Journal of Cybersecurity and Privacy

MDPI

Article

The Cybersecurity Focus Area Maturity (CYSFAM) Model

Bilge Yigit Ozkan [1,*], Sonny van Lingen [1] and Marco Spruit [2,3]

[1] Department of Information and Computing Sciences, Utrecht University, Princetonplein 5, 3584 CC Utrecht, The Netherlands; sonny200@hotmail.com

[2] Leiden Institute of Advanced Computer Science, Leiden University, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands; m.r.spruit@liacs.leidenuniv.nl or m.r.spruit@lumc.nl

[3] Public Health and Primary Care, Leiden University Medical Center, Campus The Hague, Turfmarkt 99, 2511 DP The Hague, The Netherlands

* Correspondence: b.yigitozkan@uu.nl

Received: 25 December 2020; Accepted: 4 February 2021; Published: 13 February 2021

Abstract: The cost of recovery after a cybersecurity attack is likely to be high and may result in the loss of business at the extremes. Evaluating the acquired cybersecurity capabilities and evolving them to a desired state in consideration of risks are inevitable. This research proposes the CYberSecurity Focus Area Maturity (CYSFAM) Model for assessing cybersecurity capabilities. In this design science research, CYSFAM was evaluated at a large financial institution. From the many cybersecurity standards, 11 encompassing focus areas were identified. An assessment instrument—containing 144 questions—was developed. The in-depth single case study demonstrates how and to what extent cybersecurity related deficiencies can be identified. The novel scoring metric has been proven to be adequate, but can be further improved upon. The evaluation results show that the assessment questions suit the case study target audience; the assessment can be performed within four hours; the organization recognizes itself in the result.

Keywords: cybersecurity; cybersecurity risk assessment; cybersecurity capability improvement; cyber-risks; cyber-attacks; design science research; standards

1. Introduction

The Global Risks Report 2020 revealed that cyberattacks rank seventh place in terms of likelihood and eighth place in terms of impact among the top 10 risks. In 2021, cybercrime damages are estimated to reach 6 trillion USD [1].

Almost daily, incidents prove that cybersecurity-related risks are high and both individual hackers and professionally organized cybercrime groups are responsible for these incidents [2,3]. Understanding the cybersecurity risks and possible countermeasures is of paramount importance due to both the likelihood and the impact of these risks. In the era of cyber-physical systems (CPS) and the Internet of Things (IoT), cybersecurity is beyond the scope of a particular organization. The consequences of cyber-attacks are often borderless and expand to societies. Recent research in cybersecurity put forward a diversity of areas to investigate, such as: transportation [4,5], IoT, CPS [6,7], and healthcare [8,9]. Nevertheless, due to the ever-changing nature of cyber-risks, and with the continual inclusion of new assets, organizations need a holistic and persistent approach to cybersecurity. The present research focuses on cybersecurity from an organizational perspective to help generic organizations tackle cybersecurity challenges.

Standards have been a trustworthy resource for those (individuals, organisations, governments, etc.) who seek the answer to the question "what is the best way of doing this?" [10]. As in every domain,

standards on cybersecurity and information security build on experience and best practices that may help organisations to cope with cyber threats.

As a result of the attention given to cybersecurity, there has been an abundance of scientific research with increasing intensity in this decade. However, little research has been performed in developing a standard-based process improvement framework. The small number of frameworks available are mostly based on the Capability Maturity Model (CMM) [11,12], but they received some critical remarks; mainly related to implementation costs, applicability, and reliability [13].

Previous scientific work has shown that focus area maturity models (FAMs) have several advantages as improvement frameworks [14]. Furthermore, focus area maturity modelling has been shown to be suitable for developing a valid maturity model ISFAM (Information Security Focus Area Maturity) model [15]. ISFAM focuses on information security capabilities. In this paper, the authors provide a holistic view of all security domains—information security, cybersecurity, network security, application security, etc.—and their relationships. The aim is to propose a comprehensive cybersecurity capability coverage to accompany information security capabilities.

The present research aims to answer the following research question: "How can cybersecurity capabilities for generic organisations be modelled in a focus area maturity model?" This paper presents the CyberSecurity Focus Area Maturity (CYSFAM) model that was developed using the method presented by [14]. Amongst several existing cybersecurity maturity models, CYSFAM has distinctive characteristics; it is mainly based on international standards and frameworks, it is intended for generic organisations and it is structured as a focus area maturity model—the only cybersecurity focus area maturity model. The present paper contributes to the cybersecurity maturity modeling body of knowledge as a mainly standard-based focus area maturity model for generic organizations. Using CYSFAM, practitioners can assess and improve their cybersecurity capabilities with the help of 144 assessment questions/capabilities categorized into 11 focus areas. The paper presents an overarching approach to cybersecurity that can enable organizations to see the broad view on cybersecurity domain. The analysis and the visual presentation of the dependencies between the capabilities facilitate capability improvement planning.

The rest of the paper is organized as follows: first, the related work on security domains, existing information security and cybersecurity maturity models, the concept and design of FAMs, and the ISFAM are introduced. Second, the design science research framework and methodology applied for artifact development are described. Third, CYSFAM is presented. Fourth, the evaluation of the model and its results are presented. Fifth, the findings are discussed. Lastly, conclusions are drawn and the areas for future research are given.

2. Related Work

In this section, firstly, cybersecurity and its relationship with other security domains are discussed. Secondly, the information and cybersecurity maturity models found in the literature are presented. Thirdly, standard categories, information security and cybersecurity standards for generic organisations are discussed. Fourthly, the perspective and design of FAMs are presented. Lastly, ISFAM is presented.

2.1. Cybersecurity and Other Security Domains

There are gaps and overlaps in the definition of cybersecurity in standardisation [16]. In the analysis of several standards and the definitions provided by the cybersecurity-related technical committees of standards developing organizations (SDOs), the following definition can be derived: cybersecurity is protecting the confidentiality, integrity, and availability of assets in cyberspace from cyber-attacks. Cyberspace is an environment of interconnected computers, devices, electronic communications systems and services, wire communication, and electronic communication, including the information contained therein [16]. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) recognizes a distinct relationship between cybersecurity and other security-related domains [17]. This relationship can be modelled as shown in Figure 1,

which depicts both the relationships of the security domains and the standards ISO/IEC has published specifically for these domains.

