applied sciences

MDPI

Article

A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom

Aliyu Aliyu, Leandros Maglaras *, Ying He *, Iryna Yevseyeva, Eerke Boiten, Allan Cook and Helge Janicke

School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK; P17243308@my365.dmu.ac.uk (A.A.); iryna@dmu.ac.uk (I.Y.); eerke.boiten@dmu.ac.uk (E.B.); allan.cook@dmu.ac.uk (A.C.); helge.janicke@cybersecuritycrc.org.au (H.J.)

* Correspondence: leandros.maglaras@dmu.ac.uk (L.M.); ying.he@dmu.ac.uk (Y.H.)

Received: 15 April 2020; Accepted: 18 May 2020; Published: 25 May 2020

Abstract: As organisations are vulnerable to cyberattacks, their protection becomes a significant issue. Capability Maturity Models can enable organisations to benchmark current maturity levels against best practices. Although many maturity models have been already proposed in the literature, a need for models that integrate several regulations exists. This article presents a light, web-based model that can be used as a cybersecurity assessment tool for Higher Education Institutes (HEIs) of the United Kingdom. The novel Holistic Cybersecurity Maturity Assessment Framework incorporates all security regulations, privacy regulations, and best practices that HEIs must be compliant to, and can be used as a self assessment or a cybersecurity audit tool.

Keywords: assessment framework; cybersecurity; GDPR; PCI-DSS; DSPT; NISD

1. Introduction

In an age of information growth, technology plays a key role in shaping all aspects of human life. In the education sector, teachers and students can make use of the ever-expanding resources available, creating a diverse learning experience that caters for many teaching and learning styles. However, with this adoption of technology, Higher Education Institutions (HEIs) are finding themselves the targets of malicious cyberactivities, with a recent JISC report [1] reaffirming that UHEIs in the UK are not well prepared to defend against, or recover from cyberattacks.

Due to their nature, HEIs hold a significant amount of information and accumulated knowledge. As a result, they are attractive to threat actors who target research findings, financial data, and computing resources. Katz [2] identified that HEIs are under continual risk of cyberattacks. Consequently, HEIs face a constant challenge of balancing public access in the interest of sharing information, whilst protecting their information assets.

A study of businesses students in New England was conducted by Kim [3] on the attitude of students regarding Information Security Awareness (ISA). It was evident in the findings that students who participated found the ISA training important and necessary in improving their knowledge in cybersecurity. Studies in 2013 by the Kaspersky Lab [4] showed over the period of a year that 91% of organisations surveyed reported their IT infrastructure had been the victim of at least one cyberattack. Additionally stated in the report, there was an increase in cybercrime such as email phishing, unauthorised network access, malware, and theft of mobiles in 2013 compared to 2012. The study focused on corporate IT infrastructures and highlighted that for years, IT infrastructures such as those in HEIs had been deficient in terms of security and had always been a target for threat actors.

In the market, there are currently many frameworks available for organisations to adopt to improve the effectiveness of their cybersecurity. These frameworks support action at both an individual and organisational level. Aloul [5] highlights that for the success and security of any security improvement program adopted by an institution, it is important that students and staff are given training and education in information security awareness. This should be made part of the risk/security assessment plan adopted by all levels of administration, from students, to teachers, and all administrative employees, as teaching the front-end users will serve as the first line of defence against attackers [6].

To build a secure environment, providing a relevant security awareness program is the initial step. There should be constant training and education provided to equip students, staff, and employees to deal with the latest cyberthreats and modern prevention methods [7]. There should also be effectiveness metrics that the institution can measure and monitor. Changes to management and audits can be adopted by the institution to strengthen the level of cybersecurity [8]. One important set of tools that HEIs can use in order to measure their cybersecurity readiness and compliance levels is maturity models [9].

Matthew J. Butkovic [10] defined the maturity model as "a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline". The artefacts that make up the model are typically agreed on by the domain or discipline, which validates them through application and iterative recalibration. In order to make maturity models more effective, the measurable transitions between levels should be based on empirical data that have been validated in practice. This means each level in the model should be more mature than the previous level. In essence, what constitutes mature behaviours must be characterised and validated. This can be challenging to achieve unambiguously in many maturity models.

Our proposed Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) is based on a process methodology called a Capability Maturity Model (CMM) [11]. CMMs were originally developed by the Carnegie Mellon University Software Engineering Institute (CMU/SEI) to improve the management of software development, and have been subsequently used in many other domains, such as cybersecurity. A maturity model defines a set of metrics for measuring organisational competency or maturity in terms of a set of recognised best practices, skills, or standards. Metrics are organised into categories and quantified on a performance scale. Using specific rating criteria, organisations can measure their performance against these maturity levels.

This paper makes the following contributions,

- It proposes a novel Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) for HEIs that can be used in order to conduct a gap analysis against 15 security requirements.
- The proposed framework incorporates several regulations and security best practices into one lightweight online self-assessment guide.
- It produces compliance reports against all regulations that the HEI must be compliant with in order to facilitate mitigation plans.
- It can be adapted and expanded in order to be used on other critical sectors of the UK and abroad.

The rest of the paper is organised as follows: In Section 2, we present related work, while in Section 3 we describe our system framework. In Section 3.4, we present the validation procedure. Finally, in Section 5, we conclude this paper and present future work.

2. Related Work

2.1. Essential Components of a Maturity Model

A maturity model should follow a structure to ensure its consistency. It typically includes the components, levels, attributes, appraisal and scoring methods, and model domains. Levels represent

the measurement aspect of a maturity model, however, if the scaling is inaccurate or incomplete, we may not be able to validate the model and the results produced may not be accurate or consistent.

Attributes represent the main content of the model and are classified by domains and levels. Attributes are defined at the intersection of a domain and a maturity level, which are typically based on observed practices, standards, or other expert knowledge. These can be expressed as characteristics, indicators, practices, or processes. In capability models, attributes also express qualities of organisational maturity (e.g., planning and measuring) for supporting process improvement regardless of the process being modelled.

Appraisal and scoring methods are used to facilitate the assessment. They can be formal or informal, expert-led or self-applied. Scoring methods are algorithms devised by the community to ensure consistency of appraisals and they are common standards for measurement. Scoring methods can include weighting (so that important attributes are valued over less important ones) or can value different types of data collection in different ways (e.g., providing higher marks for documented evidence than for interview-based data).

