information

Article

Cybersecurity Awareness Framework for Academia

Mohammed Khader [1], Marcel Karam [2,*] and Hanna Fares [3]

[1] Computer Science Department, Applied Science Private University, Al Arab St. 21, Amman 11931, Jordan; m_khader@asu.edu.jo
[2] Department of Information Technology, Saint George University of Beirut, Beirut 1100-2807, Lebanon
[3] Department of Biology, Saint George University of Beirut, Beirut 1100-2807, Lebanon; hfares@sgub.edu.lb
* Correspondence: mkaram@sgub.edu.lb; Tel.: +961-1-577-055

Abstract: Cybersecurity is a multifaceted global phenomenon representing complex socio-technical challenges for governments and private sectors. With technology constantly evolving, the types and numbers of cyberattacks affect different users in different ways. The majority of recorded cyberattacks can be traced to human errors. Despite being both knowledge- and environment-dependent, studies show that increasing users' cybersecurity awareness is found to be one of the most effective protective approaches. However, the intangible nature, socio-technical dependencies, constant technological evolutions, and ambiguous impact make it challenging to offer comprehensive strategies for better communicating and combatting cyberattacks. Research in the industrial sector focused on creating institutional proprietary risk-aware cultures. In contrast, in academia, where cybersecurity awareness should be at the core of an academic institution's mission to ensure all graduates are equipped with the skills to combat cyberattacks, most of the research focused on understanding students' attitudes and behaviors after infusing cybersecurity awareness topics into some courses in a program. This work proposes a conceptual Cybersecurity Awareness Framework to guide the implementation of systems to improve the cybersecurity awareness of graduates in any academic institution. This framework comprises constituents designed to continuously improve the development, integration, delivery, and assessment of cybersecurity knowledge into the curriculum of a university across different disciplines and majors; this framework would thus lead to a better awareness among all university graduates, the future workforce. This framework may be adjusted to serve as a blueprint that, once adjusted by academic institutions to accommodate their missions, guides institutions in developing or amending their policies and procedures for the design and assessment of cybersecurity awareness.

Keywords: cybersecurity; awareness; curriculum; computer science; information technology; education; framework; courses; content design

Citation: Khader, M.; Karam, M.; Fares, H. Cybersecurity Awareness Framework for Academia. *Information* **2021**, *12*, 417. https://doi.org/10.3390/info12100417

Academic Editor: Sokratis Katsikas

Received: 7 June 2021
Accepted: 4 October 2021
Published: 12 October 2021

1. Introduction

The advancement, proliferation, and accessibility of the internet, communication, and mobile technologies have brought opportunities for clients/users of public and private sectors to engage in online transactions; this is increasingly generating digital data, which are normally stored on servers (cloud) in various locations. To safeguard the data and help reduce the number of possible cybercrimes that originate from illegal online activities, those entrusted with critical data, such as banking data, invested heavily in cybersecurity by hiring security experts, developing complete security policies, incorporating advanced security technologies, and continuously training their security professionals. While this investment has resulted in safer and more protected networks, operating systems, and programs, relatively less investment has been put forward to increase security awareness among clients or users of these sectors, making clients/users the weakest link. As a result, organized cyber criminals have shifted their attention to human elements by pushing significant efforts to research and develop advanced hacking techniques that exploit clients'

trust and tendency to help, in an effort to compromise their data. Online chat forums, emails, phishing, fraud, identity theft, ransomware, cyberbullying, and social engineering are some common ways in which attackers target their victims to launch cybersecurity attacks. As the cybersecurity attack methods, types, and tools that target the vulnerability of users are continuously growing and dynamically changing, the significance of the human factor in cybersecurity awareness and management has become of paramount importance. This means that, to counter cybersecurity attacks designed to exploit human factors and protect information assets, it is necessary to create cybersecurity awareness programs that make users aware of their roles and responsibilities. Studies show that a lack of awareness of the threat of cybersecurity attacks is one of the driving factors that contribute to the increasing number of internet-related attacks [1–3]. In academic institutions where the vast majority of users are students, cybersecurity awareness is essential, as students usually facilitate data breaches and digital misconduct owing to their lack of knowledge and awareness of cybersecurity and the consequences of cybercrime. Indeed, university students are prime targets of cyberattacks as the students' frequent and increased access and exposure to various online applications and social platforms have increased the cybersecurity risks associated with these daily activities. Most students have no knowledge of either the basic concepts of cybersecurity or the best practices on how to protect their devices from malware, viruses, and scams [4,5]. Students in Silicon Valley universities (a tech-savvy environment in the USA), for example, reported low levels of two-factor authentication usage or password complexity for accounts, and even felt comfortable providing personally identifiable information to an entire university population despite being aware of the possible consequences [6]. A cybersecurity survey in the United Kingdom reports that organizations within the educational sector have become the most prominent targets in terms of identified successful data breaches or attacks in 2020 [7]. As such, developing a cybersecurity awareness related to understanding network security and protection measures in academic institutions has become crucial. This leads to an urgent need to implement a common approach to improve cybersecurity awareness among college students, increase their knowledge of these issues, and educate them on ways to protect themselves from potential cyberattacks.