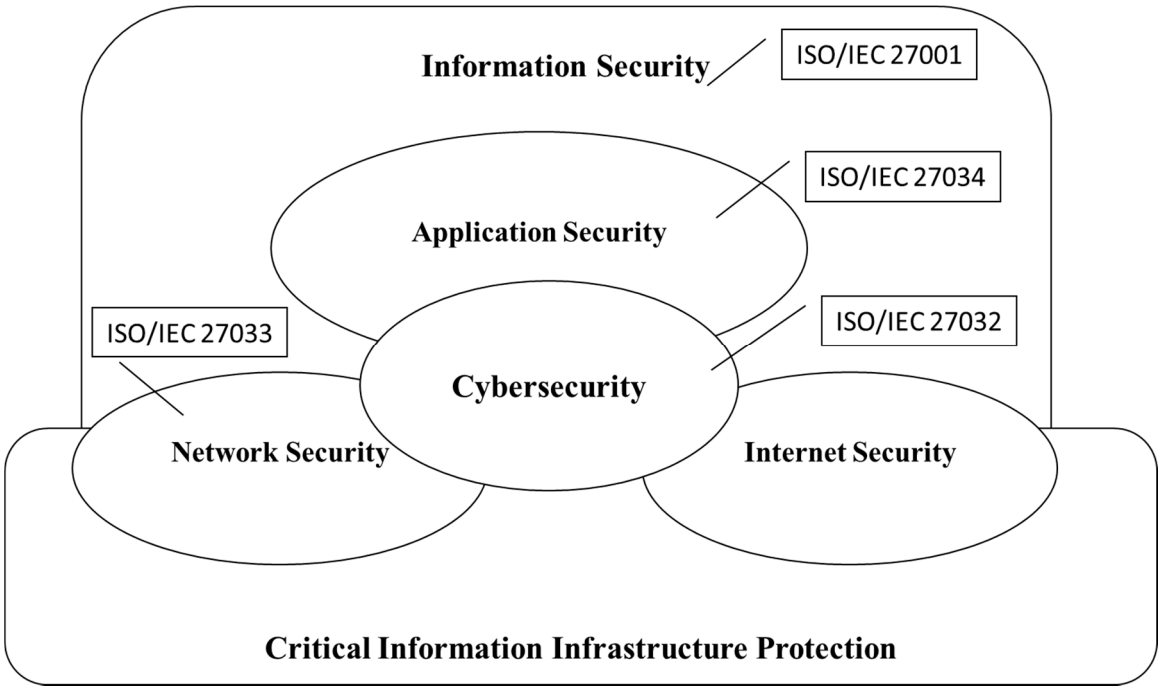

Figure 1. Relationship between cybersecurity and other security domains and the related standards (redrawn from International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27032 [17]).

2.2. Information Security and Cybersecurity Standards

Standards can be categorized into five groups according to their publishers as follows [18]:

1. International standards are developed by international SDOs and made available to the public, possibly at cost. ISO (International Organization of Standardization) standards are the most well-known ones.
2. Regional standards are adopted by a number of nations in a particular region. European Committee for Standardization (CEN) standards are examples of this category.
3. National standards are developed for use in a particular country.
4. Industry standards are adopted by a particular industry for common use. An example is the Security Industry Association (SIA) standard.
5. Proprietary or company standards are constructed by organizations (mainly commercial) with little to no attention to external parties.

In order to help to improve general awareness on standardization, certification, and labelling in cybersecurity, the European Cybersecurity Organisation (ECSO) published an overview of existing cybersecurity standards and certification schemes [19]. Given the extensive number of domain-related standards, this document helps organisations and individuals to address the relevant standards easily.

In this state of the art syllabus document, ECSO not only focuses on the standards specific to sectors, but also the standards applicable to generic organisations. The generic organisations in this sense are those not associated with any particular industry vertical (e.g., energy, healthcare, and telecom). It should be noted that the standards applicable to generic organisations are also perfectly applicable to industry verticals but may not include the sector-specific requirements.

Table 1 lists the ISO standards for generic organisations provided in the overview of cybersecurity standards [19]. The first column presents the related security domain or topic. Compared to Figure 1, this list includes additional standards: privacy, incident management, and supplier relationships security.

Table 1. Cybersecurity standards for generic organisations published by ISO [19].

Security Domain/Topic	Standard	Reference
Information security	ISO/IEC 27001:2013—Information technology—Security techniques—Information security management systems—Requirements	[20]
Cybersecurity	ISO/IEC 27032:2012—Information technology—Security techniques—Guidelines for cybersecurity	[17]
Network security	ISO/IEC 27033-1:2015—Information technology—Security techniques—Network security—Part 1: Overview and concepts	[21]
Application security	ISO/IEC 27034-1:2011—Information technology—Security techniques—Application security—Part 1: Overview and concepts	[22]
Incident management	ISO/IEC 27035-1:2016—Information technology—Security techniques—Information security incident management—Part 1: Principles of incident management	[23]
Supplier relationships security	ISO/IEC 27036-1:2014—Information technology—Security techniques—Information security for supplier relationships—Part 1: Overview and concepts	[24]
Privacy	ISO/IEC 29100:2011—Information technology—Security techniques—Privacy framework	[25]

2.3. Information Security and Cybersecurity Maturity Models

Previous studies have investigated information security and cybersecurity maturity models [26–28]. These maturity models have different focuses according to their purpose and target. Some examples of purpose and target for the existing maturity models are critical infrastructures, generic organisations, and cybersecurity workforce planning [29]. Among the information security and cybersecurity maturity models in the literature, ISFAM [15] is the only focus area maturity model, and it is based on widely-implemented industry standards. This model is elaborated upon in Section 2.5. There is no previously developed focus area cybersecurity maturity model in literature. We believe the capability interdependency presentations in focus area maturity models have the benefit of providing organisations with guidance for capability implementation planning.

In Table 2, we present the comparison of several information security and cybersecurity maturity models. The list of the maturity models presented in Table 2 is as follows:

- CYSFAM: The Cybersecurity Focus Area Maturity Model introduced in the present paper.
- C2M2: Cybersecurity Capability Maturity Model [30].
- SSE-CMM: System Security Engineering Capability Maturity Model [31].
- NICE: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [32].
- O-ISM3: The Open Group Information Security Management Maturity Model [33].
- ISFAM: The Information Security Focus Area Maturity Model [15].

The features in Table 2 are briefly explained as follows:

Cybersecurity-focused: This feature shows whether the maturity model is designed to cover the cybersecurity domain. It is obvious for the information security maturity models that they are not focused on cybersecurity but information security.

FAM or CMM: This feature shows whether the maturity model is of focus area maturity model type (FAM) or capability maturity model type (CMM).

Target sector: This feature shows whether the maturity model's target audience is a specific sector or any generic organization.

Table 2. Comparison of the features of information security and cybersecurity maturity models.

Features	CYSFAM	C2M2 [30]	SSE-CMM [31]	NICE [32]	O-ISM3 [33]	ISFAM [15]
Cybersecurity-focused	Yes	Yes	No	Yes	No	No
FAM or CMM	FAM	CMM	CMM	CMM	CMM	FAM
Target sector	Generic	Critical infrastructures	Security engineering	Workforce	Generic	Generic
Incorporates standards	Mainly	Partly	No	No	Partly	Mainly
Analysis of interdependencies between the processes/capabilities	Yes	No	No	No	No	Yes

Incorporates standards: This feature shows whether the maturity model incorporates processes or capabilities derived from standards. *Mainly* means that most of the capabilities or the processes are derived from standards. *Partly* means some of the capabilities or the processes are derived from standards. As the development phases of all of the maturity models in Table 2 are not clearly known to us, our decisions for this feature were based on available information on the maturity model.

Analysis of interdependencies between the processes/capabilities: This feature shows whether the maturity model provides an analysis of interdependencies between the processes and capabilities. The FAMs entail this feature by design, whereas CMMs only state that lower-level processes are to be implemented before higher-level processes.

The characteristics of CYSFAM in comparison to existing alternatives can be seen in Table 2. CYSFAM has the following advantages: focusing on cybersecurity of generic organisations, being mainly based on standards, and showing the interdependencies between capabilities to facilitate implementation planning.

2.4. Focus Area Maturity Models (FAMs)

FAMs were first proposed by Koomen and Pol [34]. Steenbergen et.al. notably formalized and provided a process deliverable diagram to develop this type of maturity model. In the present paper, we followed the process presented by Steenbergen et.al. [14]. We elaborately present the development steps of CYSFAM (the artifact) in Section 4. An FAM aims to provide complete coverage of the domain for which it is designed by presenting the capabilities the domain entails and positioning the capabilities in a matrix relative to each other according to their dependencies [29].

FAMs consist of several focus areas. Each focus area comprises unique capabilities (2–6) that are indicated with a capital letter [35]. The building block of an FAM, a capability, is defined as "an ability to achieve a predefined goal that is associated with a certain maturity level" [14].