Model domains essentially define the scope of a maturity model. Domains are a means for grouping attributes into an area of importance for the subject matter and intent of the model. In capability models, the domains are often (but not necessarily) referred to as process areas as they are a collection of processes that make up a larger process or discipline (e.g., software engineering). Depending on the model, users may be able to focus on improving a single domain or a group of domains.

2.2. Maturity Model Types

Caralli [12] classified maturity models into three different types—progression models, capability models, and hybrid models. Progression models represent a simple progression or scaling of a characteristic, indicator, attribute, or pattern in which the movement through the maturity levels indicates some progression of attribute maturity. Progression models typically place their focus on the evolution of the model's core subject matter (such as practices or technologies) rather than attributes that define maturity (such as the ability and willingness to perform a practice, the degree to which a practice is validated, etc.). In other words, the purpose of a progression model is to provide a simple road map of progression or improvement as expressed by increasingly better versions (for example, more complete, more advanced) of an attribute as the scale progresses [10]. For capability models such as CMM, the dimension that is being measured is a representation of organisational capability around a set of characteristics, indicators, attributes, or patterns—often expressed as processes. A CMM measures more than the ability to perform a task; it also focuses on broader organisational capabilities that reflect the maturity of the culture and the degree to which the capabilities are embedded (or institutionalised) in the culture [10]. Hybrid models merge two abilities; the ability to measure maturity attributes and the ability to measure evolution or progression in progressive models. This type of model reflects transitions between levels that are similar to capability model levels (i.e., that describe capability maturity) but also account for the evolution of attributes in a progression model [10].

2.3. Existing Work on Maturity Models

Evaluation of maturity capability was developed in 1986 by the US Department of Defense for assessing maturity capabilities of Software Engineering processes of the software companies they worked with [13]. This model was later adopted by different domains including cybersecurity.

Various cybersecurity maturity models were developed according to the needs of organisations. Currently, the most popular and widely used maturity models are incorporated into (inter)national standards. For instance, ISO/IEC 27001 [14,15] and NIST [16]—European and American standards for cybersecurity, respectively. ISO/IEC 27001 was developed based on the British Standard BS7799 and ISO/IEC 17799 to provide requirements as well as to maintain and improve Information Security

Management System (ISMS) [13]. ISO/IEC 27001 defines ISMS as a part of the overall management system, which "establish, implement, operate, monitor, review, maintain and improve information security" [14,15].

Sabillon et al. [17] proposed a Cybersecurity Audit Model (CSAM) in order to improve cybersecurity assurance. The CSAM was designed to be used for conducting cybersecurity audits in organisations and Nation States. CSAM evaluates and validates audit, preventive, forensic, and detective controls for all organisational functional areas. The CSAM was then tested, implemented, and validated along with the Cybersecurity Awareness TRAining Model (CATRAM) in a Canadian higher education institution. Adler et al. [18] created a Dynamic Capability Maturity Model for improving cybersecurity. It extends an existing cybersecurity CMM into a dynamic performance management framework. It is a software-based framework that enables organisations to create, test, validate, or refine plans to improve their cybersecurity maturity levels. Almuhammadi et al. identified the gaps of the NIST Cyber Security Framework for Critical Infrastructure (NIST CSF) by comparing it to the COBIT, ISO/IEC 27001, and ISF frameworks, and then proposed an Information Security Maturity Model (ISMM) to fill in the gaps and measure NIST CSF implementation progress [19]. Miron et al. reviewed Cybersecurity Capability Maturity Models for providers of critical infrastructure, and provided recommendations on employing capability maturity models to measure and communicate readiness [20].

Akinsanya et al. investigated the effective assessment of healthcare cybersecurity maturity models for healthcare organisations using cloud computing [21]. The findings showed that the assessment practices are sometimes considered ineffective since the measurements of individual IS components were not capable of depicting the overall security posture within a healthcare organisation. The effects of cloud computing technology in healthcare were also not taken into account.

The existing maturity models offer a manageable approach for assessing the security level of a system or organisation, however, it is difficult to establish sound security models and mechanisms for protecting the cyberspace, as the definitions and scopes of both cyberspace and cybersecurity are still not well defined [22]. Most of the existing maturity models provide a minimum compliance model rather than an aspired cybersecurity model that can address emerging threat landscape. The model should allow multiusers including management, security experts, and practitioners to assess the overall security status of the organisation/system and take measures to address the weaknesses identified from the assessment. Most of the existing models are measured by qualitative metrics/processes, however quantitative metrics should be essential for security assessment [22,23].

2.4. Selected Existing Models Adopted for HEIs Maturity Assessment

Existing models were reviewed for their applicability for HEIs maturity assessment. The basis of our maturity model was formed according to the CMMI [24]. The CMMI was used as it provides an evolutionary path to performance improvement.

The starting point of a cybersecurity assessment is the definition of requirements for an Information Security Management System (ISMS) of an organisation. ISO/IEC 27001 Information Security Management [14,15] is the best-known standard for providing a set of necessary requirements and this was used in our framework.

In addition to the evaluation of maturity, our model provides a set of cybersecurity actions and controls to be implemented to close the existing gaps in HEI cybersecurity. For this, we reviewed a number of well-established models and selected the most critical ones to be used for HEIs' protection from known cyberattack vectors. The CIS Controls [25] are specifically technical controls that can be used to mitigate from specific attacks. ENISA's guidelines on assessing DSP security and OES compliance with the NISD security requirements [26] provided insight into the self-assessment/management framework for the DSP security against the security requirements. The cybersecurity evaluation tool provided a systematic approach for evaluating an organisation's security posture by assessing operational resilience, cybersecurity practices,

organisational management of external dependencies, and other key elements of a robust cybersecurity framework.

Except the above models, Citigroup's Information Security Evaluation Model (CITI-ISEM) [20], Computer Emergency Response Team / CSO Online at Carnegie Mellon University (CERT/CSO), and the U.S. Cybersecurity Capability Maturity Model (C2M2) and its National Initiative for Cybersecurity Education's Capability Maturity Model (NICE-CMM) were also reviewed [20]. These models were reviewed in order to check that we did not miss any important security controls from incorporating them into our framework.

The work of Mbanaso et al. titled Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework [27] was also reviewed and it provided insight into measuring the effectiveness and efficiency of organisation's controls with respect to cybersecurity resilience, and also the steps that can be taken to improve resilience maturity. Lastly, the work of Butkovic and Caralli titled Advancing Cybersecurity Capability Measurement using the CERT-RMM Maturity Indicator Level Scale [28] provided insight into how the CMMI maturity levels can be utilised to show incremental improvement in maturity.