The rest of the related work in this article will focus on the following cybersecurity awareness aspects: students in higher education; the public; government initiatives; cyberbullying; content design and delivery, including game-based learning; awareness frameworks; and best practices.

1.1. Cybersecurity Awareness—Students in Higher Education

Cybersecurity awareness for students in higher education has been and still is being researched to better understand students' attitude, knowledge, behavior, and other relevant impacting factors. An information security survey was conducted among students of the College of Business and Economics at California State University, Los Angeles in the Spring 2011 semester [8]. It was determined that the major problem with security awareness is not a lack of security knowledge, but rather lies in the way students apply that knowledge in real-world situations. Recommendations were made to assist colleges in designing curricula that include more context-based cybersecurity awareness training. Another study identified several important factors that impact the awareness and its relationship to other factors, such as how religious indicators and social pressure influence peer performance [9]. The recommendation was that higher education institutions should develop policies and procedures that motivate students to apply proper responses to avoid security incidents. An evaluation of cybersecurity awareness knowledge, attitude, and behavior of students in seven Kuwaiti universities reported poor levels and recommended that priority be given to formal cybersecurity awareness training [10]. Early results were reported from a study aiming to investigate student awareness and attitudes toward cybersecurity and the resulting risks in one of the most advanced technology environments: Silicon Valley in California, USA. Their statistical analysis suggested that college students, despite their

belief that they are observed when using the internet and that their data are not secure even on university systems, are not fully aware of how to protect their data [6]. An empirical comparison was conducted to determine the level of cybersecurity awareness (knowledge and behavior) among college students who use smartphones relative to computers [11]. The findings showed that all students were highly aware of some information security concepts; however, they behaved differently in protecting their smartphones compared with their computers. The recommendation was to increase training campaigns that educate students on the possible information security risks related to smartphone usage in educational settings. A study reporting the preliminary results of a quantitative survey aimed to identify students' awareness and enthusiasm to learn cybersecurity in Nigerian Universities [7]. The objective of the survey was to determine whether students in this developing country were aware of cyber-attacks, identify ways to mitigate the attacks, and to determine whether cybersecurity awareness programs are part of university programs. The preliminary results indicated that the students claimed to have basic cybersecurity knowledge, but were not aware of how to protect their data. In addition, most universities did not have an active cybersecurity awareness program to improve students' knowledge on how to protect themselves from any threats. Interestingly, the surveyed students showed an interest in learning more about cybersecurity. One report outlined the findings of several information technology security awareness studies conducted among students and professionals in the United Arab Emirates [12]. It recommended the importance of assessing the security awareness by running controlled audits and presented several key factors to help increase the security awareness among users. Another study that investigated the students' awareness of basic knowledge of cybersecurity in the Department of Computer Science at Yobe State University, Nigeria, found that half of the students were not aware of how to protect their data [13]. This study recommended that an active cybersecurity awareness program be incorporated. Another study identified the need to educate and train Majmaah University, Kingdom of Saudi Arabia, students in cybersecurity awareness and practices [4]. Computer security and ethics awareness were investigated among undergraduate information technology students and education students from two different universities in Malaysia [14]. The findings revealed satisfactory levels of awareness among the students surveyed, with slightly higher level of awareness among information technology students. While male students reported higher level of computer security and ethics violations than their female counterparts, female students were more conscious of security and ethics while using computers. Information technology students were also more aware of internet security and ethics facts, but largely ignored this knowledge and were more engaged in unethical activities and illegal internet practices when compared with education students. An survey on the cybersecurity awareness of college students was conducted in major cities of Tamil Nadu [15]. The survey included questions about security threats like email, virus, phishing, fake advertisement, popup windows, and other attacks from the internet. The results showed that these college students had an above-average level of cybersecurity awareness. The work in [16] tested students on cybersecurity knowledge, self-perception of cybersecurity skills, actual cybersecurity skills and behavior, and cybersecurity attitudes. The findings revealed the need for cybersecurity campaigns to raise cybersecurity awareness.

All of the above mentioned studies collectively identify an urgent need for universities to develop well-structured cybersecurity awareness programs. Ideally, these would be based on a system-level approach that addresses current needs and has the capacity to evolve to address constantly emerging trends. Indeed, that is our contribution in this work.