2.5. ISFAM: The Information Security Focus Area Maturity Model

ISFAM [15] is the only existing FAM on information security within the literature. ISFAM's broad coverage comes from its 13 focus areas, 51 information security capabilities, and 161 statements that are derived from well-known industry standards. ISFAM was proposed to help organisations, especially small and medium-sized enterprises (SMEs), achieve strategy-information technology (IT) security alignment in ever-changing security risk environments [15].

3. Materials and Methods

The design science research (DSR) paradigm has been promoted as an information systems (IS) research paradigm and recognised to improve the relevance and rigor of IS research [36]. Design science research aims at the development of artifacts in the form of different types of constructs (i.e., concepts, methods, models). In the present research, the artifact of the research is CYSFAM. Various methodologies have been proposed to support DSR [37,38]. In the present research, we follow the steps proposed by Peffers et al. [37]. Following this DSR methodology, our research includes realising a problem situation, reviewing the literature, identifying the cybersecurity focus areas and capabilities, identifying the dependencies and positioning the capabilities in the maturity matrix, developing the scoring mechanism for capability assessment, evaluating CYSFAM with domain experts, demonstrating CYSFAM in a case study company, and communicating the research objectives, structure and results to the other researchers.

To provide a better understanding of our research context, our research framework based on Hevner et al. is depicted in Figure 2 [36].

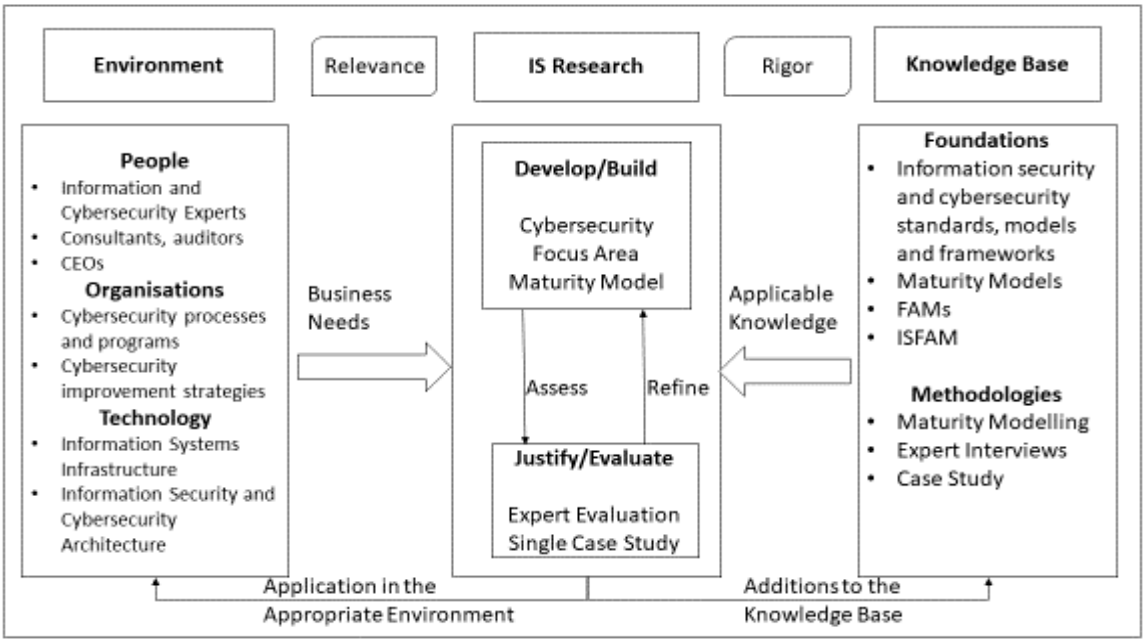

Figure 2. Research Framework based on Hevner et al. [36].

4. Artifact Development

This section presents the development steps of CYSFAM (including the literature search, the process of identifying the focus areas and the capabilities).

4.1. Identifying the Initial Set of Focus Areas, Relevant Standards and Frameworks

To identify the focus areas, the authors used international standards that characterize the cybersecurity domain. Due to their high level of usage and acceptance, the standards published by ISO were used to compose the initial list of cybersecurity focus areas. As described in Section 2, the authors relied on the standards (see Figure 1) presented in the main cybersecurity standard from ISO: ISO/IEC 27032-Cybersecurity guidelines. In addition, the authors included the ISO/IEC 27035- Information security incident management standard as it is related to all security domains. Incident management is also covered as the "Framework of information sharing and coordination" in ISO/IEC 27032. The final list that the investigation of the focus areas involved is given in Table 3.

Table 3. Baseline of cybersecurity standards to identify the initial set of focus areas.

Standard	Reference
ISO/IEC 27032:2012—Information technology—Security techniques—Guidelines for cybersecurity	[17]
ISO/IEC 27033-1:2015—Information technology—Security techniques—Network security—Part 1: Overview and concepts	[21]
ISO/IEC 27034-1:2011—Information technology—Security techniques—Application security—Part 1: Overview and concepts	[22]
ISO/IEC 27035-1:2016—Information technology—Security techniques—Information security incident management—Part 1: Principles of incident management	[23]

The relationship model of cybersecurity with other security domains (Figure 1) shows that cybersecurity has intersections with application security and network security. To discover these intersections, the authors included the corresponding ISO standards in their investigation. The information security standard (ISO/IEC 27001, [20]) was excluded since this domain was already covered in ISFAM (see Section 2). Internet security is regarded as an extension of network security and no specific standard

was mentioned for this domain [17]. The authors also performed a search on ISO's website by using the keyword "internet security", resulting in no dedicated standard. As the research question addresses generic organisations, the standards for critical infrastructure security were not included.

The initial set of focus areas identified in this first iteration are listed in Table 4.

Table 4. The initial set of focus areas of CYSFAM.

Focus Area	Reference
Server protection (elaborated upon in ISO/IEC 27032)	[17]
End-user controls (elaborated upon in ISO/IEC 27032)	[17]
Controls against Social Engineering (elaborated upon in ISO/IEC 27032)	[17]
Network security (the main focus of ISO/IEC 27033)	[21]
Application security (the main focus of ISO/IEC 27034)	[22]
Cyber/Information Security Incident Management (the main focus of ISO/IEC 27035)	[23]

In the second iteration, the references in the standards (Table 3) were analysed. Additional standards and frameworks identified in this iteration are given in Table 5.

Table 5. Standards and frameworks identified after analysing the reference sections. ITU, International Telecommunication Union; ISA, International Society of Automation; NIST, National Institute of Standards and Technology; NERC, North American Electric Reliability Corporation.

Standard or Framework	References
ITU-T ICT Security Standards Roadmap	[39]
Guidebook on National Cyber Security Strategies	[40]
ISA/IEC-62443	[41]
NIST 800-12 and NIST 800-14	[42,43]
NERC Critical Infrastructure Protection (CIP) Standards	[44]
NERC Security Guidelines	[45]

Finally, a multi-vocal (scientific and grey) literature search was performed to gather relevant articles with the details depicted in Table 6.

Table 6. The search platforms and the keywords used in the literature search.

Search Platforms	Most Prominent Keywords
Google Scholar	[information/cyber] security frameworks
Google	[information/cyber] security risks
Mendeley	[information/cyber] security controls
CIO.com	[information/cyber] security vulnerabilities
Gartner	[information/cyber] security maturity model
	[information/cyber] security capability

A number of inclusion criteria were defined in this focused literature search:

- Articles have to be written in the English language.
- Articles have to originate from a trustworthy source (e.g., a professional, specialized organization).
- Articles have to be published in the year 2010 or later.
- Articles have to be accessible without cost (note that institutional subscriptions were used).

