle the ever-escalating cyberattacks, we propose a system-wide approach to safeguard HEI cybersecurity and highlight the necessity to reassess prioritised areas. By taking an extensive literature review and desk research of methods that could respond to the cybersecurity vulnerabilities of the next decade, we synthesise our findings with a set of institutional strategies, with takeaways designed to equip HEIs better to address cybersecurity threats into the future. The strategies include: (1) Strengthening Institutional Governance for Cybersecurity; (2) Revisiting Cybersecurity KPIs; (3) Explicating Cybersecurity Policies, Guidelines and Mechanisms; (4) Training and Cybersecurity Awareness Campaigns to Build Cybersecurity Culture; (5) Responding to AI-based Cyber-threats and Harnessing AI to Enhance Cybersecurity; (6) Introduction of New and More Sophisticated Security Measures; (7) Paying Attention to Mobile Devices Use, Using Encryption as a Daily Practice; and (8) Risk Management. We believe that cybersecurity can be safeguarded throughout the new decade when these strategies are considered thoroughly and with the concerted effort of relevant HEI stakeholders.

**Keywords:** cybersecurity; cyber threats; management strategies; KPI; higher education



**Citation:** Cheng, E.C.K.; Wang, T. Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information* **2022**, *13*, 192. https://doi.org/10.3390/info13040192

Academic Editor: Sherali Zeadally

Received: 7 March 2022
Accepted: 8 April 2022
Published: 12 April 2022



## 1. Introduction

With new developments in technologies such as artificial intelligence (AI) and the Internet of Things (IoT), cybersecurity threats have increased exponentially in recent years. The constant and rapid change in means and ends of cybersecurity threats have posed a heavy burden on organisations. While virtually every major industry faces cybersecurity challenges, the higher education sector is particularly vulnerable [1].

There are several reasons behind the security vulnerabilities of higher education. Firstly, risks posed by cyberattacks extend beyond financial losses for the world of higher education. Indeed, higher education institutions (HEIs) house a vast volume of sensitive information, such as student personal records, sensitive research data, and valuable intellectual properties [2,3]. Information loss or compromise could pose a grave threat to the individuals involved and cause significant damage to a university's reputation [1]. Secondly, HEIs are often the home of critical infrastructure and user-intensive systems (e.g.,

Internet exchange point of backbone network) that a nation or a city needs to be depending on; any cybersecurity incidents could be disastrous. Thirdly, compared to business corporations, IT systems of many HEIs are often characterised by a decentralised structure—it makes sense from an operational perspective for individual faculties/departments to operate under their own IT structures due to their varied technological needs. However, this kind of piecemeal setup creates apparent security vulnerabilities that attackers can exploit. Fourthly, academia's unique culture, which prides itself on a degree of openness and transparency that most industries lack, also presents security vulnerabilities. HEIs have historically been designed to be accessible to the public, and such accessibility would also mean that their networks are as open as their campuses [4]. Finally, since the dramatic shift to remote working and online learning in 2020 due to the COVID-19 pandemic, more non-university-provided personal devices are connecting to the HEI's network and IT systems, and the stakes of cyber security have become an all-time high [5].

Because of these vulnerabilities, HEI cybersecurity is receiving greater attention. The inauguration of a new Information Security issue of Horizon Report in 2021 [6] is an example of such heightened attention. Meanwhile, as HEIs continue to invest in the talent and infrastructure needed to meet cybersecurity challenges going forward, institutional leaders and policy-makers beg for institutional strategies to prioritise their resources and efforts in order to tackle the pain point. Unfortunately, much existing research on cybersecurity has limited referencing value for institutional leaders and policy-makers because they are usually technology-focused. Publications that showcase best practices often lack system-wide perspectives towards cybersecurity in HEIs. Our paper, therefore, aims to bridge this literature gap, explore institutional strategies for cybersecurity in HEIs from the system perspective, and provide handy takeaways as HEI leaders and policy-makers work towards these strategies.

This paper first reviews how the cybersecurity landscape has evolved over the last few decades and its latest trends and projections for the next decade. By understanding these historical developments and new changes, we further illuminate the importance of revisiting HEI cybersecurity issues. As we explore why HEIs face severe challenges to tackle the ever-escalating cyberattacks, we propose a system-wide approach to safeguard HEI cybersecurity and highlight the necessity to reassess prioritised areas. By taking an extensive literature review and desk research [7] of methods that could respond to the cybersecurity vulnerabilities of the next decade, we synthesise our findings with a set of institutional strategies with takeaways designed to equip HEIs better to address cybersecurity threats into the future.

## 2. An Overview of Cyberattacks in the Past Decades

In the 1960s, security was primarily concerned with safeguarding entity assets; organisations relied on physical measures such as passwords, multi-layered protection, and existing fire system [8]. Cybersecurity issues first gained attention in the 1970s, with companies shifting their computers from centralised mainframes to decentralised, end-user-based systems [9]. As more software applications were developed on microcomputers, these small form factor systems became the targets for security attacks. Programmes that can detect and remove threats were made as a response. Originally designed as a security test to see if a self-replicating program was possible [10], Creeper was regarded as the first known computer virus that could move about in the ARPANET (The Advanced Research Projects Agency Network, the precursor to the Internet). Reaper was subsequently made to move across the ARPANET and the self-replicating Creeper was deleted. The conflict between the two programmes exposed the network vulnerability of ARPANET and raised the issue of network security [11]. Although the Creeper virus was not destructive, many new and more dangerous cybersecurity vectors quickly followed. Along with the Internet becoming available to the public in the late 1980s, how computer worms distributed via the Internet could cause damage gained mainstream media attention for the first time. In 1988, a graduate student at Cornell University became the first person convicted under the

Computer Fraud and Misuse Act of the United States for spreading the Morris worm and causing damage to computers [12].