1.2. Cybersecurity Awareness—The Public

Cybersecurity awareness for the public at large has been and still is being researched to better understand the public's attitude, knowledge, behavior, and other relevant impacting factors. An examination of the level of cybersecurity awareness among the general public in the Kingdom of Saudi Arabia confirmed that it is extremely low; it also appears to be

related to the nature of Saudi culture [17]. Another study investigated, using a quantitative online survey, the cybersecurity awareness of the people in the same country [18]. Although the participants had a good knowledge of information technology, their awareness of the threats associated with cybercrime, cybersecurity practices, and the role of government and organizations in ensuring information safety across the internet was very limited. Employees of educational institutions in the Middle East (academic and employees) were evaluated to understand their level of awareness of information security, and the associated risks and overall impact on the institutions [19]. Not all employees had the requisite knowledge and understanding of the importance of information security principles and their practical daily applications. It was thus recommended that comprehensive awareness and training programs be adopted at all levels of the institutions to avoid negative consequences on the institutions and their employees.

Thus, cybersecurity is a pervasive issue that may be addressed early on by instituting awareness and training programs in schools and universities.

1.3. Cybersecurity Awareness—Government Initiatives

Most countries have prioritized the importance of cybersecurity, and some have provided guidelines for private and public sectors. This resulted in the development of cybersecurity training programs to increase awareness about the impact of cyber breaches or attacks. The United States, for example, developed the National Initiative for Cybersecurity Education to address awareness, formal education, professional training, and workforce structure in an effort to improve the long-term cybersecurity attitude of its citizens [20]. The United Kingdom developed a national program that aimed at enhancing cybersecurity education and skills, with a cyber policy that mandated the incorporation of cybersecurity education at all levels, starting from the age of 11 years [21]. Saudi Arabia established the National Cybersecurity Authority (NCA) in 2017 to centralize cybersecurity controls. Concurrently, the National Cyber Security Center (NCSC) was established to serve as the arm for the technical and operational component of the NCA. The NCSC monitors supervisory control and data acquisition systems among government entities, specifically in the sectors of energy and industry [17]. It is worthy to note that, although countries differ in the cybersecurity legislative laws, one universal fact can be deduced from the overseas studies mentioned in this article; cybersecurity awareness is universally needed. Our proposed generic framework allows universities worldwide to design, with their local cybersecurity legislative laws in mind, cybersecurity awareness modules that are integrated into the curricula of students.

1.4. Cybersecurity Awareness—Cyberbullying in Schools

Cyberbullying occurs when an individual is tormented, threatened, harassed, humiliated, or embarrassed by other individuals via online or digital technologies [22]. Indeed, studies have identified cyberbullying as a cybersecurity risk that children may face and recommended that awareness programs be available in schools [23]. Although there is no evidence in the literature to suggest that cyberbullying leads to serious cyberattacks, cyberbullying rightfully merits its own place in cybersecurity awareness programs. In fact, some schools in the UAE introduced cyberbullying as part of the cybersecurity awareness programs required by students [24].

1.5. Cybersecurity Awareness—Content Design and Delivery

Cybersecurity awareness programs' content design and delivery have been and still are being researched to better understand what content is most effective and the ideal method to deliver the message behind the content. One study, for example, used two class groups of students at a university to examine the usefulness of cybersecurity awareness vocabulary test set to assess awareness levels, and observed a significant relationship between knowledge of concepts (vocabulary) and behavior [25]. Some researchers experimented with machine learning techniques to explore and identify linear relationships

among the questions in a dataset to identify the most critical questions that should be used to determine the most accurate level of cybersecurity awareness [7].

1.5.1. Infusing Cybersecurity into Computer Science Curricula or Courses

Various authors have explored how security content can be integrated into computer science curricula to increase cybersecurity awareness. One approach suggested ways to incorporate security courses into the computer science curriculum [26,27]. Later studies discussed an approach for integrating security concepts into several existing courses in the regular curriculum [28]. Some studies even showed how secure coding concepts, like integer overflow, buffer overflow, and input validation, could be introduced into introductory computer science courses [29]. Some studies explored how computer science educators could work as a community to teach cybersecurity and subsequently integrate hands-on cybersecurity exercises into the computer science curriculum [30,31]. A cybersecurity curriculum development methodology that aims to break the isolation of different knowledge units and lab practices was presented in [32]. This method guides the development of chained, hands-on cybersecurity modules based on real-world, multiple-step attacks. The resulting curriculum enabled better cybersecurity workforce development, specifically the production of graduates who are more career-ready as a result of being more skilled with logical inference and cross-field communication. Some key issues were described that prevented the cybersecurity workforce from successfully expanding in Wisconsin, USA [33]. Potential resources were identified to create a cybersecurity curriculum that uses a challenge-based learning methodology to ensure that proper cybersecurity practices and skills are age-appropriate for students and teachers. The work also outlined ways in which older adults could be encouraged to get educated on matters of privacy and security.