Table 7 presents the results of this literature search.

Table 7. The standards and frameworks that were identified after the literature search. NIST, National Institute of Standards and Technology; IASME, Information Assurance for Small and Medium-Sized Enterprises; ISF, Information Security Forum.

Standard or Framework	Reference
Critical Security Controls for Effective Cyber Defense	[46]
Cyber Security Self-Assessment Guidance	[47]
NIST 800-53	[48]
Cybersecurity Capability Maturity Model (C2M2)	[30]
The IASME Governance Standard for Information and Cyber Security	[49]
A Maturity Model for Enterprise Key Management	[50]
ISF Standard of Good Practice for Information Security	[51]
Guidelines for Managing the Security of Mobile Devices in the Enterprise	[52]
Guide to Enterprise Patch Management Technologies	[53]

4.2. Defining the Cybersecurity Focus Areas and Capabilities

The following steps were followed to identify the cybersecurity focus areas and capabilities.

1. The findings from the ISO/IEC 2703x were translated to an initial number of focus areas (Table 4).
2. The additional 15 standards and frameworks (Tables 5 and 7) were analysed and translated to a number of focus areas. These standards and frameworks were to identify the focus-areas that the ISO/IEC standards did not explicitly have in scope. This led to a long list of focus areas (77 in total) that could serve as an augmentation of CYSFAM.
3. This long list of candidates CYSFAM focus areas was analysed to define the final set of CYSFAM focus areas. Within this set of focus areas, the decision to either adopt or exclude a focus area was based on the following criteria.
    - The focus area is meaningful to CYSFAM; it concerns a cybersecurity-related area.
    - The focus area is not yet adequately represented in existing focus areas in the ISFAM (see Section 2) or CYSFAM.
    - The focus area is not specific to a particular domain or organization-type; it serves a broad range of organizations.

After the deduction process, the complete list of CYSFAM focus areas (11 in total) was established as shown in Table 8.

4. The next step was to determine the capabilities under each focus area by analysing the resources that led the authors to the focus areas. The number of capability statements identified for each focus area and related standards, models, and frameworks are given in Table 8. The total number of capability statements was 144.

Table 8. Focus areas of CYSFAM and reference standards, models, and frameworks.

#	Focus Area	Number of Capability Assessment Questions	Standard/Model/Framework
1	Server protection	16	ISO/IEC 27032 [17], The ISF Standard of Good Practice for Information Security [51,53]
2	End-user controls	15	ISO/IEC 27032 [17]
3	Controls against Social Engineering	7	ISO/IEC 27032 [17]
4	Network security	12	ISO/IEC 27033 [21]
5	Application security	8	ISO/IEC 27034 [22]
6	Cybersecurity Incident Management	16	ISO/IEC 27035 [23]
7	Cybersecurity awareness	16	Security Awareness Roadmap [54], ISO/IEC 27001 [20]
8	Cryptography	16	A Maturity Model for Enterprise Key Management [50]
9	Cybersecurity governance	14	Cyber Security Self-Assessment Guidance [47]
10	Mobile security	16	Guidelines for Managing the Security of Mobile Devices in the Enterprise [52]
11	Vulnerability management	**8**	Critical Security Controls for Effective Cyber Defense [46]

4.3. Identifying the Dependencies and Positioning the Capabilities in the Maturity Matrix

Another step in developing CYSFAM was to identify the dependencies of the capabilities and positioning them in a maturity matrix. Some capabilities in CYSFAM required that one or more other capabilities, either in the same focus area or in another focus area, be implemented first.

In this section, first, dependencies between the capabilities are explained. Second, a matrix that presents the dependencies visually is presented.

The paragraphs below describe the dependencies of the capabilities and the arguments of these dependencies.

Establishing cybersecurity capabilities in an organisation starts with management commitment. The management should allocate resources for further implementations of cybersecurity capabilities [20]. The first capability to be implemented is, therefore, capability A of Cybersecurity Governance.

Capability B of Cybersecurity Governance follows next. With this capability, the roles and responsibilities within the organisation are defined. This capability enables all the other organisational capabilities to be implemented. Regarding the technical capabilities, network security should be implemented before every other technical control in cyberspace can be implemented. Therefore, Network Security capability A enables the other technical capabilities.

Cybersecurity Governance C requires serious security breaches to be escalated is, therefore, it is dependent on Incident Management B. Incident Management B requires incident response teams to receive vulnerability information from reliable sources. This constitutes a dependency on Vulnerability Management B. Mobile Security A requires an employee awareness program, therefore, it is dependent on Cybersecurity Awareness A.

Social Engineering Controls C requires a training and awareness program; therefore, it is dependent on Cybersecurity Awareness capability B. End-user Control B requires the measurement of patch delays; therefore, it is dependent on Server Protection A.

Cryptography A requires secure application development practices and, therefore, it is dependent on Application Security A. Application Security B requires awareness training for the development staff; therefore, it is dependent on Cybersecurity Awareness A.

Incident Management C requires specialised training for the CIRT (Critical Incident Response Team) members; therefore, it is dependent on Cybersecurity Awareness B. Social Engineering Controls

D requires social engineering risks to be incorporated in the organisation's risk assessments; therefore, it is dependent on Cybersecurity Governance capability D.

Server Protection D requires that the technical compliance checking solution is connected to the organizations' incident management system; therefore, it is dependent on Incident Management B.

The dependencies are presented in Table 9. The "From Capability" column shows the prerequisite capability and the "To Capability" column shows the dependent capability.

Table 9. Dependencies of the capabilities in CYSFAM.

#	Prerequisite Capability	Dependent Capability
1	Cybersecurity Governance A	Cybersecurity Governance B
2	Cybersecurity Governance B	Network Security A
3	Cybersecurity Governance B	Social Engineering Controls A
4	Cybersecurity Governance B	Incident Management A
5	Cybersecurity Governance B	Cybersecurity Awareness A
6	Network Security A	Server Protection A
7	Network Security A	End-user Controls A
8	Network Security A	Application Security A
9	Network Security A	Cryptography A
10	Network Security A	Mobile Security A
11	Network Security A	Vulnerability Management A
12	Incident Management B	Cybersecurity Governance C
13	Vulnerability Management B	Incident Management B
14	Server Protection A	Vulnerability Management B
15	Cybersecurity Awareness A	Mobile Security A
16	Cybersecurity Awareness B	Social Engineering Controls C
17	Server Protection A	End-user Controls B
18	Application Security A	Cryptography A
19	Cybersecurity Awareness A	Application Security B
20	Cybersecurity Awareness B	Incident Management C
21	Cybersecurity Governance D	Social Engineering Controls D
22	Incident Management B	Server Protection D

In the next step, the dependencies were positioned in a maturity matrix. Following the rules proposed by [14], capabilities that are dependent on other capabilities were always positioned further to the right. The resulting matrix is presented in Figure 3. Blue arrows in Figure 3 visually show the dependencies.