With the growth of interconnections via the Internet, the number of cyberattacks increased significantly, and the form of attack changed. Before the Internet, viruses spread on PCs by infecting executable programmes or the boot sectors of floppy disks. The blossoming of the Internet in the late 1990s made it possible for self-reproducing programmes to actively transmit themselves over the network, infect other computers, and self-replicate without infecting files. Malware (Malware refers to harmful software that disrupts or manipulates a digital device's normal operation) emerged, and there was an increased number of organised crimes committed through the web. Firewall and real-time protection antivirus programmes were developed in response [9]. The growth of web applications also created new opportunities for cybercriminals. Cyber threats such as spyware, spam, phishing (phishing is a method of identity theft that relies on individuals unwittingly volunteering personal details or information that can be then be used for nefarious purposes. It is often carried out through the creation of a fraudulent website, email, or text appearing to represent a legitimate firm), website defacement (website defacements are the unauthorised modification of web pages, including the addition, removal, or alteration of existing content) and Denial-of-Serve (DoS) (a DoS attack is an attempt to make a service, usually a website, unavailable by bombarding it with high traffic from multiple machines so that the server providing the service is no longer able to function correctly) further took advantage of the WWW. Because organisations lacked barriers in their networks and systems and were vulnerable to attacks, risk analysis and threats and vulnerability, detection methods began to develop [13].

The new millennium has seen more legislation introduced relating to computer crime sentencing details as well as guides for enhanced penalties. With this legislation, proper punishments could be given to those who commit hacking and cybercrime, and those who carry out serious hacking activities now face more severe sentences. In the 2010s, social media such as Facebook and Twitter became a new vector for cyber-attacks [14]. Meanwhile, hacking evolved into more complicated forms, often resulting in massive data breaches. Some high-profile data breach incidents followed. In 2013, Snowden used compromised credentials to retrieve classified documents from the National Security Agency (NSA, Fort Meade, MD, USA), many of which he could not access at his security clearance level [15]. In the same year, 3 billion Yahoo user accounts and personal data was compromised, which caused a 350-million drop in the company's sale price [16]. Among these cases, some of the cybersecurity vulnerabilities identified were malware, phishing, SQL injection attack, cross-site scripting (XSS), DoS, session hijacking, man-in-the-middle attacks and credential reuse. DoS was most used towards the exploitable weak spot, followed by malware and phishing [17]. As a type of cyberattack in which an unauthorised user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons [18], cyber espionage became one of the top threats in 2014 [19]. New cybersecurity technologies and attack mitigation options, such as DoS protection, network behavioural analysis, and web application firewalls, were developed. Cyber threats, meanwhile, were also shifting their motive and means. More powerful and new forms of malware, such as ransomware used by cybercriminals to extort money, also appeared. For example, the WannaCry ransomware infected 23,000 companies across 150 countries in 2017—user's files were held hostage, and a Bitcoin ransom was demanded for their return [20]. Cryptojacking, a threat that embeds itself within a computer or mobile device and then uses its resources to mine cryptocurrency, first appeared as a top threat in 2018 [19]. Unlike other types of malware, cryptojacking scripts do not damage computers' or victims' data. However, they do steal computer processing resources. With the crackdowns by law enforcement and the closing down of the Coinhive service, which can be used for malicious cryptomining, cryptojacking declined in 2020 [21].

## 3. Potential Cybersecurity Risks in the New Decade

As Industry 4.0 unfolds, cybersecurity risks have reached a new height [13]. For example, the World Economic Forum [22] recorded that malware and ransomware attacks increased by 358% and 435%, respectively, in 2020 and the threats are outpacing societies' ability to prevent or respond to them effectively. "Lower barriers to entry for cyberthreat actors, more aggressive attack methods, a dearth of cybersecurity professionals and patchwork governance mechanisms are all aggravating the risk" [22].

Like in previous decades, these challenges reflect several changes and the new development of technologies. They are related to cloud computing, mobile technologies, AI, and the IoT. Privacy issues of the systems also present more-significant-than-ever concerns.

Partially because of their easy management and low costs [23], a growing number of institutions and organisations are migrating their systems and infrastructure to the cloud, shifting the hosting to Cloud Service Providers (CSO) such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. Although the cloud service provider usually takes on more responsibility for ensuring that the hosting is well-protected, security could still be compromised, especially when it comes to data safety [24]. Cybercriminals use social engineering techniques such as phishing, spoofing websites, and social media spying to steal users' login credentials and subsequently gain unauthorised access to the critical information stored in the cloud network [25]. A data breach could occur without users even realising that their accounts are being hijacked.

In recent years, the rapid advancement of AI technologies has expanded the threat landscape and fuelled the attack capabilities [26], taking the cybersecurity battle to the next level. Research [19] expected that data analytics would not only mitigate threats but develop attacks. For example, Cybercriminals can use AI, often featuring automation and self-learning, and can make it difficult to detect, scope and identify vulnerable applications, devices, and networks to scale their attacks. Cybercriminals can also employ AI to assist with the scale and effectiveness of their social engineering attacks; AI can learn to spot patterns in behaviour, adapt itself for more effective phishing approaches, and subsequently trick users into handing over sensitive data. AI-powered malware, particularly "Ransomware as a Service" (RaaS), allows even non-technical criminals to execute attacks [27]. The growing penetration of AIs also makes them the targets of cyberattacks. AI-powered systems present specific features that can be attacked in non-traditional ways. For example, attackers can manipulate the datasets used to poison AI, making subtle changes to parameters or crafting carefully designed scenarios to avoid raising suspicion while gradually steering AI in their desired direction. By modifying input data to make proper identification difficult, AI systems can be manipulated into bias and misclassification, leading to severe consequences in decision-making.

Kaloudi and Li [26] classify AI-based attacks into five categories: next-generation malware, voice synthesis, password-based attacks, social bots, and adversarial training. Kahn [28] identified ten potential cyber threats in the future, most of which are AI-fuelled. These include malicious chips that are used to hack hardware; crypto-jacking that continues to grow with cryptocurrencies; data poisoning via machine learning and AI that expand companies' potential attack surface; compromised data; authentication attacks and evolving authentication techniques which open up another arena susceptible to attack or exploitation; more powerful malware such as ransomware, crypto-jacking, destructive malware that will continue to increase alongside the connectivity of devices and networks; a skills shortage (there is a shortage of security professionals); a false sense of security that comes from an overreliance on AI-powered security tools; cyber weapons that could cause serious economic impact; and compliance, which may distract security professionals from all the pressing security matters.