The curricular foundations for cybersecurity have been argued to require the existence of a K-12 component, model curricula, and accreditation criteria as clear markers of cybersecurity as an academic discipline [34]. The substantial workforce demands create a pressing need to query the direction this field has to take for the next generation of cybersecurity programs.

It has been argued that infusing security concepts pervasively into an undergraduate computer science program is a crucial and attainable best practice [35]. Indeed, it has been posited that a five-step methodology can be incorporate into a traditional computer science curriculum in a way that maintains disciplinary integrity without adding substantially new curricular content.

1.5.2. Cybersecurity Awareness—Delivery Methods

A study focused on identifying security awareness delivery methods that would be most successful in providing information security awareness, and identified delivery methods that were preferred by users [36]. Information security awareness was conducted using text-, game-, and video-based delivery methods with the aim of determining user preferences. The recommendation was that combined delivery methods would be most effective. As our proposed framework uses game-based learning, we will elaborate on it in the next subsection.

Game-Based Learning

Games have been used as learning tools for hundreds of years. Chess was used to learn strategic thinking since the Middle Ages; similarly, the game of Kreigsspiel was invented in 1812 primarily to teach Prussian officers strategic planning. Even Friedrich Fröbel's notion of learning by play was the birth of kindergarten in the mid-1800s [37]. The central principle behind game-based learning is to teach through repetition, failure, and objective achievement. Video games are based on this concept. The player starts slowly and gains experience until the player can handle the most challenging stages skillfully [37]. Instructive games may be considered, quite possibly, the latest resources used to assist/facilitate and motivate students' learning experience [38]. Game-based

learning will lead to a measurable improvement in enjoyment in higher education that noticeably increases deep learning, especially when the game is aligned with the curriculum and learning outcomes [37]. Game-based learning is already successfully applied in many fields (e.g., healthcare, defense, and management), and it has been proven that it can be an effective training tool. In cybersecurity, game-based approaches have shown the potential of improving cyber security learning and training effectiveness. In [39], for example, it was reported that various studies have showed that trainees who used games reported significant improvements in acquiring knowledge and skills, diligence, and motivation. Young students reported that engaging in game-based educational approaches is more entertaining than engaging in traditional approaches [40]. Kahoot is one of the platforms for game-based learning that enables teachers to easily create and share learning games and quizzes. In addition to making the learning process fun and entertaining, this game simplifies learning assessment through reports. Indeed, the Kahoot platform has more than forty million ready-to-play games in various topics [41]. Every month, millions of people use Kahoot as a game-based learning tool in schools and colleges, corporate offices, social environments, and sporting and cultural events all over the world [41].

In cybersecurity, many games that target groups, such as employees, professional and non-professional end-users are found in academic publications or through a search in the domain of cyber security [42]. For example, the work in [43] introduced a game that teaches professional users computer and network security using real life scenario questions. In [44], a gamification that uses real-life scenarios with a focus on cybersecurity attacks detection and handling was used to teach both professional and nonprofessional end-users incident detection and response procedures that must be followed in the event of a cybersecurity threat. Some games adopt certain dynamic complexities that are based on the players' performance, level of difficulties, and time allocated to complete a task. Scenario-based learning in a gaming environment also supports active learning strategies such as problem-based or case-based learning by using interactive scenarios; participants must apply their subject knowledge, critical thinking, and problem solving skills to solve a question by working their way through a storyline that is usually based on an ill-structured or complex problem [45].

1.6. Cybersecurity Awareness Frameworks

A framework was developed to guide the implementation of a knowledge management system for improving security awareness in an organizational context [46]. The contributions of this framework to improving security awareness were evaluated by cybersecurity experts using a prototype, and were found to be applicable in many organizational settings. The results obtained from end-users who were not familiar with computer threats reflected the positive effects of improving security awareness.

On 12 February 2014, National Institute of Standards and Technology released its final cybersecurity framework, titled "Framework for Improving Critical Infrastructure Cybersecurity" [47]. This framework adopts industry standards and best-practices to provide a set of voluntary, risk-based measures that can be used by organizations to address their cybersecurity risk; it also provides a tool for organizations to assess themselves and to use as a baseline measure of their cybersecurity programs. Rather than providing a design of a cybersecurity awareness program, it is a reference point for objective evaluations of an organization's cybersecurity program.

The work in [48] proposed a cyber-security awareness and education framework for South Africa to assist in creating a cyber-secure culture in South Africa among all internet users. The framework was based on key factors extrapolated from a comparative analysis of relevant developed countries, and subsequently validated by cybersecurity experts with a series of questions, including the following: Is the framework comprehensive enough? Do you think the framework would contribute to the cultivation of the suggested culture? Are there any other frameworks of which you are aware, to which you can refer me? The work in [49] proposed a conceptual framework for the design and implementation of cyber

security games to improve, using game-based approaches, cyber security education, and pedagogical effectiveness. Various data and statistical measure were used to assess the mindset of internet users for preparing a cybersecurity awareness framework [50]. The resulting recommendations included the need to provide practical sessions on various cyber restriction and monitoring tools, such as parental locking and website blocking.