Recently, ENISA [29] published a report that presents a mapping of the main security objectives between the NISD and General Data Protection Regulation (GDPR) in order to support organisations in their process of identifying appropriate security measures. At the same time, ISO issued the ISO 27701 Standard [30] in order to help organisation establish, implement, maintain, and continually improve a Privacy Information Management System by combining the ISMS with the privacy framework and principles defined in ISO/IEC 29100. NIST has also published the Privacy Framework [31] that follows the structure of the Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework) in order to facilitate the use of both frameworks together. It is obvious that all major security organisations and authorities have identified the need for mapping cybersecurity requirements from different frameworks, but until now, only initial works that map GDPR with NIST and NISD have been published.

Apart from the lack of a security maturity model tailored for HEIs, the other identified gaps in the review of these maturity models occur in the aspect of adoption: the maturity models are either too complicated to implement, or they require the organisation's processes to be refined to suit their implementation. HEIs have more fluid and less controllable environments, which render many of ISO controls nonapplicable or introduce too significant barriers for HE to manage effectively.

A holistic framework that incorporates all regulations and can be used either offline or online with easily followed and understood maturity assessment metrics was needed for the HEIs. The proposed framework incorporates several regulations and security best practices into one lightweight online self assessment guide that can be run as a self assessment or audit tool. HCYMAF supports the assessment of the maturity of each of the 15 specified domains to identify weak and strong practices and can be easily extensible in order to incorporate other domains, e.g., IoT, blockchain [32] etc.

3. Proposed Maturity Framework

An appraisal is an activity that helps identify the strengths and weaknesses of an organisation's processes and to examine how closely the processes relate to identified best practices. Appraisals are typically conducted to determine how well the organisation's processes are when compared to related identified security best practices and to identify areas where improvement can be made. Our proposed Maturity Assessment Framework (MAF) can be used in order to inform external customers and suppliers about how well the organisation's processes are when compared to related identified security best practices. The model can also be used as a gap-analysis and compliance-checking tool that any organisation can use in order to define how well contractual requirements are met. The MAF is established based on the following:

- A review of security requirements that HEIs must follow in order to demonstrate compliance with the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard

(PCI DSS), Data Security and Protection Toolkit (DSPT), and any other regulation that may apply to them;
- A literature review of existing research on maturity models in cybersecurity as well as in other areas.

This framework, entitled "A Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) for Higher Education Institutes (HEIs)", aims at designing a cybersecurity maturity assessment framework for all higher education institutes in the United Kingdom. The framework can be used as a self-assessment tool by the HEIs organisation in order to establish their security level and highlight the weaknesses and mitigation plans that need to be implemented. The framework is a mapping and codification tool for HEIs against all regulations that the HEIs must comply with, such as the GDPR, PCI DSS, DSPT, etc.

The framework uses six different levels of maturity against which the cybersecurity performance of each organisation can be measured. The framework will be validated through three pilot implementations, of which one has already been conducted with positive results and feedback obtained. This model is important and novel because HEIs, by using this framework, will be able to assess the security level of their organisation, conduct a gap analysis, and create appropriate mitigation plans. The model also informs whether the organisation is compliant with the expected regulations, thus helping them in self-assessment and improvement by producing relevant compliance reports.

It is necessary to design a maturity model that will be able to facilitate the organisations and the National Cyber Security Center (NCSC) of the UK. To achieve this, the model must have the following characteristics. It must

- Cover the full extent of the requirements of the different regulations;
- Be able to be used as a self-assessment tool;
- Be able to be used as a basis for an independent assessment;
- Provide clear results regarding the security posture of the organisations;
- Produce compliance reports;
- Be able to be used as guidance for implementation of a concrete security policy by the HEIs;
- Be measurable;
- Be easily extractable and reusable.

3.1. Security Requirements

As illustrated in Figure 1, the proposed maturity assessment model has 15 requirements. The 15 requirements followed are categorised as 'General Security Requirements'. The General Security Requirements, which are the foundation of the model, is based on cybersecurity best practices such as the CIS Controls, NIST Framework, etc. The 15 requirements were divided into 3 groups. IDENTIFY (I), PROTECT & DETECT (P), and RESPOND & RECOVER (R). It should be noted that the DETECT controls of NIST were merged into our protect & detect requirements in order to keep our model lightweight.

Requirements $I1$–$I4$ fall under Identify, Requirements $P5$–$P13$ fall under Protect & Detect, whilst Requirements $R14$–$R15$ fall under Respond & Recover. All the requirements of the category Identify are necessary for the facilitation of the understanding of the business and operational ecosystem of the organisation. All the requirements of Protect & Detect are necessary in order to detect incidents and protect all assets supporting the services of the organisation i.e., (people, procedures, and technologies). Lastly, all the requirements of Respond & Recover are necessary in order to respond and manage an information security incident that may have the ability to influence the provision of the services offered by the HEIs. Finally, it should be noted that some requirements do have sub-requirements (See Figure 2).