As mobile devices such as smartphones and tablets break into the mainstream, Abomhara and Koien [29] have projected that the battleground of cyberattacks in the future would switch from conventional computers to these always-connected, personal platforms. The cyberattacks on mobile devices are often subtle and tend to go unnoticed. For example,

users download Apps that look legitimate but skim data from their device. Forms of attack could also include fake public Wi-Fi networks and text message phishing scams. With the increasing use of mobile devices for sensitive businesses such as banking, their security issues are becoming more critical.

The scope of cyberattacks in the coming decade can also extend to IoT devices. Starting with the simple goal of connecting any standalone device to the Internet and thereby converting it to a smart device, the IoT is the next wave of technology that will significantly impact social life and empower the business environment. Unfortunately, IoTs are even more vulnerable to cyberattacks due to a combination of their multiple attack surfaces, real-time data collection, privacy issues, and lack of security standardisations and requirements [30]. In some extreme cases, attackers can hijack the IoT devices and find malicious ways to interfere with the operations of an organisation, and IoT drones can compromise privacy and potentially be used as weapons [31]. In response to these threats, some new and novel methods for IoT cyberattack detection are being proposed by computer scientists (e.g., [32,33]).

## 4. Managing Cybersecurity in HEIs: A Call for Change

A fundamental transformation underlying, and responsible for, many of the changing practices has been the movement toward the "corporatisation" of higher education—a rationale that, by adopting the structure and practices of the corporate world, higher education will be better able to meet its current challenges [34,35]. Since the inception of "corporatisation" in the early 2000s, Key Performance Indicators (KPIs) have been introduced in many HEIs to monitor and assess institutional performance towards accountability [36].

For cybersecurity, KPIs measure the probability and the potential consequences of identified risk, gauge the effectiveness of the security operations, the adequacy of security control, and indicate where to focus limited resources. The basic assumption of developing cybersecurity KPIs is that KPIs can help pinpoint risks [37]. The organisations can conduct a security risk assessment to identify their assets, evaluate their value, and classify them to determine the potential loss and probability of occurrence.

Aven [38] identified three types of security KPIs commonly applied in organisations. The first one is the technical security KPI, which is used to diagnose problems and measure technical security activities. The second type is security program KPIs used to measure overall program effectiveness such as risk management, policy compliance, employee training and identity management. The third is a security scorecard that applies technical and programme metrics to build a balance security scorecard.

While the existing KPIs might have worked in the past, it seems that the measures are gradually losing their validity in evaluating cybersecurity success. Data collected by relevant KPIs may not accurately predict the new cybersecurity issues. As a result, the risk mitigation measures fail to catch up with the drastic changes of the cyber threat landscape. Moreover, outliers of regression models that predict the risk are difficult to conceptualise and explore in detail. Such an outline of cases typically occurs at a low frequency but create high severity and dominate loss events. There are also many implementation challenges in measuring cybersecurity KPIs. For example, stakeholders' unwillingness to share information, a lack of standard definitions for terms and metrics, legal concerns and low participation are roadblocks for gaining reliable data. Without reliable data for estimating cybersecurity incident occurrence likelihood and loss expectancies, the accuracy of KPI results could be questionable [39].

Besides KPI validity issues, other challenges hinder Cybersecurity in HEIs as well. For example, aligned with KPIs, cybersecurity strategies in organisations have been technology-focused and mainly driven by the availability and implementation of specific infrastructure, hardware, software, and web systems [40]. When security incidents occur, responsibilities are often not clear and many of the recent indents caused by human factors (e.g., unconscious wrong practice and noncompliance with policy), rather than not having protecting technology in place [41–43]—a situation that is consistent with the findings drawn by the

World Economic Forum that 95% of cybersecurity incidents occurred in 2020 can be traced to human factors [22]. Moreover, organisations rely on best practice standards as a guidance rather than dynamic risk assessments for strategic planning. Since best practices are supported by contextualised organisation factors that may not exist in other organisations, KPIs derived by best practices cannot focus on the context and needs of the organisations.

Because of all these issues and challenges and the reality that cybersecurity risk development outpaces HEI cyber-resilience, there has been a call for change in managing cybersecurity in HEIs.

## 5. Strategies for Addressing the Challenges of Cybersecurity in HEIs: A System-Wide Approach

While there is no single formula nor silver bullet for cybersecurity, there are strategies that may help HEIs address cybersecurity challenges in a sustainable manner. Moving from a technology-centric mentality, we propose a system-wide approach to safeguard HEI cybersecurity. By taking an extensive review and desk research [7] of the literature and promising practices that could respond to the changing landscape of cybersecurity, we synthesise our findings with a set of institutional strategy recommendations designed to equip HEIs better in order to address cybersecurity threats into the future.

### *5.1. Strengthening Institutional Governance for Cybersecurity*

As "the leadership, organisational structures, and processes involved in the protection of informational assets" [44], a governance approach to organisational cybersecurity has been recommended by some researchers. This approach calls for bringing cybersecurity to the attention of senior management [45]. Besides senior management involvement [46], the leadership's will and attitudinal commitment are equally crucial [47]. Additionally, leadership needs to recognise that, while cybersecurity is an integral component of IT governance [48,49], it should no longer be solely the responsibility of IT departments but the focus of institution-wide efforts [50]. As digital technologies are strategically aligned with business strategy, the same should be done with cybersecurity [50].

The establishment of a new institutional structure and the checks and balances could effectively strengthen institution governance for cybersecurity [51]. Reporting to the Provost/Vice-President, a steering committee that consists of senior management members, the Chief Information Officer, and departmental representatives has the leadership responsibility to provide oversight of all cybersecurity-concerned initiatives in HEIs. Through this committee, strategic plans for preventing, detecting, and remediating cybersecurity issues could be developed [52]. KPIs aligned with the strategic plans could also be developed for monitoring and holding accountability purposes.