Based on the investigated level of security awareness among college and high school students, a module was developed that used interactivity and presentation of shocking consequences of careless cyber habits of common internet/technology users to increase the awareness of the students [51].

1.7. Security Awareness—Best Practices

The following best practices are based on the work in [52]:

- Build an institution-wide culture and participation where decision-making and application of cybersecurity best practices become daily pursuits for end-users at all levels.
- Clearly communicate to upper-level management and all end-users that it is critical to understand the value and purpose of cybersecurity education before implementing training.
- Gauge program success by conducting a comparative study to see if there is a reduction in institutional employee-driven cybersecurity incidents over time.
- Conduct regular, ongoing assessments and training so that end-users are given the benefit of regular cybersecurity education, and the opportunity to learn over time and develop new skills.
- Create a clear link between assessments and training.
- Maintain awareness of cybersecurity best practices for end-users by revisiting topics on a regular basis and incorporating ongoing awareness activities; without reinforcement, the institution must regularly rebuild rather than build upon.
- Be consistent in tracking and reporting progress.
- Keep the end-user motivated and engaged by applying gamification techniques that use rewards and positive reinforcement to raise end-user interest and participation and elevate the effectiveness of your program.

The related work in this article focused on seven categories of cybersecurity awareness: students in higher education; the public; government initiatives; cyberbullying; content design and delivery, including game-based learning; awareness frameworks; and best practices.

The study of these categories highlights the importance of creating cybersecurity educational/awareness programs that (1) are based on a domain-specific framework that can be systematically applied across an institution, organization, enterprise, or simply a specific group of people; (2) incorporate continuous improvement to assess its effectiveness and to incorporate advances in technologies; (3) focus on the education of users; and (4) incorporate game-based activities to improve learning outcomes. The goal of this study is to design a Cybersecurity Awareness Framework for Academia that (a) seamlessly integrates cybersecurity awareness into curricula to mainstream the delivery and assessment of infusing cybersecurity awareness into the academic programs in institutions of higher learning; and (b) links this integration with certificates to students who complete cybersecurity awareness modules.

Untrained faculty and staff can also contribute to cybersecurity breaches. Therefore, the proposed framework ought to be extended to support the registration of faculty members and staff in the general Cybersecurity Awareness Training Modules, and follow a similar path of certificate completion as that of students.

2. Method Used to Design the Cybersecurity Awareness Framework

A literature review was carried out that queried the following databases: Academic Search Ultimate; Education Research Complete; Professional Development Collection; Taylor and Francis Journals; Emerald Journals; Sage Journals; and Science Direct. Keywords,

such as "cybersecurity awareness", "cyberattacks", "awareness frameworks", "integration of cybersecurity in courses", and "game-based learning", and similar terms were used; the results of this review are outlined in the Introduction. The Cybersecurity Awareness Framework for Academia (CAFA) proposed in this work is conceptual and was developed based on this review and the experiences of the authors in higher education, primarily in computer science, information technology, biology, and the STEM disciplines. The main goal of CAFA is to integrate the following three elements:

1. The infusion of game-based cybersecurity awareness learning and assessment into the curricula of academic institutions using training modules that are part of students' study plan.
2. The incorporation of continuous improvement practices in cybersecurity awareness.

The proposed CAFA is crucial for the development of systems that ensure adequate cybersecurity awareness of all university graduates, irrespective of majors or disciplines. This study focuses on three constituents of CAFA (discussed in Section 3), expanding them into sequences of units and their phases; these could aid academic institutions in designing and delivering awareness-based certificates for different stages throughout the university residency.

3. Conceptual Cybersecurity Awareness Framework for Academia

The CAFA is based on two interacting constituents linked by the Student Information System (SIS) (Figure 1). The term constituent is used to represent a composite of activities that include support, design, and assessment. As such, constituents do not have to correspond to discrete units/offices/departments in academia, although that correspondence is an option. The three constituents of the CAFA are as follows:

1. An academic institution's "information and communication technology support" (ICTS) constituent that manages the learning management system (LMS), coordinates with the student information systems (SISs), provides support during the design of cybersecurity awareness modules by faculty members, and provides support for the assessment of students.
2. An academic institution's "cybersecurity awareness center" (CAC) constituent conducts research on the latest cybersecurity awareness trends and related best practices, defines/adjusts the cybersecurity awareness topics and assessments for training modules, populates test banks and creates all training modules on the learning management system (LMS), reports on the assessment results to the student information system (SIS), and recommends actions for further improvements.