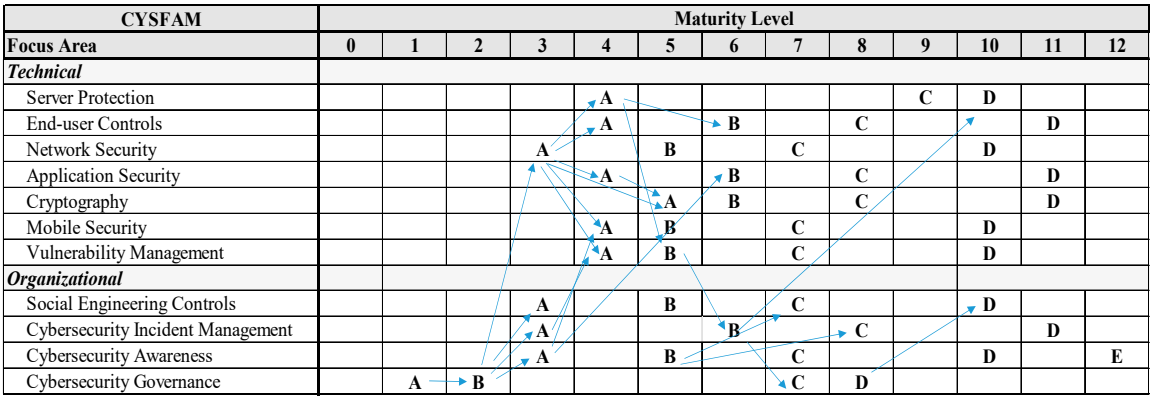

Figure 3. CYSFAM maturity matrix and dependencies of the capabilities: The letters (A–E) represent the capabilities; arrows (in blue) depict the dependencies.

In Figure 3, two categories are used for grouping the focus areas to increase the understandability of the model. The "Organizational" category includes capabilities related to non-technological factors,

processes, risk management, and human factors. A large body of literature has investigated the role of human factors and awareness on information security or cybersecurity [55–57]. The "Technical" category comprises focus areas that require technical capabilities to become mature.

4.4. Focus Area Scoring

There have been some signals that the scoring mechanism that is currently used in ISFAM [15] has a deficiency. This deficiency relates to the rigid manner the achievement of the maturity level per capability is calculated. According to [15], every question within a capability has to be answered with "yes" before the entire capability is marked as achieved. For instance, when three out of four metrics in capability A have been answered with "yes", capability B can never be achieved.

To resolve this inequity, which could even lead to reduced accuracy in scoring the focus area maturity levels, CYSFAM makes use of an alternative, experimental scoring mechanism. Since alternative scoring mechanisms for FAMs are lacking in the literature (except perhaps for [58]), we propose one on the basis of our expert opinion and on a best-effort basis. The scoring mechanism of the CYSFAM works as follows:

- Every achieved step A capability represents a worth of 0.25.
- Every achieved step B capability represents a worth of 0.5.
- Every achieved step C capability represents a worth of 0.75.
- Every achieved step D capability represents a worth of 1.
- Every achieved step E capability represents a worth of 1.25.

The mechanism follows a number of preconditions:

- If the assessment of any focus area results in a total score that has decimals behind the point, the score is rounded to its nearest natural number.
- A value of 0.25 is subtracted per unachieved capability at a previous level, when at least one of the capabilities from a higher level is met.

5. Results

This section presents CYSFAM with a focus area example.

Focus Area Example: Server Protection

This subsection describes the process for determining the capabilities of the "Server Protection" focus area.

According to ISO/IEC 27032 [17], server protection entails the protection of servers against unauthorized access and hosting of malicious content. Capabilities found for the "Server Protection" focus area are listed in Table 10. As shown in Table 8, the "Server Protection" focus area has 16 capability statements within these capabilities.

Table 10. Initial set of capabilities for server protection focus area.

Capability	Reference
Configuration according to a baseline security configuration	ISO/IEC 27032 [17]
Testing and deployment of updates for the server operating system and the applications	[53]
Implementing security incident event monitoring (SIEM)	[51]
Implementing technical state compliance monitoring (TSCM)	[51]

These capabilities were represented in levels of maturity (A–D), as shown in Table 11. In the CYSFAM—conforming to the design principles of FAMs [14]—the capabilities are depicted by letters, where a letter that is higher in the alphabetical order implies a higher level in the evolutionary maturity path.

Table 11. The final set of capabilities for server protection focus area.

Capability Statements	Capability
1. The organization's baseline security configuration is described. 2. Patch management is tool-supported (patch-management suites). 3. A SIEM solution is in place. 4. A technical compliance checking solution is in place.	A
1. The baseline security configuration is based on an open standard. 2. The deployment of patches is tested and approved at least once before deployment in the production environment. 3. The SIEM implementation is based on a baseline set of events. 4. Technical compliance checking is performed manually (supported by appropriate tools).	B
1. The baseline security configuration is reviewed at least once a year. 2. A process is in place that assures the organizations learns about patch releases as soon as possible. 3. The SIEM implementation includes events that were identified during a risk assessment. 4. Technical compliance checking is performed with the assistance of automated tools (with a reporting functionality).	C
1. The baseline security configuration is updated after every significant configuration change or demonstrated vulnerability. 2. The prioritization of patches is risk-based; the business cruciality is taken into account. 3. The SIEM solution is connected to a security operations center (SOC) for a correlation of events and is connected to the organization's incident management system. 4. The technical compliance checking solution is connected to the organizations' incident management system.	D

The other 10 focus area (Table 8) capabilities were developed following the same approach.

The final CYSFAM focus areas and capabilities are depicted in Figure 4. The coloured cells show the highest possible capabilities identified in the model.

CYSFAM	Maturity Level												
Focus Area	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Technical													
Server Protection					A					C	D		
End-user Controls					A		B		C			D	
Network Security				A		B		C			D		
Application Security					A		B		C			D	
Cryptography						A	B		C			D	
Mobile Security					A	B		C			D		
Vulnerability Management					A	B		C			D		
Organizational													
Social Engineering Controls				A		B		C			D		
Cybersecurity Incident Management				A			B		C			D	
Cybersecurity Awareness				A		B		C			D		E
Cybersecurity Governance		A	B					C	D				

Figure 4. Focus areas and capabilities of CYSFAM. The letters (A–E) represent the capabilities; shaded areas show the maximum capability in the corresponding focus area.

All of the focus areas and 144 capability statements/assessment questions for the capabilities included in the model were published in a technical report which is openly accessible [59].

6. Evaluation

In this section, the evaluation of CYSFAM by means of both expert evaluations and a case study is described. In this research, two interviews were conducted with the aim of expert evaluation.

The evaluations of the experts were incorporated in CYSFAM, and this improved version was used in the case study.

6.1. Expert Evaluation and Results

In a mixed-methods qualitative research engagement, expert interviews are a very suitable and fruitful way to establish construct validity as discussed by [60]. Therefore, it was decided to evaluate CYSFAM by means of expert evaluations. The selection criteria for the experts were as follows:

- The interviewee is experienced in the information or cybersecurity domain—a minimum of 5 years of experience is required.
- The interviewee is capable of thinking outside of the context of the case study company.
- The interviewee can prove their knowledge by providing Certified Information Systems Security Professional (CISSP) certification [61].

Two suitable domain experts were approached to participate in the evaluation.

The first interviewee was an IT security expert who had 15 years of experience and was working at the case study company at the time of the interview was conducted. The second interviewee was an external IT security consultant who was specialized in security in large organizations. Both interviewees had CISSP certification. CYSFAM and the methods applied to develop the CYSFAM were introduced to the interviewees. The interviewees evaluated CYSFAM in separate sessions without the researchers' intervention. Finally, they provided the researchers with their evaluation results.

Interviews with the experts resulted in the following most important remarks:

1. CYSFAM entirely lacks a module on security in Cloud Computing, which is one of the most prevalent security concerns for now and in the upcoming years. That certainly needs to be included in the final model.
2. The scoring method is hard to grasp and, in its rigidness, it is somewhat harsh. However, compliance agencies and auditors are usually also harsh; thus, that warrants such a setup.
3. CYSFAM is very control-based. It would be an idea to introduce two dimensions per focus area: control-based and process-based (or process maturity).
4. CYSFAM contains quite some jargon. That is not necessarily an issue, but you need to be clear about the intended target audience of CYSFAM (security experts, rather than management—upper level or not).
5. There are a number of capabilities that could be better rephrased in CYSFAM.