### *5.2. Revisiting Cybersecurity KPIs*

Decisions about how best to reduce cybersecurity risks can be contentious, and HEI leaders have to decide which efforts they should prioritise. KPIs are commonly used to measure business strategies' effectiveness and drive business operations. Unfortunately, KPIs used in HEIs are gradually losing their validity in this function. Cybersecurity KPIs must be revisited to help HEI leaders gain accurate cybersecurity performance reporting and make meaningful strategic decisions.

A central step in building valid KPIs is understanding the key factors or domain areas of cybersecurity involved. Recent research such as Diesch, Pfaff, and Krcmar [53] suggests that organisations consider a set of factors, including physical security, vulnerability, access control, infrastructure, and awareness of cyber risk, to formulate their cybersecurity KPIs. Similarly, the National Institute of Standards and Technology [54] of the United States listed key domain areas in managing cybersecurity risk: identify, protect, detect, respond, and recover. While these factors and domain areas are highly relevant in responding to today's cybersecurity landscape, HEI leaders, in a real sense, should also consider the institutional factors, available resources, security goals, and sustainability in formulating the strategy

and countermeasures—the situation could vary in macro and micro levels between HEIs. In other words, cybersecurity KPIs have to be made more contextually and dynamically.

To determine the appropriate KPIs for individual HEIs, the institutional governing body for cybersecurity, such as the steering committee we recommended, can conduct a landscape review with the latest scholarly literature, organisation report, popular media articles, and relevant websites to gain a comprehensive and up-to-date understanding on cybersecurity matters. Some of the best practices and KPIs from peer HEIs of similar contexts should also be learned. The key insights gained can be categorised and synthesised into a concept matrix for developing institutional KPIs. Precise definitions of each add greatly to an understanding of what is being measured. An explanation of how it is assessed is also vital. The institutional governing body for cybersecurity can examine their institutional relevancy with input from stakeholders. KPIs are subsequently removed from or added to the matrix as a result. Additionally, HEI leaders need to consider how KPIs are collated and reported internally. It may make more sense to report KPIs separately for each department in some instances. Whether the KPIs choose to remain relevant over time should also be regularly reviewed.

### *5.3. Explicating Cybersecurity Policies, Guidelines and Mechanisms*

Policies for cybersecurity are formal high-level statements that embody an organisation's course of action regarding the use and safeguarding of information and digital assets [55]. For HEIs, policy development is the first step to demonstrating their cybersecurity commitment [56]. It also provides institutional leaders with an opportunity to set a clear cybersecurity plan and describe its role in supporting the institution's missions [57].

From the point of view of management, Baskerville and Siponen [55] stressed the separation between "what should be protected" and "how the policy is enforced" (p. 337). To ensure they can be effectively implemented, policies need to be drafted through a consensus-building process with consultation and feedback from all concerned stakeholders. A careful balance must be reached to ensure that the policy enhances institutional security by providing enough detail that staff understand their expected role and contribution. The dialogues between institutional policy-makers and concerned stakeholders would help establish consensus and ease the resistance from those who are not accustomed to heightened attention and tightened security measures [50]. Policy statements, which also clearly communicate the institution's beliefs, goals, and objectives for cyber security, can be formalised and well-documented with these engagements.

Policies are not the only documents that end-users should look to when trying to understand an HEI's information security stance. While policies may state the high-level institutional goals around expected behaviours and outcomes, other documents may be used to display a threshold of personal strategies for security vulnerabilities, acceptable behaviour, good practices to follow, or recommended measures to take [17].

Considering that many cybersecurity risks in the new decade are information-related, mechanisms for protecting information safety and privacy should also be developed [49]. Additionally, policies and guidelines would also require periodic reviewing and updating mechanisms to ensure the stated intent and corresponding expectations are consistent and relevant over time and reflect new changes in technology, laws, common practices, and other factors.

### *5.4. Training and Cybersecurity Awareness Campaigns to Build Cybersecurity Culture*

HEIs need to respond to the fact that human factors are the weakest links in today's cybersecurity landscape [42,43]. Researchers and cybersecurity experts have argued that building a cybersecurity culture is essential to change attitudes, perceptions, and to instill good security behaviours [58,59]. Enabling cybersecurity culture is also critical in supporting the smooth realisation of security-related plans and policies [60].

To foster such a cybersecurity culture, Da Veiga, Astakhova, Botha, and Herselman [58] further highlighted the necessity of regular communication and security education, train-

ing and awareness building. Alshaikh [60] also examined the initiatives of building organisational cybersecurity culture, namely creating a brand for the cybersecurity team, establishing a cybersecurity champion network, building a cybersecurity hub and aligning security awareness with campaigns. His findings suggest that these initiatives had helped organisations exceed minimal standards-compliance to create functional cybersecurity cultures.

Following Alshaikh's [60] practices, it appears that building cybersecurity culture in HEIs could also be achieved by training and cybersecurity awareness campaigns. More specifically, staffs who may handle personal data in an HEI need to receive appropriate awareness training and regular updates to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each staff type/level need to be defined and documented in alignment with the institution's security policy. Staff also need to understand that cybersecurity is a shared responsibility, and doing the right thing must be the norm [58,61]. Promoting organisational cybersecurity awareness may start from the employment phase. All new employees should participate in orientation workshops and be provided with pertinent information, including security policies and procedures and potential disciplinary processes/actions for any security breaches. These workshops must be human-centric for greater content uptake and digestion [62]. Meanwhile, new employees should also be required to sign an acknowledgement indicating that they read and understand the institution's security-related policies, recognise the gravity of information security issues of the institution, and dedicate themselves to safeguarding and responding to cybersecurity according to and beyond their work role. Existing staff should also be required to take training and awareness campaigns on HEI's cybersecurity practices and acknowledge their understanding of its cybersecurity policies and procedures. Instead of one-off events, cyber security education and awareness training should be an ongoing practice. Fostering Communities of Practice (CoP) [63] may deepen the staff members' understanding of cybersecurity and contextualise the promising practices learned. Additionally, having all the training available in an online repository would be helpful for staff to revisit the materials on an as-need basis. Given the constant evolvement of cyber threats, institutions should provide updated cyber security information on a defined schedule and offer just-in-time training as needed.