The effective design, delivery, and assessment of cybersecurity awareness modules requires cooperation that is based on clear processes between the two constituents and the SIS. The CAFA would guide the development of policies and procedures for each of the two constituents with their related continuous improvement mechanisms. Indeed, the establishment of a Cybersecurity Awareness Framework ensures the efficacy of the current awareness cycle and, ideally, establishes procedures for the continuous improvement of awareness contents.

This work highlights important elements of the "cybersecurity awareness center" (CAC) and the "information and communication technology support" (ICTS) constituents of the cybersecurity awareness framework, and provides sequential guidelines for the design, delivery, and assessment of cybersecurity awareness training modules in academia (Phases I and II of CAC).

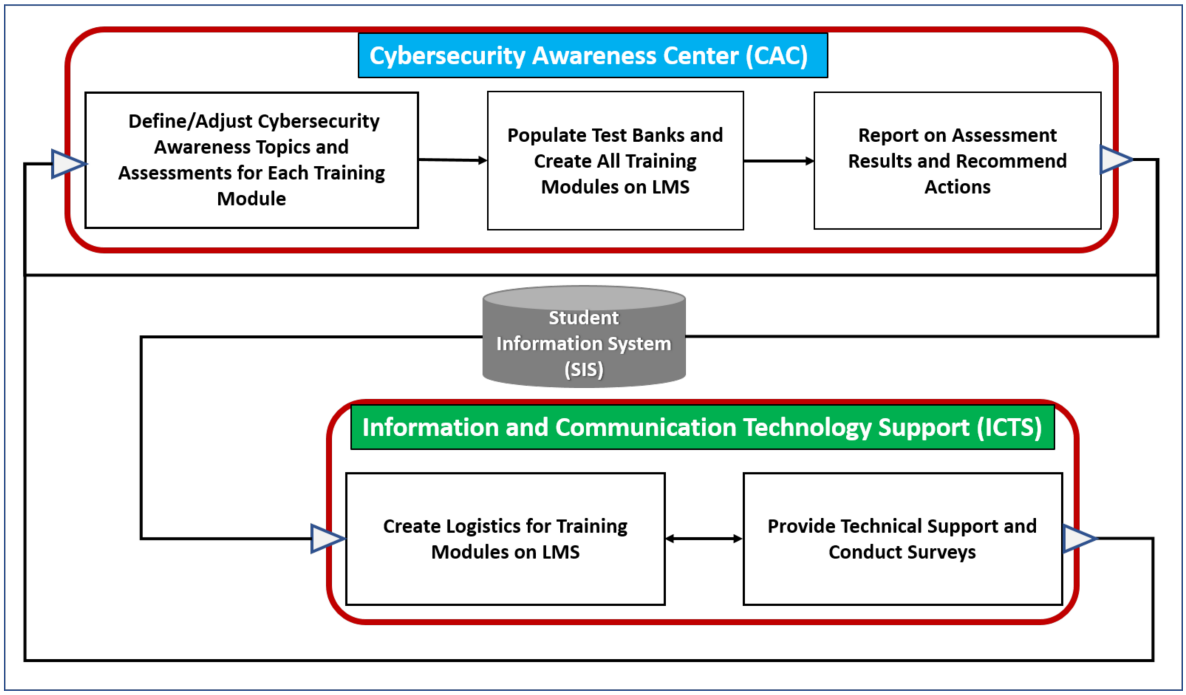

Figure 1. Cybersecurity Awareness Framework for Academia (CAFA).

4. The Cybersecurity Awareness Center

The Cybersecurity Awareness Center (CAC) constituent includes three sequential phases, each phase organized as a series of activities (Figure 2). Faculty members in an academic institution are the major stakeholders of the CAC constituent because of their central role in the design/adjustment of cybersecurity awareness topics and scenario-based gamified assessments of the training modules; these faculty members should be provided by the CAC with the necessary knowledge (series of workshops) to allow them to align training modules with course learning outcomes. For example, the English faculty member in charge of infusing the cybersecurity awareness topics in an English course should ensure that the learning outcomes of the course are maintained while accomplishing the purpose of educating English major students on cybersecurity awareness.

4.1. Phase 1—Define/Adjust Cybersecurity Awareness Topics and Assessments for Training Modules

This phase of the CAC constituent encapsulates the activities of researching recent trends in cybersecurity attacks, defining/adjusting cybersecurity awareness topics in training modules, defining/adjust scenario-based gamified assessments in training modules, creating/adjusting scenario-based gamified questions in the test banks of the LMS, populating each training module with assessments from test banks, reporting assessment results to the student information system, analyzing the results for each training module, and reporting for possible actions to continuously improve the modules (Figure 2).