The authors addressed these remarks as follows: for remark #1, cloud computing was investigated in depth with regard to the security-related capabilities and controls that are in place. The results of this investigation showed that, considering the range of this topic, a cloud security maturity model could very well be an extensive maturity model on its own. Recently, a study on cloud computing security maturity modelling addressed this gap in the literature [62]. Since cloud security computing was considered as reasonable to be a separate maturity model, it was not incorporated as a focus area in CYSFAM. For remarks #2 and #3, there were obvious limitations (lack of knowledge, resources) to not include them in this version of CYSFAM. They do, however, form important challenges for future research engagements. Remark #4 is inherent to the design and scope of this study; cybersecurity is a domain that is largely embraced by technical specialists, rather than management and directors. The improvements proposed along with remark #5 were incorporated in CYSFAM. The authors went through six improvement proposals of the experts–three by each expert– and a common one proposed by both experts. All seven improvements were reflected in the capabilities.

6.2. Case Study and Results

The following requirements concerning the case study company were identified (inspired by [63]):

- The case study company is sufficiently large; there is a grounded possibility that the concepts found in the literature are part of the case study company's routine.
- The case study company is active in a "security-sensitive" domain; the case study company manages and/or governs systems usually containing data that are of value.
- The case study company can provide the resources (time, money) and the conditions (culture) which are required to carry out the research.

The case study was conducted at a Western European bank, which almost perfectly met the conditions described above.

CYSFAM is considered to be successful if the following points can be verified (partly inspired by [15]:

- CYSFAM assessment can be performed within a 4 h timeframe provided that the conditions are suitable (timely communication with experts where needed is guaranteed).
- The questions make sense—at least to information and cybersecurity domain experts. This is the most significant target audience for CYSFAM, notwithstanding that other information technology professionals could consider CYSFAM beneficial.
- The case study organization recognizes itself in the assessment results.

Considering the verification points described above, it can be concluded that the assessment of CYSFAM during the case study was proven to be successful. The organisation's experts were able to answer all the questions within four hours. The end-result of the assessment reflects the cybersecurity maturity stage that the organization is currently in, i.e., effort has been put into improving cybersecurity; however, there is a lot of work to be done, whereas the optimal stage of maturity is not in sight yet. The assessment results are depicted in Figure 5. As can be seen from this figure, the cells shaded present the capabilities achieved by the organisation.

CYSFAM	Maturity Level												
Focus Area	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Technical													
Server Protection					A					C	D		
End-user Controls					A		B		C			D	
Network Security				A		B		C			D		
Application Security					A		B		C			D	
Cryptography						A	B		C			D	
Mobile Security					A	B		C			D		
Vulnerability Management					A	B		C			D		
Organizational													
Social Engineering Controls				A		B		C			D		
Cybersecurity Incident Management				A			B		C			D	
Cybersecurity Awareness				A		B		C			D		E
Cybersecurity Governance		A	B					C	D				

Figure 5. The outcome of the CYSFAM assessment within the case study organization. The letters (A–E) represent the capabilities; shaded areas show the maximum capability achieved for the corresponding focus area.

The evaluation results are further discussed in the next section.

7. Discussion

In this research, the authors identified the cybersecurity focus areas and capabilities by using standards, frameworks, and other resources resulting from the literature search. These focus areas and capabilities were then structured to develop a maturity model conforming to the design principles of focus area maturity models.

The different security domains and their relationships according to the ISO/IEC 27032—cybersecurity guidelines—[17] were discussed in the Section 2. CYSFAM incorporates cybersecurity, application security, and network security but not information security domains. The information security domain incorporates a number of cybersecurity capabilities (see Figure 1); however, information security capabilities offer insufficient depth and perspective for exploring cybersecurity capabilities. Therefore, in this research, cybersecurity standards, frameworks and models were investigated thoroughly.

To evaluate CYSFAM, both expert interviews and a case study were conducted. The expert evaluations led to several improvements that were discussed in Section 6. As a result of the case study, a number of the cybersecurity deficiencies which came to light after the assessment were reflected in the organization's internal cybersecurity roadmaps. The impression expressed in the case study was that the questions in the model were understandable and actionable. Due to the way that they were phrased, the questions could seem a bit complex to digest when reading superficially; however, in general, they were found to be comprehensible.

For a healthy and truly resistant setup of security, it is considered important that these security domains are harmonized in one model. To provide a complete security scope, a federated toolkit that combines the focus areas of ISFAM and CYSFAM is proposed in the next subsection. In the Federative Information Security Toolkit (FIST) (Figure 6), the authors opt to depict how cybersecurity capabilities would complement information security capabilities. We believe that this is the first structured attempt to construct a harmonized, federative information security toolkit. In doing so, the existing models' focus areas were reshuffled to fit in the framework shown in Figure 1.

CYSFAM might benefit from a more accurate and scientifically grounded focus area scoring method. However, the scoring method presented was proven to be efficient in practice, as with the proposed method in the ISFAM [15]. Nonetheless, there are signals that both methods are not optimal. In addition, certain focus areas may have been overlooked in the process. Existing literature was used in composing the CYSFAM. A logical consequence is that only focus areas that were opportune in the (recent) history were included. There is absolutely no way to guarantee to what extent this model is future-proof. This maintainability issue can be handled by a maintainability-by-design approach possibly by implementing a rule-based system. This also stands for the FIST.

Small and medium-sized enterprises (SMEs) have more challenges in adopting security practices due to limited resources [64]. The issue of adapting existing maturity models to SME characteristics was addressed by several studies [29,65,66]. With the benefit of guidelines and personalised advice, SMEs would be able to improve their security profile; therefore, our current research focuses on developing a unified and personalised information security FAM specifically for SMEs.

Federated Information Security Toolkit

This section describes the proposed Federated Information Security Toolkit (FIST) as an intertwined FAM, by combining the ISFAM [15] and the CYSFAM. It is to be noted that this model is as-of-yet a conceptual representation of what a federative information security toolkit could look like when aggregating the ISFAM and the CYSFAM into one visual representation. It is not yet a well-rounded model on its own; for that, more research is required with regards to the interdependencies of this models' focus areas and capabilities. Since the incident management capabilities identified for cybersecurity overlap with those for information security, this focus area is only presented in the information security part.

Federative Information Security Toolkit					
Focus Areas	Capabilities				
	A	B	C	D	E
Information Security					
Risk Management					
Policy Development					
Organizing Information Security					
Human Resource Security					
Compliance					
Identity and Access Management					
Secure Software Development					
Incident Management					
Business Continuity Management					
Change Management					
Physical and Environmental Security					
Asset Management					
Architecture					
Application Security					
Application Security					
Network Security					
Network Security					
Cybersecurity					
Server Protection					
End-user Controls					
Social Engineering Controls					
Cryptography					
Mobile Security					
Vulnerability Management					
Cybersecurity Awareness					
Cybersecurity Governance					

Figure 6. Federative Information Security Toolkit (FIST) integrating the ISFAM and CYSFAM—structured according to the ISO/IEC 27032 security domains. The letters (A–E) represent the capabilities; shaded areas show the maximum capability achieved for the corresponding focus area.

8. Conclusions

The research presented in this paper contributes to the domain of cybersecurity frameworks, particularly, cybersecurity self-assessment frameworks and maturity models. By surveying extensive literature, the domain-expert evaluations, and a case study in a large organization, a scientifically grounded cybersecurity focus area maturity model (CYSFAM) was developed which complements the information security focus area maturity model (ISFAM) [15]. By presenting the way CYSFAM complements ISFAM, we provide organisations with the broad view of an overarching security approach. The expert evaluations resulted in improvements that were incorporated within the cybersecurity capabilities. The case study showed the applicability of the model, and results helped the formulation of a company's cybersecurity improvement plan.