### *5.5. Responding to AI-Based Cyber-Threats and Harnessing AI to Enhance Cybersecurity*

Given that AI technologies in recent years have expanded the threat landscape and fuelled the attack capabilities [26], HEIs need to equip themselves to respond to AI-based cyber-threats.

Bécue, Praça, and Gama [64] proposed several technological countermeasures to address AI-based cyber-threats. These measures include introducing a Network Intrusion Detection System (NIDS) and a Host Intrusion Detection System (HIDS). As a defence-in-depth protection in addition to a firewall [65], these systems may provide significant improvements in detection performance, support enhanced automation of investigation steps, and enhance the robustness of the algorithms and human/machine behaviour monitoring. Meanwhile, it is important to note that cybersecurity is not just a technical concern but a management issue. Technology management is crucial for preventing AI-based cyber-threats; therefore, organisations should have a good grasp of the technology components and the company and the vulnerability.

Despite facilitating new/enhanced forms of attack [26], AI can also improve cybersecurity practices substantially. For example, Bécue, Praça, and Gama [64] suggest machine learning, a subfield of AI that automates analytical model building, can be applied in intrusion and human-factor risk detection. Similarly, Alhawi, Baldwin, and Dehghantanha [66] also proposed leveraging machine-learning techniques for windows ransomware network traffic detection. Blockchain-based [67], deep-learning-based [68] cyber-attack detections are also explored by researchers. Zhan, Xu, and Xu [69] proposed a cyber-attack prediction method to proactively evaluate security threat levels and help users decide the most

effective defence strategies. With all these possibilities, HEIs are encouraged to harness the power of AI and upgrade their cybersecurity defence capacity. Considering that AI is a double-edged sword, some form of control is still necessary to ensure the deployment of 'reliable AI' for cybersecurity enhancement [70].

### *5.6. Introduction of New and More Sophisticated Security Measures*

A single sign-on (SSO) allows users to authenticate one time for subsequent access to various applications within/across an institution's IT systems. By eliminating the need for separate logins that require unique usernames and passwords, SSO reduces the probability of lost, forgotten, or stolen credentials resulting in security breaches [71].

Establishing identity assurance means ensuring that a person is who they say they are, as a password alone is not sufficient for this purpose. There is a need to add another layer of factors to verify one's identity. Multi-factor Authentication (MFA) is an authentication method by which individuals are granted access to the system after presenting two or more pieces of evidence to verify their identity. MFA is effective because cybercriminals usually do not have more than one type of credential information, and account owners would be alerted when multiple authentication attempts are made [72]. While MFA implementations in organisations are still far and in between [73], they may effectively counter modern ransomware [74].

As a state-of-the-art password alternative, adaptive authentication can be piloted in HEIs, especially in those departments where IoT devices have been used [75,76]. Such a user access permission control system dynamically selects the best mechanisms for authenticating a user depending on contextual factors, taking into consideration the user's circumstances such as geographic location, job function, patterns of past behaviour, proximity to devices, and time of day to give a context on why the user needs access and what they will do with it [77]. Although adaptive authentication has yet to become a method that is ready for a full-scale adoption at HEIs, it presents a promising direction for HEI to explore ways that combat human-factor or data-related risks.

### *5.7. Paying Attention to Mobile Devices Use, Using Encryption as a Daily Practice*

Mobile devices are ubiquitous, and their use in institutions (e.g., BYOD—"Bring Your Own Device" refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device) is becoming more commonplace. Meanwhile, because of the COVID-19 pandemic, work-from-home and remote learning have become a forced reality. The widespread dependency on mobile devices and the blurring line between personal and professional use of these devices have brought significant challenges for HEI cybersecurity. Noting mobile device uses will probably remain as a "new normal" [78], HEIs should pay special attention to managing their related cybersecurity risks. More specifically, HEI security professionals need to understand better how remote working and online learning are taking place in order to cater for those scenarios while ensuring that cybersecurity requirements are met.

In addition to having SSO and MFA in place and encouraging HEI staff to use VPN (Virtual Private Network) and VDI (Virtual Desktop Infrastructure), encryption is a straightforward defence strategy against various risk scenarios such as data breaches on using personal devices. Although many have recommended using encryption (e.g., [79]), it has yet to become a common, daily practice in HEIs. Given that documents could sometimes be shared via mobile instant messaging such as WeChat and Whatsapp, HEIs should develop clear policies and guidelines to help define the appropriate use of encryption and related key management methods. The scope and scale of the encryption policies and guidelines have to be explicit. This is particularly important because the level of encryption could vary, and the managing of trade-offs would have to be made clear to institution members; some files do not need to be encrypted for operational conveniences, but specific types of data require higher degrees of security. Usmonov et al. [80] also suggested using digital wa-

termarks, a kind of invisible marker secretly embedded in digital objects or noise-tolerant signals for protecting digital intellectual property (IP).

### *5.8. Risk Management*

In the context of the ever-changing and increasingly advanced cyber-attack forms, a group number of institutions are moving from a "maturity-based" to a "risk-based" approach for managing cybersecurity [81]. Risk management comprises all the ongoing and coordinated activities to direct and control how an organisation responds to the risks. For HEI cybersecurity risk management, it should cover not only the IT function but also all relevant perspectives. Effective HEI cyber security risk management should also entail cooperation and strong security awareness and culture across a full spectrum of institution members. Clear ownership and management accountability of the risks associated with cyber-attacks and related risk management measures should be established.

An entry point of risk management is self-assessment using institutional KPIs. It will allow the HEI leaders to develop a snapshot of HEI's cyber security status and steer growth to a more robust security standing. HEIs can identify the weak links that might compromise the institution's cybersecurity, the severity of the potential risks, and their possible impacts on the institution. Although specific methodologies may vary, self-assessment should be taken from a holistic perspective. As an essential intangible asset, big data of HEIs should not be overlooked as the information source for self-assessment. Big data such as user activity logs and security event logs can be analysed to gain security insights [82]. The result of the self-assessment can be presented with visualisations that enable HEI leaders and policy-makers to obtain a comprehensive view of different cybersecurity perspectives at once, and how they relate to each other. Based on the result, HEI leaders can develop achievable short-term, mid-term and long-term goals, plan strategies that can address the gaps, and initiate actions for the concerned parties.