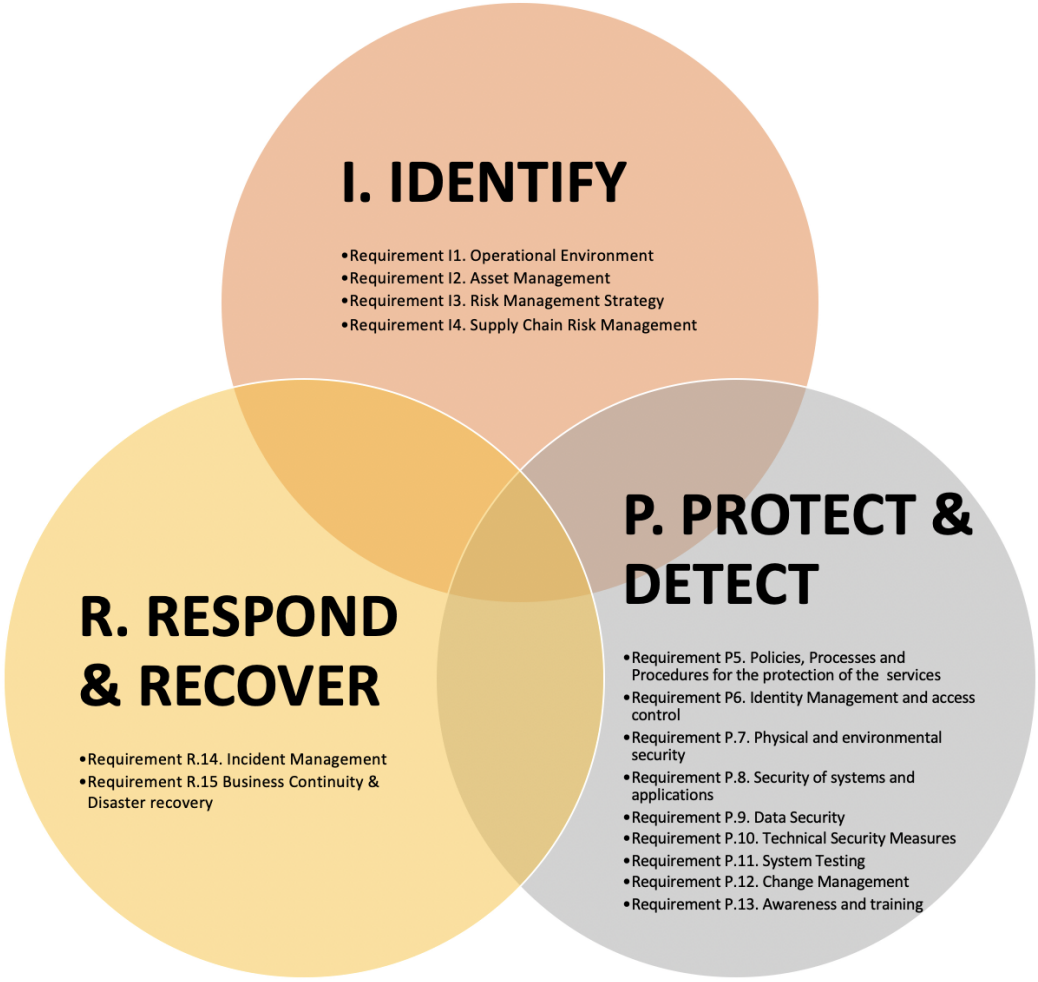

Figure 1. Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) requirements are divided into three groups.

3.2. Mapping of Regulations

It is worth stating that we incorporated the regulation requirements of GDPR, PCI DSS, and DSPT into our General Security Requirements. The mapping of the different regulations into the HCYMAF is shown in the upcoming Figures 3–5. This was done by focusing on each individual regulation and mapping it into one of our requirements. For example, in terms of GDPR, we focused on the 7 principles of GDPR—as shown in Figure 3—and mapped each of the principles into one of our requirements. For example, the first principle of GDPR is lawfulness, fairness, and transparency. This was mapped into Sub-Requirement P5.1: GDPR Compliance. The second principle, which is purpose limitation, was mapped into Requirement P5: Policies, Processes, and Procedures for the protection of the services, and so on.

In terms of incorporating PCI DSS, we focused on the 6 principles of PCI DSS, as each of these principles had its requirements (See Figure 4). In terms of incorporating DSPT, we also focused on the 10 principles of the regulation and likewise each of those principles was mapped into one of our requirements (See Figure 5). Overall, all the aforementioned regulations were incorporated into our model and merged to form a solid maturity model, as illustrated in Figure 6.

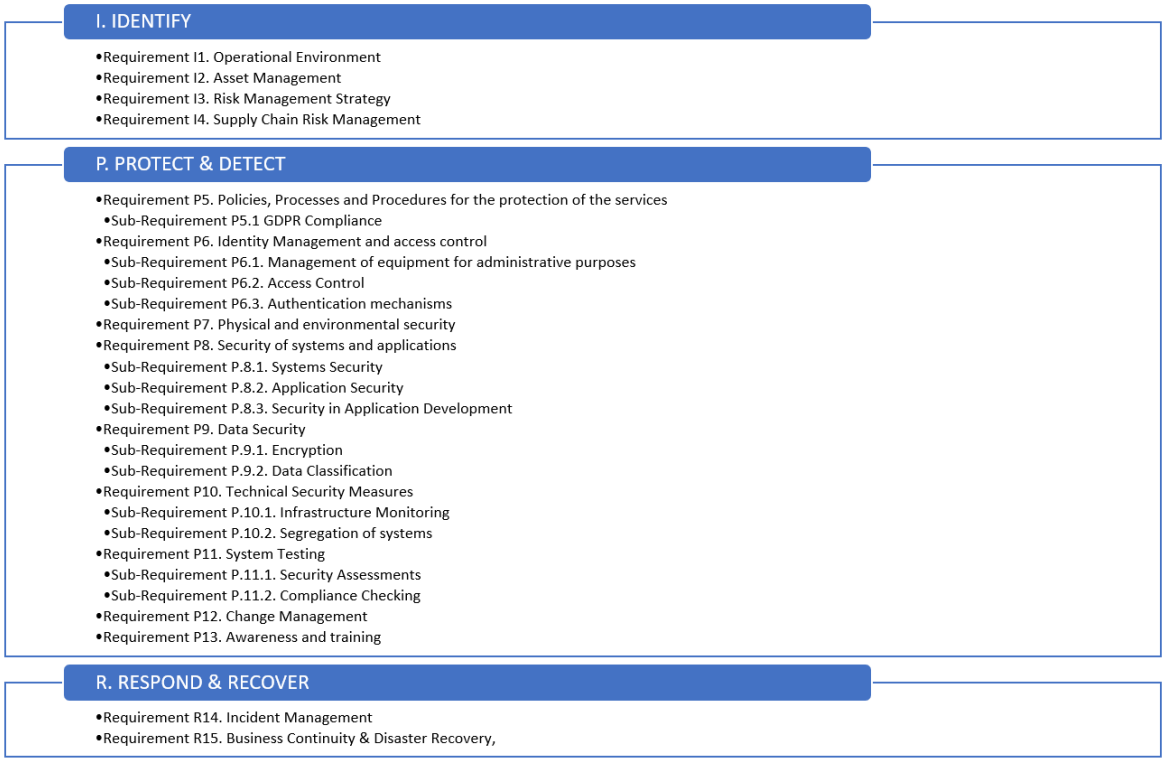

Figure 2. The proposed HCYMAF model in detail.