The CYSFAM encompasses 11 focus areas (sub-domains) in the cybersecurity domain. These focus areas are grouped into two categories as Technical and Organizational to facilitate understanding and manageability. As CYSFAM is a maturity model, it has assessment and measurement components in it. The 144 assessment questions to assess the cybersecurity capabilities constitute a large part of the model and they are included in a separate report which is openly accessible. The visual presentation and accompanying description of the cybersecurity capabilities in the CYFAM can enable organisations to formulate their capability implementation plan. As CYSFAM was evaluated by cybersecurity experts and demonstrated in a case study company, it provides a solid foundation for organisations to start

their cybersecurity endeavours with. CYSFAM is characterized by being a focus area maturity model based mainly on standards. As the assessment questions are mostly derived from standards and frameworks, CYSFAM can inherently facilitate awareness of and adherence to standards. In addition, due to its high granularity, CYSFAM can provide tangible process improvement advice.

To get the most benefit from the CYSFAM as an improvement instrument, including implementation guidelines per capability and personalized advice would be considered as a significant future research area. As we further elaborated in Section 7, maintainability of the model and adaptability of the model by SMEs are the most predominant areas for future research. Our ongoing research focuses on designing an adaptable cybersecurity maturity model considering the characteristics SMEs and their roles in the digital ecosystem.

Author Contributions: Conceptualization, M.S.; Formal analysis, B.Y.O. and S.v.L.; Funding acquisition, M.S.; Investigation, B.Y.O. and S.v.L.; Methodology, B.Y.O. and S.v.L.; Resources, M.S.; Software, S.v.L.; Supervision, M.S.; Validation, B.Y.O. and S.v.L.; Writing—original draft, B.Y.O. and S.v.L.; Writing—review and editing, B.Y.O. and M.S. All authors read and agreed to the published version of the manuscript.

Funding: This work was made possible with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). During this research, Bilge Yigit Ozkan was a full time PhD candidate supported by the SMESEC project. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

CEN	European Committee for Standardization
CMM	Capability Maturity Model
CIRT	Computer Incident Response Team
CISSP	Certified Information Systems Security Professional
ECSO	European Cybersecurity Organisation
FAM	Focus area Maturity Model
FIST	Federative Information Security Toolkit
IASME	Information Assurance for Small and Medium-sized Enterprises
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IS	Information Systems
ISA	International Society of Automation
ISO	International Organization of Standardization
ITU	International Telecommunication Union
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
SDO	Standards Developing Organizations
SME	Small and Medium-sized Enterprises
SIEM	Security Information and Event Management
SOC	Security Operations Center

References

1. World Economic Forum. *The Global Risks Report 2020*; World Economic Forum: Cologny, Switzerland, 2020.
2. Center for Strategic and International Studies (CSIS). *Significant Cyber Incidents Since 2006*; Center for Strategic and International Studies: Washington, DC, USA, 2019.
3. Symantec. *Internet Security Threat Report*; Symantec: Mountain View, CA, USA, 2018.
4. Kour, R.; Karim, R.; Thaduri, A. Cybersecurity for Railways—A Maturity Model. *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit* **2020**, *234*, 1129–1148. [CrossRef]

5. Khan, S.K.; Shiwakoti, N.; Stasinopoulos, P.; Chen, Y. Cyber-Attacks in the next-Generation Cars, Mitigation Techniques, Anticipated Readiness and Future Directions. *Accid. Anal. Prev.* **2020**, *148*, 105837. [CrossRef] [PubMed]
6. Choo, K.-K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A Multidisciplinary Approach to Internet of Things (IoT) Cybersecurity and Risk Management. *Comput. Secur.* **2021**, *102*, 102136. [CrossRef]
7. Radanliev, P.; de Roure, D.; Walton, R.; van Kleek, M.; Montalvo, R.M.; Maddox, L.; Santos, O.; Burnap, P.; Anthi, E. Artificial Intelligence and Machine Learning in Dynamic Cyber Risk Analytics at the Edge. *SN Appl. Sci.* **2020**, *2*, 1773. [CrossRef]
8. Williams, C.M.; Chaturvedi, R.; Chakravarthy, K. Cybersecurity Risks in a Pandemic. *J. Med. Internet Res.* **2020**, *22*, e23692. [CrossRef] [PubMed]
9. Bhuyan, S.S.; Kabir, U.Y.; Escareno, J.M.; Ector, K.; Palakodeti, S.; Wyant, D.; Kumar, S.; Levy, M.; Kedia, S.; Dasgupta, D.; et al. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *J. Med. Syst.* **2020**, *44*, 98. [CrossRef] [PubMed]
10. International Organization for Standardization (ISO). Benefits of Standards. Available online: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/benefits-of-standards.html (accessed on 8 June 2019).
11. Paulk, M.C.; Curtis, B.; Chrissis, M.B.; Weber, C.V. Capability Maturity Model, Version 1.1. *IEEE Softw. Los Alamitos* **1993**, *10*, 18–27. [CrossRef]
12. Capability Maturity Model Institute (CMMI). *CMMI Development*; CMMI Institute: Illinois, IL, USA, 2018.
13. Poeppelbuss, J.; Niehaves, B.; Simons, A.; Becker, J. Maturity Models in Information Systems Research: Literature Search and Analysis. *CAIS* **2011**, *29*, 2927. [CrossRef]
14. van Steenbergen, M.; Bos, R.; BrinkkemperInge, S.; van de Weerd, I.; Bekkers, W. The Design of Focus Area Maturity Models. In *Global Perspectives on Design Science Research*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 317–332.
15. Spruit, M.; Roeling, M. ISFAM: The Information Security Focus Area Maturity Model. In Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, 9–11 June 2014; p. 15.
16. European Union Agency for Cybersecurity (ENISA). Definition of Cybersecurity—Gaps and Overlaps in Standardisation. Available online: https://www.enisa.europa.eu/publications/definition-of-cybersecurity (accessed on 24 December 2020).
17. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC 27032:2012-Information—Security Techniques—Guidelines for Cybersecurity. Available online: https://www.iso.org/standard/44375.html (accessed on 14 December 2017).
18. Scarfone, K.; Benigni, D.; Grance, T. Cyber Security Standards. In *Wiley Handbook of Science and Technology for Homeland Security*; American Cancer Society: Atlanta, GA, USA, 2009; pp. 1–10. ISBN 978-0-470-08792-3.
19. European Cyber Security Organisation (ECSO). *State of the Art Syllabus V2*; ESCO: Essex, UK, 2017.
20. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC 27001:2013-Information Technology—Security Techniques—Information Security Management Systems—Requirements. Available online: https://www.iso.org/standard/54534.html (accessed on 15 December 2017).
21. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC 27033-1:2015-Information Technology—Security Techniques—Network Security—Part 1: Overview and Concepts. Available online: https://www.iso.org/standard/63461.html (accessed on 15 December 2017).
22. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC 27034-1:2011-Information Technology—Security Techniques—Application Security—Part 1: Overview and Concepts. Available online: https://www.iso.org/standard/44378.html (accessed on 15 December 2017).
23. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC 27035-1:2016-Information Technology—Security Techniques—Information Security Incident Management—Part 1: Principles of Incident Management. Available online: https://www.iso.org/standard/60803.html (accessed on 15 December 2017).
24. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC 27036-1:2014. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/96/59648.html (accessed on 19 February 2020).

25. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC. ISO/IEC 29100:2011(En), Information Technology—Security Techniques—Privacy Framework. Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en (accessed on 19 February 2020).
26. Rea-Guaman, A.M.; San Feliu, T.; Calvo-Manzano, J.A.; Sanchez-Garcia, I.D. Comparative Study of Cybersecurity Capability Maturity Models. In Proceedings of the Software Process Improvement and Capability Determination; Mas, A., Mesquida, A., O'Connor, R.V., Rout, T., Dorling, A., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 100–113.
27. Akinsanya, O.O.; Papadaki, M.; Sun, L. Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud? In Proceedings of the 5th Collaborative European Research Conference (CERC 2019), Darmstadt, Germany, 29–30 March 2019.
28. Rabii, A.; Assoul, S.; Ouazzani Touhami, K.; Roudies, O. Information and Cyber Security Maturity Models: A Systematic Literature Review. *Inf. Comput. Secur.* **2020**, *28*, 627–644. [CrossRef]
29. Ozkan, B.Y.; Spruit, M.; Wondolleck, R.; Burriel Coll, V. Modelling Adaptive Information Security for SMEs in a Cluster. *JIC* **2019**, *21*, 235–256. [CrossRef]
30. Christopher, J.D.; Gonzalez, D.; White, D.W.; Stevens, J.; Grundman, J.; Mehravari, N.; Dolan, T. *Cybersecurity Capability Maturity Model (C2M2)*; U.S. Department of Energy: Washington, DC, USA, 2014; pp. 1–76.
31. SSE-CMM Project. *Systems Security Engineering Capability Maturity Model SSE-CMM Model Description Document*; U.S. Department of Defense: Washington, DC, USA, 2003; p. 338.
32. Newhouse, W.; Keith, S.; Scribner, B.; Witte, G. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.
33. The Open Group. *Open Information Security Management Maturity Model (O-ISM3), Version 2.0.*; The Open Group: Berkshire, UK, 2017.
34. Koomen, T.; Pol, M. *Test Process Improvement: A Practical Step-by-Step Guide to Structured Testing*; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 1999; ISBN 978-0-201-59624-3.
35. van Steenbergen, M.; Bos, R.; Brinkkemper, S.; de van Weerd, I.; Bekkers, W. Improving IS Functions Step by Step: The Use of Focus Area Maturity Models. *Scand. J. Inf. Syst.* **2013**, *25*, 35–56.
36. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design Science in Information Systems Research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
37. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–77. [CrossRef]
38. Baskerville, R.; Pries-Heje, J.; Venable, J. Soft Design Science Methodology. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology; Association for Computing Machinery: New York, NY, USA, 2009; pp. 1–11.
39. International Telecommunication Union (ITU). ICT Security Standards Roadmap. Available online: https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx (accessed on 21 February 2020).
40. European Union Agency for Cybersecurity (ENISA). *National Cyber Security Strategies: An Implementation Guide*; ENISA: Heraklion, Greece, 2012.
41. International Electrotechnical Commission (IEC). *Industrial Communication Networks: Network and System Security. Pt. 3,3: System Security Requirements and Security Levels*; International Electrotechnical Commission (IEC): Geneva, Switzerland, 2013; ISBN 978-2-8322-1036-9.
42. Nieles, M.; Dempsey, K.; Pillitteri, V.Y. *An Introduction to Information Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.
43. Swanson, M.; Guttman, B. *Generally Accepted Principles and Practices for Securing Information Technology Systems*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 1996.
44. North American Electric Reliability Corporation (NERC). *Critical Infrastructure Protection Standards*; NERC: Atlanta, GA, USA, 2010.
45. North American Electric Reliability Corporation (NERC). NERC Security Guidelines. Available online: https://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/Electricity%20Sector%20Physical%20Security%20Guideline%20(Approved%20by%20CIPC%20-%20October%2028,%202013).pdf (accessed on 30 August 2018).
46. SANS Institute. *Critical Security Controls for Effective Cyber Defense*; SANS Institute: Bethesda, MD, USA, 2018.
47. Office of the Superintendent of Financial Institutions (OSFI). *Cyber Security Self-Assessment Guidance*; OSFI: Toronto, ON, Canada, 2013.

48. National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Federal Information Systems and Organizations*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013.
49. Information Assurance for Small and Medium Enterprises (IASME) Consortium. *The IASME Governance Standard for Information and Cyber Security*; IASME: Malvern, UK, 2018.
50. Kostick, C. *A Maturity Model for Enterprise Key Management*; Ernst & Young: Baltimore, MD, USA, 2010.
51. Information Security Forum (ISF). *The ISF Standard of Good Practice for Information Security*; ISF: Surrey, UK, 2018.
52. Souppaya, M.; Scarfone, K. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013.
53. Souppaya, M.; Scarfone, K. *Guide to Enterprise Patch Management Technologies*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013.
54. SANS Institute. *Security Awareness Roadmap*; SANS Institute: Bethesda, MD, USA, 2016.
55. 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]
56. Marble, J.L.; Lawless, W.F.; Mittu, R.; Coyne, J.; Abramson, M.; Sibley, C. The Human Factor in Cybersecurity: Robust & Intelligent Defense. In *Cyber Warfare: Building the Scientific Foundation*; Jajodia, S., Shakarian, P., Subrahmanian, V.S., Swarup, V., Wang, C., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 173–206. ISBN 978-3-319-14039-1.
57. Hadlington, L. Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours. *Heliyon* **2017**, *3*, e00346. [CrossRef] [PubMed]
58. Spruit, M.; de Boer, T. Business Intelligence as a Service: A Vendor's Approach. Available online: www.igi-global.com/article/business-intelligence-as-a-service/126896 (accessed on 25 February 2020).
59. Spruit, M.; van Lingen, S.; Ozkan, B.Y. The CYSFAM Questionnaire: Assessing Cyber Security Focus Area Maturity. Available online: http://www.cs.uu.nl/research/techreps/UU-CS-2019-003.html (accessed on 6 June 2019).
60. Muskat, M.; Blackman, D.; Muskat, B. Mixed Methods: Combining Expert Interviews, Cross-Impact Analysis and Scenario Development. *Electron. J. Bus. Res. Methods* **2012**, *10*, 9–21. [CrossRef]
61. $(ISC)^2$. Cybersecurity Certification|CISSP-Certified Information Systems Security Professional|(ISC)2. Available online: https://www.isc2.org:443/Certifications/CISSP (accessed on 21 February 2020).
62. Ngoc, L.; Hoang, D. Capability Maturity Model and Metrics Framework for Cyber Cloud Security. *Scalable Comput. Pract. Exp.* **2017**, *18*, 1329. [CrossRef]
63. Guenther, J.; Falk, I. Generalising from Qualitative Research: Case Studies from VET in Contexts. In Proceedings of the AVETRA 10th Annual Conference, Footscray, VIC, Australia, 8–10 April 2007.
64. Kertysova, K.; Bhattacharyya, K.; Frinking, E.; van der Dool, K.; Maričić, A.; Bhattacharyya, K. *Cybersecurity: Ensuring Awareness and Resilience of the Private Sector across Europe in Face of Mounting Cyber Risks-Study*; European Economic and Social Committee: Bruxelles, Belgium, 2018.
65. Mayer, N. A Cluster Approach to Security Improvement According to ISO/IEC 27001. In Proceedings of the 17th European Systems & Software Process Improvement and Innovation Conference (EUROSPI'10), Grenoble, France, 1–3 September 2010.
66. Baars, T.; Mijnhardt, F.; Vlaanderen, K.; Spruit, M. An Analytics Approach to Adaptive Maturity Models Using Organizational Characteristics. *Decis. Anal.* **2016**, *3*, 1–26. [CrossRef]