A risk assessment is not merely a project or one-time event. HEIs must always be mindful of the ever-evolving nature of the cybersecurity landscape and be willing to alter their risk response because digital activities and institutional circumstances can change over time. Senior management should periodically engage with the IT department to ensure the adequacy of the cybersecurity controls with respect to the emerging cyber-threats found within and beyond the institution. If vulnerabilities and cybersecurity control gaps are identified, their size of impact and likelihood of occurrence needs to be further investigated. With this evaluation, the IT department should then establish a concrete risk mitigation plan that may cover upgrades or alternative compensating controls of IT systems. This plan would require vetting and endorsement from the senior management, as it could involve mobilisation of resources and staffing. In addition, the HEI leaders should also demand periodic reports from the departmental leaders so as to monitor any significant risks that emerge at the department level. Based on the risk appetite, how to prioritise and respond to those risks can be determined with concerned personnel. Since users are often the weakest link of cybersecurity controls, the departmental report should also include the status of adherence to institutional cybersecurity policies. Additionally, monitoring should entail regular independent assessment by teaming up with government agencies (e.g., Office of the Government Chief Information Officer (https://www.ogcio.gov.hk/, accessed on 20 February 2022), Hong Kong) and taking advantage of government-offered cybersecurity-concerned services (e.g., Hong Kong Computer Emergency Response Team Coordination Centre (https://www.hkcert.org, accessed on 20 February 2022) managed by the Hong Kong Productivity Council) so that HEIs can gain external evaluations of their risk management effectiveness and avoid blind spots while not risking any possible national security neglect.

## 6. Conclusions and Way Forward

This digital leap of new technologies come with increased vulnerabilities. New forms of cyber-attacks will continue to test the HEI's cybersecurity capacity. In responding to

potential cybersecurity risks in the new decade and the unique circumstances of HEIs that could challenge the applicability of many existing organisational cybersecurity management methods, this study proposes a system-wide approach with prioritised institutional strategies. The strategies include: (1) Strengthening Institutional Governance for Cybersecurity; (2) Revisiting Cybersecurity KPIs; (3) Explicating Cybersecurity Policies, Guidelines and Mechanisms; (4) Training and Cybersecurity Awareness Campaigns to Build Cybersecurity Culture; (5) Responding to AI-based Cyber-threats and Harnessing AI to Enhance Cybersecurity; (6) Introduction of New and More Sophisticated Security Measures; (7) Paying Attention to Mobile Devices Use, Using Encryption as a Daily Practice; and (8) Risk Management.

Though the strategies listed above are not comprehensive and may not prevent every attack, they do, from a system-wide perspective, represent a relatively straightforward means that can be used to yield significant benefits in higher education's fight against would-be cyber threats. We believe that cybersecurity could be safeguarded throughout the new decade when these strategies are considered thoroughly and with the concerted effort of relevant HEI stakeholders.

Future research may examine the effectiveness of these strategies. This may be achieved in the form of empirical studies. The strategies' applicability in varied HEI contexts would also be worthy of further investigation.

**Author Contributions:** Conceptualization—E.C.K.C. and T.W.; methodology, E.C.K.C. and T.W.; analysis—E.C.K.C. and T.W.; writing—E.C.K.C. and T.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. 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]
2. Kwaa-Aidoo, E.K.; Agbeko, M. An analysis of information system security of a Ghanaian university. *Int. J. Inf. Secur. Sci.* **2018**, *7*, 90–99.
3. Pinheiro, J. Review of cyber threats on Educational Institutions. In Proceedings of the Digital Privacy and Security Conference, Washington, DC, USA, 15 January 2020; Cordeiro, C., Barbosa, H., Eds.; Universidade Lusófona do Porto: Porto, Portugal, 2020; pp. 43–51.
4. Adams, A.; Blanford, A. Security and online learning: To protect and prohibit. In *Usability Evaluation of Online Learning Programs*; IGI Global: Hershey, PA, USA, 2003; pp. 331–359.
5. Alexei, 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.
6. Kelly, B.; McCormack, M.; Reeves, J.; Brooks, D.C.; O'Brien, J. *2021 EDUCAUSE Horizon Report: Information Security Edition*; EDUCAUSE: Boulder, CO, USA, 2021.
7. Czarniawska, B. *Social Science Research: From Field to Desk*; Sage: London, UK, 2014.
8. Murphey, D. A History of Information Security. IFSEC Global. 2019. Available online: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/ (accessed on 20 February 2022).
9. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Bus. Horiz.* **2021**, *64*, 659–671. [CrossRef]
10. Easttom, C. *Computer Security Fundamentals*, 4th ed.; Pearson IT Certification: Indianapolis, IN, USA, 2019.
11. Ferbrache, D. *A Pathology of Computer Viruses*; Springer Science & Business Media: Berlin, Germany, 2012.
12. Grispos, G. Criminals: Cybercriminals. *Encycl. Secur. Emerg. Manag.* **2019**, *1*, 1–7.
13. Furstenau, L.B.; Sott, M.K.; Homrich, A.J.O.; Kipper, L.M.; Al Abri, A.A.; Cardoso, T.F.; Cobo, M.J. 20 years of scientific evolution of cyber security: A science mapping. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Dubai, United Arab Emirates, 10–12 March 2020; IEOM Society International: Southfield, MI, USA; pp. 314–325.