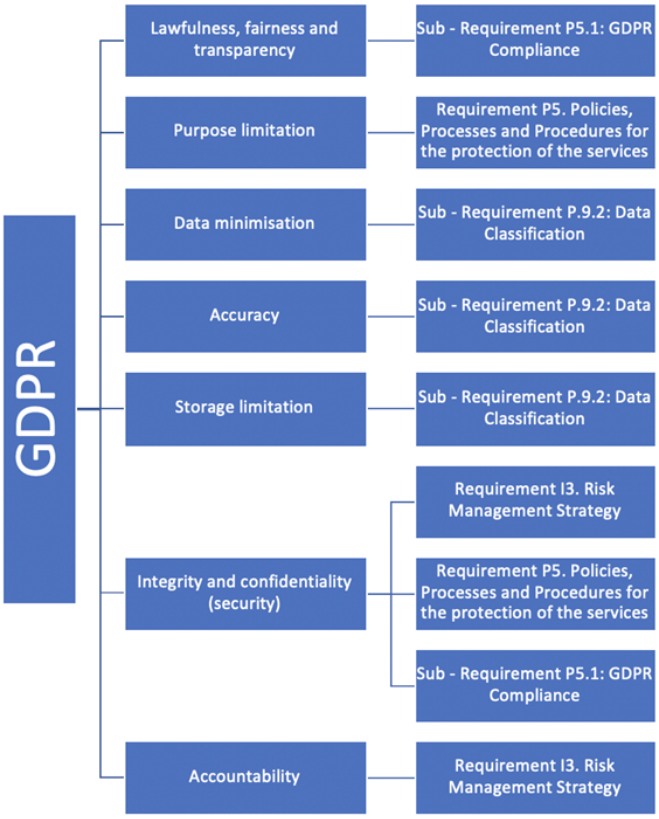

Figure 3. General Data Protection Regulation (GDPR) Mapping.

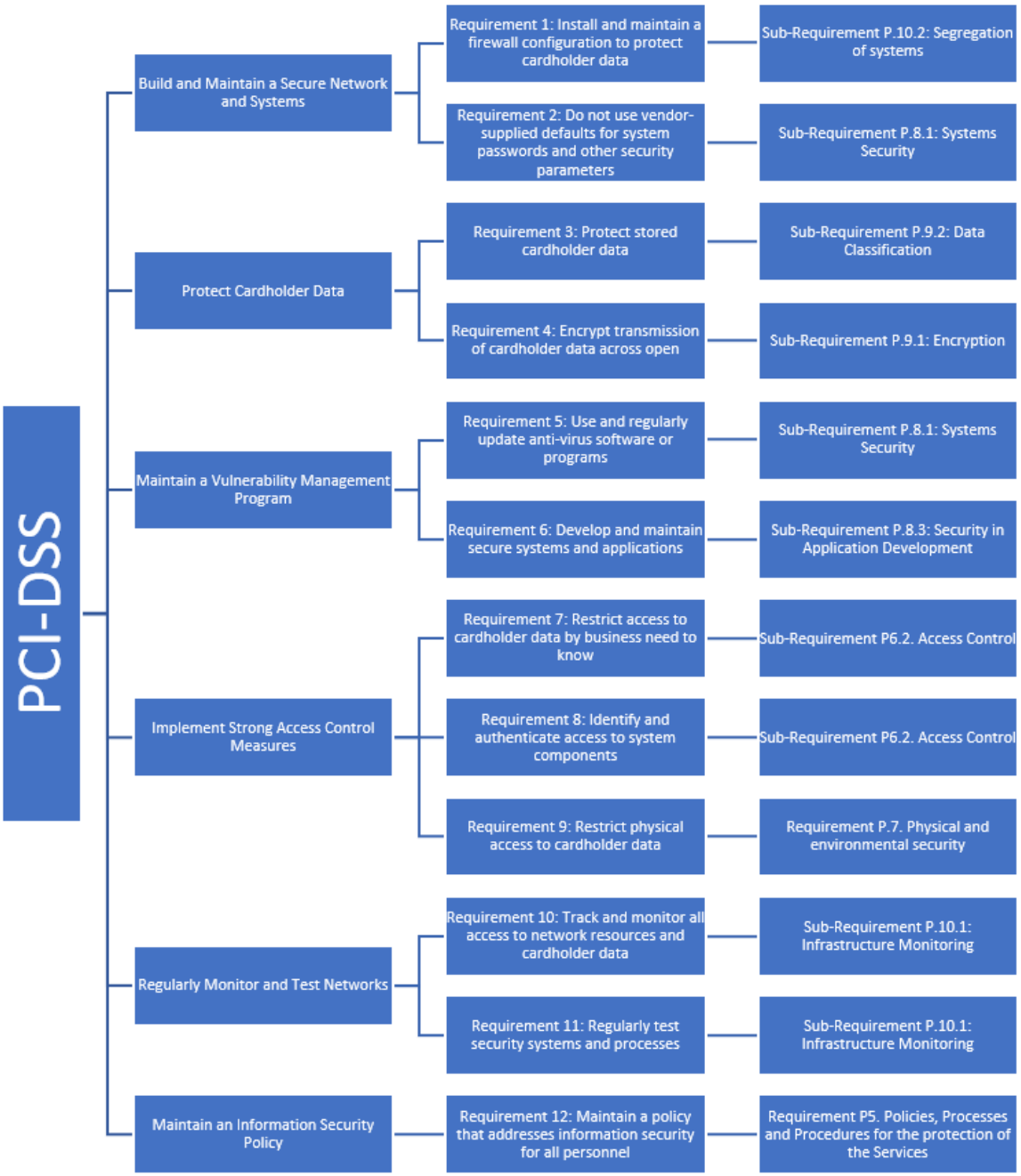

Figure 4. Payment Card Industry Data Security Standard (PCI DSS) Mapping.