4.1.1. Phase 1/Activity 1: Research Latest Cybersecurity Attack Trends

Different threatening technologies exist and are evolving and creating opportunities for more cyberattacks. Adversarial inputs, data-poisoning attacks, and model-stealing are recent favorites of cybercriminals. Every year, cybersecurity experts around the world determine and publish the cybersecurity attack trends in many industries; individuals try to familiarize themselves with these trends and adjust their practices. For example, infrastructure as a service is being increasingly hosted on the cloud, particularly for businesses with private data. This has significant cost-saving benefits and increases an organization's speed to introduce services to the market; however, it makes the organization more vulnerable to

cyberattacks, making cybersecurity services a priority for cloud users, and places attacks against cloud services on the list of trends.

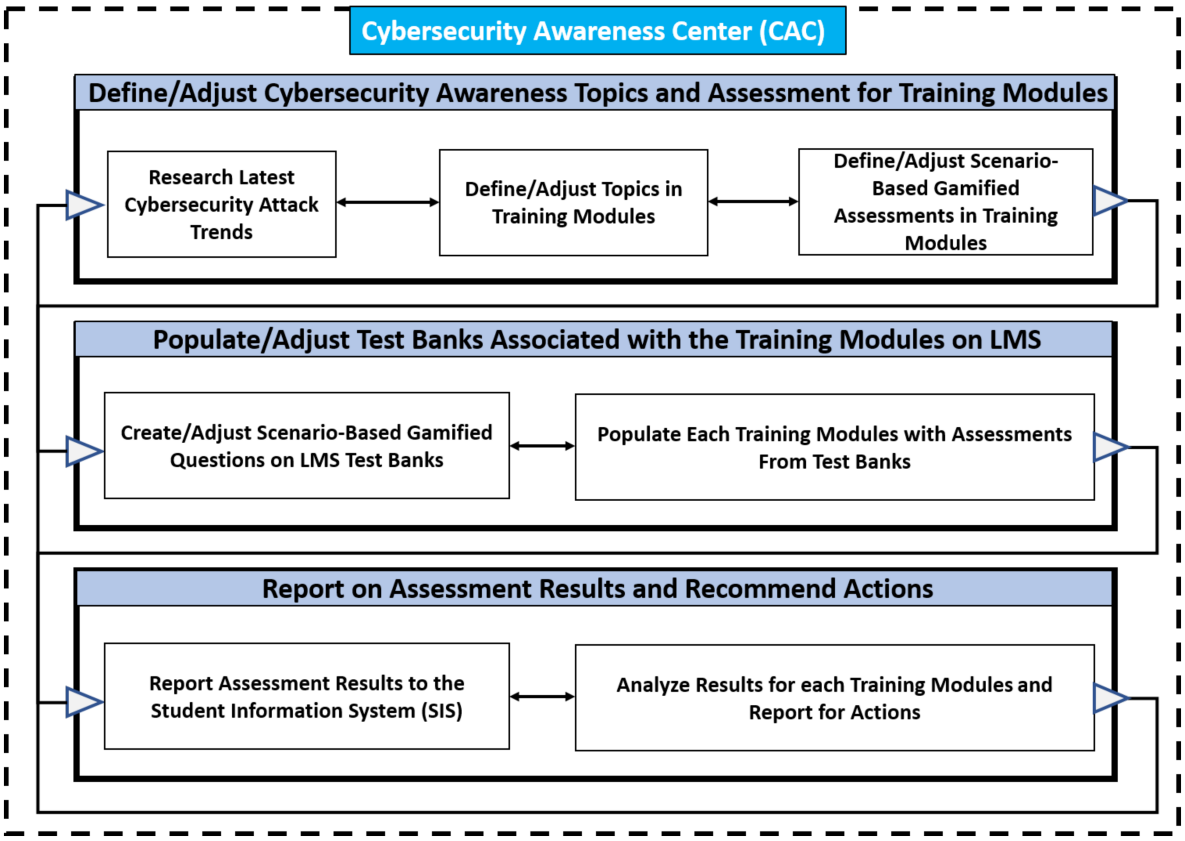

Figure 2. Cybersecurity awareness center (CAC) constituent of the Cybersecurity Awareness Framework.

4.1.2. Phase 1/Activity 2: Define/Adjust Topics in Training Modules

Faculty members, the main stakeholders of the CAC, should follow the latest trends in cybersecurity to continuously improve the design of the cybersecurity awareness topics for a training module. Faculty members in the CAC should adjust the topics in a training module based on these latest trends and on the results and corresponding recommendations of the last assessment (see Phase I/Activity 3).