14. Kunwar, R.S.; Sharma, P. Social media: A new vector for cyber attack. In Proceedings of the 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA), Dehradun, India, 8–9 April 2016; IEEE: Piscataway, NJ, USA; pp. 1–5.
15. Harding, L. *The Snowden Files: The Inside Story of the World's Most Wanted Man*; Guardian Faber Publishing: London, UK, 2014.
16. Daswani, N.; Elbayadi, M. The Yahoo Breaches of 2013 and 2014. In *Big Breaches*; Apress: Berkeley, CA, USA, 2021; pp. 155–169.
17. Humayun, M.; Niazi, M.; Jhanjhi, N.Z.; Alshayeb, M.; Mahmood, S. Cyber security threats and vulnerabilities: A systematic mapping study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
18. Wangen, G. The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information* **2015**, *6*, 183–211. [CrossRef]
19. Kettani, H.; Wainwright, P. On the top threats to cyber systems. In Proceedings of the 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), Kahului, HI, USA, 14–17 March 2019; IEEE: Piscataway, NJ, USA; pp. 175–179.
20. Mohurle, S.; Patil, M. A brief study of wannacry threat: Ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1938–1940.
21. Varlioglu, S.; Gonen, B.; Ozer, M.; Bastug, M. Is cryptojacking dead after coinhive shutdown? In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), Silicon Valley, CA, USA, 9–12 March 2020; IEEE: Piscataway, NJ, USA; pp. 385–389.
22. World Economic Forum. *The Global Risks Report 2022*, 17th ed.; World Economic Forum: Cologny, Switzerland, 2022.
23. Pardeshi, V.H. Cloud computing for higher education institutes: Architecture, strategy and recommendations for effective adaptation. *Procedia Econ. Financ.* **2014**, *11*, 589–599. [CrossRef]
24. Ananthi, C.M.T.; Arul, L.R.P.J. Implications, Risks and Challenges of Cloud Computing In Academic Field–A State-of-Art. *Int. J. Sci. Technol. Res.* **2019**, *8*, 3268–3278.
25. Corradini, I. Redefining the Approach to Cybersecurity. In *Building a Cybersecurity Culture in Organisations*; Springer: Cham, Switzerland, 2020; pp. 49–62.
26. Kaloudi, N.; Li, J. The AI-based cyber threat landscape: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–34. [CrossRef]
27. Meland, P.H.; Bayoumy, Y.F.F.; Sindre, G. The Ransomware-as-a-Service economy within the darknet. *Comput. Secur.* **2020**, *92*, 1–9. [CrossRef]
28. Kahn, A. The 2019 Cybersecurity Threat Landscape. 2019. Available online: https://www.rmahq.org/the-2019-cybersecurity-threat-landscape/ (accessed on 20 February 2022).
29. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
30. Vorakulpipat, C.; Rattanalerdnusorn, E.; Thaenkaew, P.; Hai, H.D. Recent challenges, trends, and concerns related to IoT security: An evolutionary study. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; IEEE: Piscataway, NJ, USA; pp. 405–410.
31. Bertino, E. Data Security and Privacy in the IoT. In Proceedings of the 19th International Conference on Extending Database Technology (EDBT): OpenProceedings, Bordeaux, France, 15–16 March 2016; pp. 1–3.
32. Forestiero, A. Bio-inspired algorithm for outliers detection. *Multimed. Tools Appl.* **2017**, *76*, 25659–25677. [CrossRef]
33. Forestiero, A. Metaheuristic algorithm for anomaly detection in Internet of Things leveraging on a neural-driven multiagent system. *Knowl. Based Syst.* **2021**, *228*, 107241. [CrossRef]
34. Lamal, P.A. Higher education: Social institution or business? *Behav. Soc. Issues* **2001**, *11*, 65–70. [CrossRef]
35. Kin-Keung, D.C. A comparative study on the corporatisation of higher education in Hong Kong and Singapore. In *Social Stratification in Chinese Societies*; Brill: Leiden, The Netherlands, 2010; pp. 191–224.
36. Alexander, F.K. The changing face of accountability: Monitoring and assessing institutional performance in higher education. *J. High. Educ.* **2000**, *71*, 411–431. [CrossRef]
37. Anderson, E.E.; Choobineh, J. Enterprise information security strategies. *Comput. Secur.* **2008**, *27*, 22–29. [CrossRef]
38. Aven, T. On the allegations that small risks are treated out of proportion to their importance. *Reliab. Eng. Syst. Saf.* **2015**, *140*, 116–121. [CrossRef]
39. Olsen, R.V.; Tokerud, S. Teachers' Awareness, Knowledge and Practice of Information Security in School. Master's Thesis, University of Agder, Kristiansand, Norway, 2020. Available online: https://hdl.handle.net/11250/2678221 (accessed on 20 February 2022).
40. Bojanc, R.; Jerman-Blažič, B. An economic modelling approach to information security risk management. *Int. J. Inf. Manag.* **2008**, *28*, 413–422. [CrossRef]
41. Metalidou, E.; Marinagi, C.; Trivellas, P.; Eberhagen, N.; Giannakopoulos, G.; Skourlas, C. Human factor and information security in higher education. *J. Syst. Inf. Technol.* **2014**, *16*, 210–221. [CrossRef]
42. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Comput. Secur.* **2014**, *42*, 165–176. [CrossRef]
43. Parsons, K.; Calic, D.; Pattinson, M.; Butavicius, M.; McCormac, A.; Zwaans, T. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Comput. Secur.* **2017**, *66*, 40–51. [CrossRef]
44. Johnston, A.C.; Hale, R. Improved security through information security governance. *Commun. ACM* **2009**, *52*, 126–129. [CrossRef]
45. Wilkin, C.L.; Chenhall, R.H. A review of IT governance: A taxonomy to inform accounting information systems. *J. Inf. Syst.* **2010**, *24*, 107–146. [CrossRef]