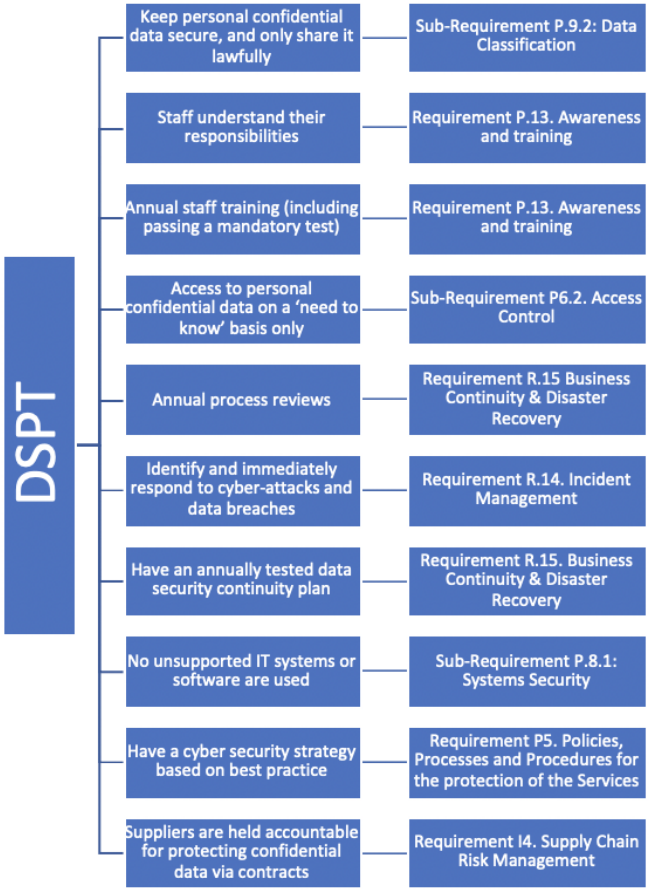

Figure 5. Data Security and Protection Toolkit (DSPT) Mapping.

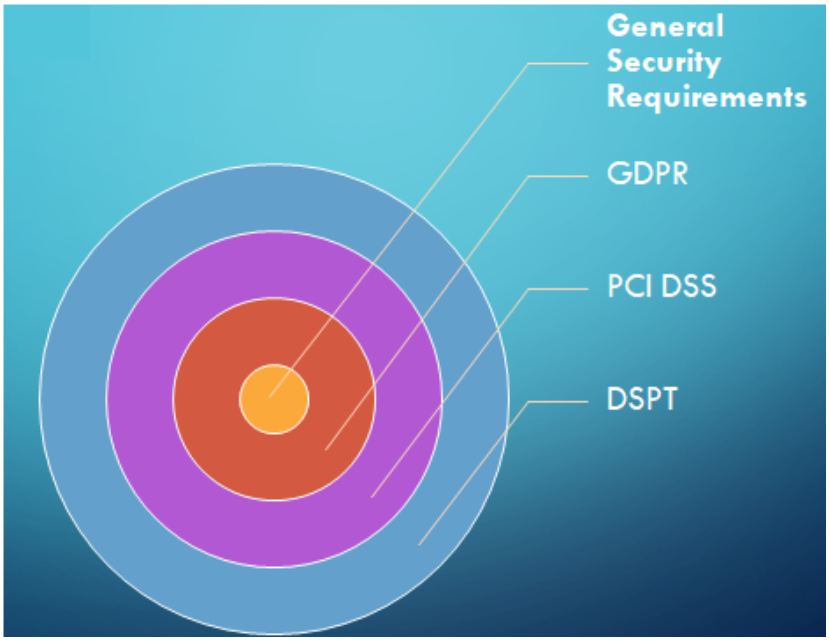

Figure 6. Merging of different requirements into the proposed HCYMAF.

3.3. Maturity Levels

The maturity model has its maturity levels. This means that each of the requirements and subrequirements has its own maturity levels. The maturity levels are 6 scores, from 0 to 5, with 0

being the lowest and 5 being the highest. Each of these maturity levels has a meaning, it represents a staged path for an organisation's performance and process improvement efforts based on predefined sets of practice areas. Each maturity level also builds on the previous maturity levels by adding new requirements. An example of such a scale is shown in Figure 7 below. A brief description of each level is presented:

- Level 0: Incomplete; Ad hoc and unknown. Work may or may not get completed.
- Level 1: Initial; Unpredictable and reactive. Work gets completed but is often delayed and over budget.
- Level 2: Managed; Projects are planned, performed, measured, and controlled.
- Level 3: Defined; the organisation is proactive, rather than reactive. There are organisation-wide standards that provide guidance across projects, programs, and portfolios.
- Level 4: Quantitatively Managed; the organisation is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.
- Level 5: Optimising; the organisation is focused on continuous improvement and is built to pivot and respond to opportunity and change.

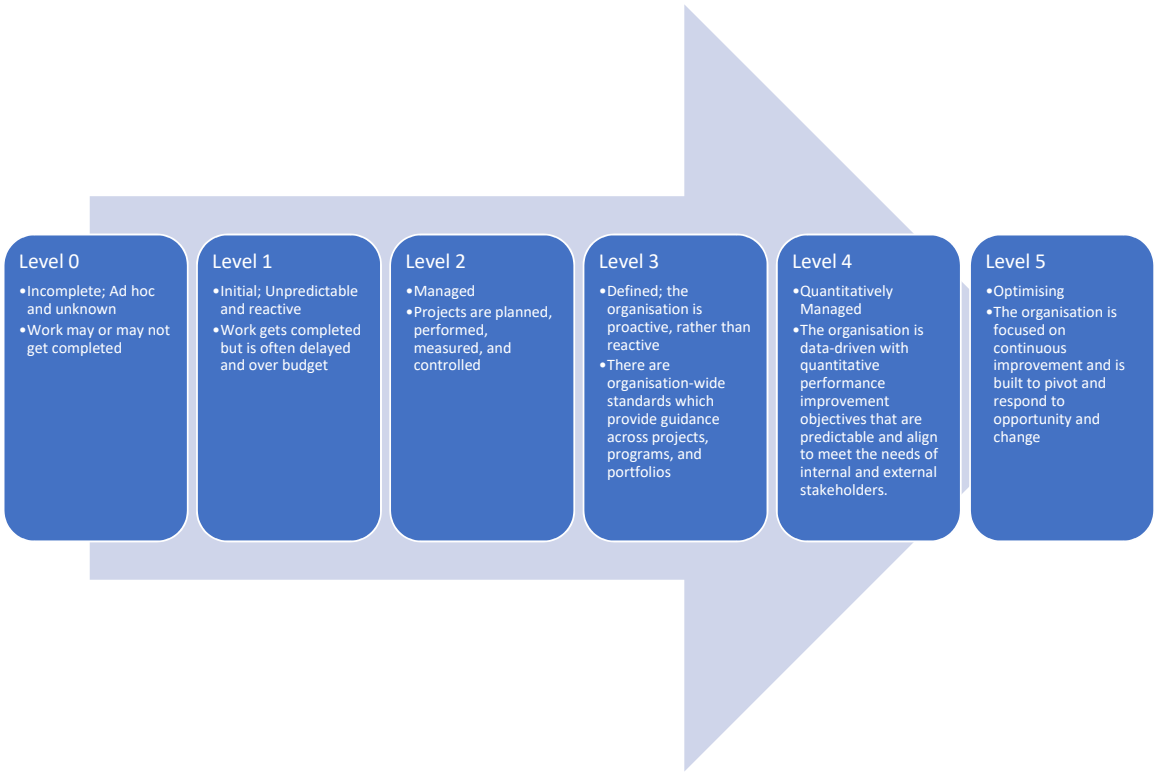

Figure 7. Maturity levels of the proposed model.

In terms of evaluation of the performance of an organisation against an individual requirement, the maturity notes should be read one at a time in ascending order (from 0 to 5). If all notes are fulfilled, then the next level should be read and examined. In order to assign a certain score, all of the lower levels must be completely fulfilled first. It should also be noted that some subrequirements have a Not Applicable (N/A) option, this is because not all subrequirements are applicable to every organisation.

3.4. Evaluation and Validation

The validation authenticates the contribution of the proposed maturity model, HCYMAF, as well as its usefulness, value, capability, and operational characteristics. A validation strategy was developed

to provide a convincing argument for the model's effectiveness and demonstrate its function within its proposed and realistic environment. It included the following:

- Interview with experts in the field of security and data protection of HEIs (DPO or Cyber Security Officers) in order to identify the different regulations that the HEIs must be compliant with, the best practices that they follow, how do organisations manage the overlap between cybersecurity and data protection (GDPR), the integration of Risk Management and the Privacy Impact Assessment among others. Apart from structured interviews that were sent to the experts, members of the team that developed the framework had many discussions. Using their advice and suggestions, the final groups and requirements were developed.
- A case study: The objectives of the case study that was conducted include the validation of the proposed structure and categories by adding or removing them from the model, which is expected to make advances to the model, and collect information related to the processes used to manage security in HEIs
- Feedback from the scientific community through the submission and presentation of academic papers—A number of research outputs will be produced alongside the study course which further enhances the validation of the research outputs.
- A webinar that will be organised and will take place later this year, where HEIs in the UK will be invited. During the webinar, the representatives of the HEIs will be given an overview of the framework, the results of the conducted case studies and the option to run the HCYMAF either offline (through a dedicated excel file and a detailed guide that we have developed) or online through our website.

Structured Interviews with Experts

1. What are the regulations that universities have to be compliant with?
2. Are universities in the UK obliged to have a security officer?
3. How do you conduct the DPIA and Risk Assessment? Do you do it in parallel or one after the other? Is data protection impact assessment under Risk Assessment?
4. Can you please briefly tell us the procedures you follow in order to be compliant with those regulations?
5. We have some categories that might not be applicable to universities, for example, 'security for software development'—what is your opinion?
6. How are the roles and responsibilities between the DPO and the security officer split?
7. How do you actually merge security requirements and Data Protection requirements during the implementation of a new service?
8. What is the procedure that is followed when a security or data breach takes place?
9. What would be the added value of a cybersecurity assessment framework? What would you expect from such a model?
10. We have created an initial pool of sectors that our HCYMAF is going to investigate. Do you think that we may miss any important category?

Before the final model is released to the HEIs, it should be validated through several pilot implementations. The model should preferably be used by organisations of different sizes and regardless of the activities they have, e.g., provide health studies. The first pilot has already been conducted, and the team at De Montfort University (DMU) in cooperation with the NCSC has already planned to run the other two cases in the next period. In the meantime, the DMU team has released the first version of the website which HEIs will use in order to perform self-assessments and receive the results in a graphical model and a gap analysis that showcases the cybersecurity sectors of HEI's IT systems that need immediate actions. Additionally, compliance reports will be produced automatically from the HCYMAF, giving the opportunity for the organisation to react fast and avoid penalties.

Each HEI representative will need to register to the platform and then go through the guide. The process can be paused and continued at a later time since a lot of information and time are needed in order to conduct a full cybersecurity assessment. The results for each organisation are only visible to the organisation along with charts and reports that will help the security and data-protection-officers to take the appropriate measures. Aggregated results will be collected and used for analysis by the NCSC in order to prioritise future security plans.

4. Discussion

Our proposed framework defines a set of metrics for measuring organisational competency or maturity in terms of a set of recognised best practices, skills, or standards. It incorporates the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Data Security and Protection Toolkit (DSPT), and can be used in order to conduct a gap analysis against 15 security requirements. The metrics are organised into categories and quantified on a performance scale. The measurable transitions between levels are based on empirical data that have been validated in practice, and each level in the model is more mature than the previous level.

By applying the proposed framework, organisations can achieve progressive improvements in their cybersecurity maturity by first achieving stability at the project level, then continuing to the most advanced-level, organisation-wide, continuous process improvement, using both quantitative and qualitative data to make decisions. For instance, at maturity level 2, the organisation has been elevated from ad hoc to managed by establishing sound security controls, procedures, and processes. As a university achieves the generic and specific goals at a maturity level, it is increasing its maturity and at the same time achieves compliance with relevant regulations and national laws.

Based on the experience we will gain out of this project, we will adapt the proposed HCYMAF for organisations in other sectors, e.g., water and power suppliers, in the future. We will incorporate the best practices, skills, or standards that are essential for different sectors. We also aim to create (working closely with the NCSC) a semiautomated self-assessment online framework. This online framework could be used by all critical organisations in the UK. The framework will include specific controls like IoT, SCADA, etc., where each organisation will fill the controls that are applicable to them. Finally, the information collected by this online tool will help the UK government to prioritise the mitigation plans related to security that need to be taken at a national level in terms of funding specific actions, launch new security tools, etc.

5. Conclusions

There have been a number of cyberattacks upon HEIs around the globe, and the recent JISC report reaffirmed that HEIs of the UK are not well prepared to defend against, or recover from, cyberattacks. Capability Maturity Models can enable organisations to benchmark current maturity levels against best practices. Although many maturity models have been already proposed in the literature, no model that integrates several regulations exists. Based on this finding, in this article we present a light, web-based model that can be used as a cybersecurity assessment tool for Higher Education Institutes (HEIs) of the UK that incorporates all security and privacy regulations and best practices that HEIs must be compliant with.