46. Ferguson, C.; Green, P.; Vaswani, R.; Wu, G. Determinants of effective information technology governance. *Int. J. Audit.* **2013**, *17*, 75–99. [CrossRef]
47. Chong, J.L.; Tan, P.; Felix, B. IT governance in collaborative networks: A socio-technical perspective. *Pac. Asia J. Assoc. Inf. Syst.* **2012**, *4*, 31–48. [CrossRef]
48. Nolan, R.; McFarlan, F.W. Information technology and the board of directors. *Harv. Bus. Rev.* **2005**, *83*, 96.
49. Rothrock, R.A.; Kaplan, J.; Van Der Oord, F. The board's role in managing cybersecurity risks. *MIT Sloan Manag. Rev.* **2018**, *59*, 12–15.
50. Spremić, M.; Šimunic, A. Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering, London, UK, 4–6 July 2018; International Association of Engineers: Hong Kong, China, 2018; pp. 341–346.
51. Huang, R.; Zmud, R.W.; Price, R.L. Influencing the effectiveness of IT governance practices through steering committees and communication policies. *Eur. J. Inf. Syst.* **2010**, *19*, 288–302. [CrossRef]
52. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. [CrossRef]
53. Diesch, R.; Pfaff, M.; Krcmar, H. A comprehensive model of information security factors for decision-makers. *Comput. Secur.* **2020**, *92*, 101747. [CrossRef]
54. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. 2018. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 20 February 2022).
55. Baskerville, R.; Siponen, M. An information security meta-policy for emergent organisations. *Logist. Inf. Manag.* **2002**, *15*, 337–346. [CrossRef]
56. Höne, K.; Eloff, J.H.P. What makes an effective information security policy? *Netw. Secur.* **2002**, *2002*, 14–16. [CrossRef]
57. Doherty, N.F.; Anastasakis, L.; Fulford, H. The information security policy unpacked: A critical study of the content of university policies. *Int. J. Inf. Manag.* **2009**, *29*, 449–457. [CrossRef]
58. Da Veiga, A.; Astakhova, L.V.; Botha, A.; Herselman, M. Defining organisational information security culture—Perspectives from academia and industry. *Comput. Secur.* **2020**, *92*, 101713. [CrossRef]
59. Wiley, A.; McCormac, A.; Calic, D. More than the individual: Examining the relationship between culture and Information Security Awareness. *Comput. Secur.* **2020**, *88*, 101640. [CrossRef]
60. Alshaikh, M. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Comput. Secur.* **2020**, *98*, 102003. [CrossRef]
61. Fennelly, L.J.; Perry, M.A. Chapter 35-Building a Sustainable Culture of Security. In *The Professional Protection Officer*; Davies, S.J., Fennelly, L.J., Eds.; Butterworth-Heinemann: Boston, UK, 2020; pp. 397–401.
62. Coffey, J.W.; Haveard, M.; Golding, G. A case study in the implementation of a human-centric higher education cybersecurity program. *J. Cybersecur. Educ. Res. Pract.* **2018**, *2018*, 4.
63. Wenger, E. *Communities of Practice: Learning, Meaning and Identity*; Cambridge University Press: Cambridge, UK, 2000.
64. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artif. Intell. Rev.* **2021**, *54*, 3849–3886. [CrossRef]
65. Pandya, P. Chapter e16-Local Area Network Security. In *Computer and Information Security Handbook*, 3rd ed.; Vacca, J.R., Ed.; Morgan Kaufmann: Burlington, MA, USA, 2013; pp. e1–e20.
66. Alhawi, O.M.K.; Baldwin, J.; Dehghantanha, A. Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. In *Cyber Threat Intelligence*; Dehghantanha, A., Conti, M., Dargahi, T., Eds.; Springer: Cham, Switzerland, 2018; pp. 93–106.
67. Guha Roy, D.; Srirama, S.N. A Blockchain-based Cyber Attack Detection Scheme for Decentralised Internet of Things using Software-Defined Network. *Softw. Pract. Exp.* **2021**, *51*, 1540–1556. [CrossRef]
68. Al-Abassi, A.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access* **2020**, *8*, 83965–83973. [CrossRef]
69. Zhan, Z.; Xu, M.; Xu, S. Predicting cyber attack rates with extreme values. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1666–1677. [CrossRef]
70. Taddeo, M.; McCutcheon, T.; Floridi, L. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nat. Mach. Intell.* **2019**, *1*, 557–560. [CrossRef]
71. Radha, V.; Reddy, D.H. A survey on single sign-on techniques. *Procedia Technol.* **2012**, *4*, 134–139. [CrossRef]
72. Boonkrong, S. Multi-factor Authentication. In *Authentication and Access Control: Practical Cryptography Methods and Tools*; Apress: Berkeley, CA, USA, 2021; pp. 133–162.
73. Das, S.; Wang, B.; Tingle, Z.; Camp, L.J. Evaluating user perception of multi-factor authentication: A systematic review. *arXiv* **2019**, arXiv:1908.05901.
74. Goettl, C. Is ransomware winning? *Cyber Secur. A Peer-Rev. J.* **2021**, *5*, 51–65.
75. Arfaoui, A.; Cherkaoui, S.; Kribeche, A.; Senouci, S.M.; Hamdi, M. Context-aware adaptive authentication and authorisation in Internet of Things. In Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
76. Fayad, A.; Hammi, B.; Khatoun, R. An adaptive authentication and authorisation scheme for IoT's gateways: A blockchain based approach. In Proceedings of the 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 18–19 October 2018; IEEE: Piscataway, NJ, USA; pp. 1–7.

77. Arias-Cabarcos, P.; Krupitzer, C.; Becker, C. A survey on adaptive authentication. *ACM Comput. Surv.* **2020**, *52*, 1–30. [CrossRef]
78. Bick, A.; Blandin, A.; Mertens, K. Work from Home before and after the COVID-19 Outbreak. 2021. Available online: https://ssrn.com/abstract=3786142 (accessed on 20 February 2022).
79. Munro, K. Desktop encryption. *Netw. Secur.* **2008**, *2008*, 4–6. [CrossRef]
80. Usmonov, B.; Evsutin, O.; Iskhakov, A.; Shelupanov, A.; Iskhakova, A.; Meshcheryakov, R. The cybersecurity in development of IoT embedded technologies. In Proceedings of the 2017 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2–4 November 2017; IEEE: Piscataway, NJ, USA; pp. 1–4.
81. Boehm, J.; Curcio, N.; Merrath, P.; Shenton, L.; Stähle, T. *The Risk-Based Approach to Cybersecurity*; McKinsey & Company: New York, NY, USA, 2019.
82. Petrenko, S.A.; Makoveichuk, K.A. Big data technologies for cybersecurity. In Proceedings of the CEUR Workshop Proceedings 2081 CEUR-WS.org, Moscow, Russia, 6–7 December 2017; Sun SITE Central Europe: Aachen, Germany, 2017; pp. 107–111.