The proposed model consists of 15 security categories, six maturity levels, and is implemented on an online platform that can be used both as a self-assessment and audit tool, facilitating organisations to perform a gap analysis and to receive automated compliance reports and graphical representations of their security posture. Information that will be collected from the platform can be used, after proper aggregation and anonymisation processes from the NCSC, in order to identify current security problems and prioritise future security plans and funding actions.

Author Contributions: Conceptualization, A.A., Y.H., and L.M.; methodology, A.A., L.M., Y.H., and A.C.; software, A.A., I.Y., and L.M.; validation, H.J., E.B., A.C., and L.M.; formal analysis, A.A. and H.J., investigation, A.A., Y.H., and I.Y.; resources, A.A., Y.H., I.Y., and A.C.; data curation, A.A. and L.M.; writing—original draft preparation, A.A., Y.H., I.Y., and L.M.; writing—review and editing, E.B., H.J., and A.C.; visualization, A.A. and Y.H.; supervision, L.M. All authors have read and agreed to the published version of the manuscript.

Funding: We thankfully acknowledge the support of the NCSC, UK funded project (RFA: 20058).

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

References

1. Chapman, J.; Francis, J. *Cyber Security Posture Survey Results 2019*; Joint Information Systems Committee (JISC): London, UK, 2019.
2. Katz, F.H. The effect of a university information security survey on instruction methods in information security. In *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*; Association for Computing Machinery: New York, NY, USA, 2005; pp. 43–48.
3. Kim, E.B. Recommendations for information security awareness training for college students. *Inf. Manag. Comput. Secur.* **2014**, *22*, 115–126. [CrossRef]
4. Kaspersky, G.C.I. *Global Corporate IT Security Risks: 2013*; Kaspersky Lab: Moscow, Russia, 2013.
5. Aloul, F.A. The need for effective information security awareness. *J. Adv. Inf. Technol.* **2012**, *3*, 176–183. [CrossRef]
6. 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]
7. Cook, A.; Smith, R.; Maglaras, L.; Janicke, H. *Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure*; BCS: Belfast, UK, 2016.
8. Rajewski, J. Cyber Security Awareness: Why Higher Education Institutions Need to Address Digital Threats. 2013. Available online: https://www.huffpost.com/entry/cyber-security-awareness-_b_4025200 (accessed on 22 May 2020).
9. Maglaras, L.; Ferrag, M.A.; Derhab, A.; Mukherjee, M.; Janicke, H.; Rallis, S. Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures. *arXiv* **2019**, arXiv:1901.03899.
10. Butkovic, M.J.; Caralli, R.A. Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale. 2013. Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69187 (accessed on 22 May 2020).
11. Humphrey, W. Characterizing the software process: A maturity framework. *IEEE Softw.* **1988**, *5*, 73–79. [CrossRef]
12. Caralli, R.; Knight, M.; Montgomery, A. *Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability*; Technical Report; Carnegie-Mellon University, Software Engineering Institute: Pittsburgh, PA, USA, 2012.
13. Proença, D.; Borbinha, J. Information Security Management Systems—A Maturity Model Based on ISO/IEC 27001. In *Business Information Systems*; Abramowicz, W., Paschke, A., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 102–114.
14. Humphreys, E. *Implementing the ISO/IEC 27001: 2013 ISMS Standard*; Artech House: Washinton, DC, USA, 2016.
15. Brewer, D. *An Introduction to ISO/IEC 27001: 2013*; BSI Standard Limited: London, UK, 2013.
16. Barrett, M. *Framework for Improving Critical Infrastructure Cybersecurity*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
17. Sabillon, R.; Serra-Ruiz, J.; Cavaller, V.; Cano, J. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In Proceedings of the 2017 International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador, 23–25 November 2017; pp. 253–259.
18. Adler, R.M. A dynamic capability maturity model for improving cyber security. In Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 12–14 November 2013, pp. 230–235.

19. Almuhammadi, S.; Alsaleh, M. Information security maturity model for NIST cyber security framework. *Comput. Sci. Inf. Technol. CS IT* **2017**, *7*, 51–62.
20. Miron, W.; Muita, K. Cybersecurity capability maturity models for providers of critical infrastructure. *Technol. Innov. Manag. Rev.* **2014**, *4*, 33–39.. [CrossRef]
21. Akinsanya, O.O.; Papadaki, M.; Sun, L. *Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?* CERC: New Delhi, India, 2019; pp. 211–222.
22. Le, N.T.; Hoang, D.B. Can maturity models support cyber security? In Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016; pp. 1–7.
23. Akinsanya, O.O.; Papadaki, M.; Sun, L. Towards a maturity model for health-care cloud security (M2HCS). *Inf. Comput. Secur.* **2019**. [CrossRef]
24. Team, C.P. Capability maturity model® integration (CMMI SM), version 1.1. In *CMMI Product Team, "CMMI for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Staged Representation (CMMI-SE/SW/IPPD/SS, V1.1, Staged)"*; Technical Report CMU/SEI-2002-TR-012; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2002.
25. Keller, N. *CIS Controls Informative Reference Details*; NIST: Gaithersburg, MD, USA, 2019.
26. ENISA. *Guidelines on Assessing DSP Security and OES Compliance with the NISD Security Requirements*; European Union Agency For Network and Information Security: Heraklion, Greece, 2018.
27. Mbanaso, U.M.; Abrahams, L.; Apene, O.Z. Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. *Afr. J. Inf. Commun.* **2019**, 1–26. [CrossRef]
28. Butkovic, M.; Caralli, R. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale*; Technical Report CMU/SEI-2013-TN-028; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2013.
29. Markopoulou, D.; Papakonstantinou, V.; de Hert, P. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Comput. Law Secur. Rev.* **2019**, *35*, 105336. [CrossRef]
30. Lachaud, E. ISO/IEC 27701: Threats and Opportunities for GDPR Certification. 2020. Available online: https://research.tilburguniversity.edu/en/publications/isoiec-27701-threats-and-opportunities-for-gdpr-certification (accessed on 22 May 2020).
31. Hiller, J.S.; Russell, R.S. Privacy in crises: The NIST privacy framework. *J. Contingencies Crisis Manag.* **2017**, *25*, 31–38. [CrossRef]
32. Ferrag, M.A.; Maglaras, L.; Janicke, H. Blockchain and its role in the internet of things. In *Strategic Innovative Marketing and Tourism*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1029–1038.