Cybersecurity Awareness Training Module Design Recommendation

The recommendation is that the CAFA supports four cybersecurity awareness training modules (CATM-0, CATM-1, CATM-2, and CATM-3). CATM-0 is designed to be taken during orientation for new students; it contains general cybersecurity awareness subjects that are easy to complete with minimal effort. Each CATM-x (where x is either 1, 2, or 3, representing Year/Level 1, Year/Level 2, or Year/Level 3, respectively; additional years can be added for lengthier programs), comprises two parts:

- The first part contains cybersecurity awareness topics and related gamified questions that are general to all students in an academic institution; these are referred to as CATM-$x_{(G)}$. These cybersecurity awareness topics and related gamified questions are appropriately designed for the relevant year. Examples of topics and one gamified question for CATM-$1_{(G)}$ are shown below.
- The second part contains cybersecurity awareness topics and related gamified questions that are specific to each major in an academic institution; these are referred to as CATM-$x_{(S)}$. For example, CATM-$1_{(S)}$ for English majors would contain gamified questions designed by the English instructor based on cybersecurity awareness topics

that are infused in a required English course that is associated with CATM-$1_{(S)}$. To elaborate a bit further, an English instructor uses content-based language instruction to teach both English language skills and cybersecurity content. For example, the English instructor would use a newspaper article that is intended for general public consumption and present it in class to teach both English skills and cybersecurity basics that will drive the cybersecurity awareness that will be used to create gamified questions; a task that can be done with the help of a cybersecurity awareness center. These "major-based cybersecurity awareness course topics" will be explained further below.

A CATM-$x_{(S+G)}$ (where x represents Year/Level 1, 2, or 3, respectively) contains both general and specific cybersecurity awareness gamified questions appropriately designed in this phase. CATM-$x_{(S+G)}$ modules can be added to students' study plans in any major so that they become required courses; that is, students enrolled in any major will have to pass CATM-1, CATM-2, and CATM-3 to graduate. Academic institutions may choose to make all the CATM-x "required but non-binding for graduation".

I. CATM-$x_{(G)}$: CATM-$1_{(G)}$ Material for First-Year Students

Table 1 shows the topics, sub-topics, and outcomes to be measured for the materials designed for the cybersecurity awareness training module for first year students, or CATM-$1_{(G)}$. This material is based on the SANS Institute's security policy project [35]. Basic security awareness training is needed as a foundation for first-year students.

Table 1. Topics to be included in the cybersecurity awareness for first year students.

Topic	Sub-Topics	Outcomes to be Measured
Hacking	Hacking definitions, types of hackers, types of cybercrimes, and ethical hacking	1. Understand the definition of hacking 2. Define types of hackers 3. Describe types of cybercrime 4. Describe ethical hacking
Social Engineering Attacks	Social engineering attacks definitions, common types of social engineering attacks	1. Understand the definitions of social engineering attacks 2. Distinguish between different types of social engineering attacks
Phishing	Definition of phishing, protect your personal information, recognize false links, recognize false emails	1. Understand the definition of phishing 2. Describe the risks associated with phishing 3. Describe different phishing techniques
Pretexting	Definition of pretexting attacks, examples of fabricated scenarios used in pretexting	1. Understand the definition of pretexting 2. Describe the risks associated with pretexting 3. Describe different pretexting techniques
Baiting	Describe the proper definition of baiting attacks, differentiate between baiting and pretexting, protecting your login credentials	1. Understand the definition of baiting 2. Describe the risks associated with baiting 3. List the differences between baiting and pretexting techniques

Table 1. *Cont.*

Topic	Sub-Topics	Outcomes to be Measured
Quid Pro Quo	Describe the proper definition of quid pro quo attacks, differentiate between baiting and quid pro quo	1. Understand the definition of quid pro quo 2. Describe the risks associated with quid pro quo 3. List the differences between baiting and quid pro quo techniques
Tailgating	Describe the proper definition of tailgating attacks, examples of tailgating attempts and their results	1. Understand the definition of tailgating attacks 2. Describe the risks associated with tailgating attacks
Rogue	Describe the proper definition of rogue attacks, examples of rogue attempts and their results	1. Understand the definition of rogue attacks 2. Describe the risks associated with rogue attacks
Strong Password Requirements	Describe the password construction requirements, password protection standards, and associated risks	1. Understand the requirement of a strong password 2. List the risks associated with a weak password
Email Security	Understand the email usage risks, opening attachment risks, and sender identification	1. Recognize the dangers of using emails 2. Determine the dangers of opening an attachment 3. Understand the financial consequences of poor email security
Securing Mobile Devices	Mobile security requirements, relevant built-in security features, and issues associated with hacked devices	1. Understand the requirements for secure mobile devices 2. Describe the steps to use built-in security features 3. Define the risks associated with compromised devices
Destroying Sensitive Data	Consequences of inappropriate data disposal, steps to destroy out-of-date sensitive data	1. Understand the consequences of inappropriate data disposal 2. Describe the steps to destroy out-of-date sensitive data
Malware Protection	Malware classifications, definitions for anti-virus software, types of virus-caused damages, best practices to prevent malware	1. Understand malware, viruses, and anti-viruses 2. Distinguish between virus types 3. Describe best practices and steps to prevent malware

II. $CATM_{-x(S)}$: Major-Based Cybersecurity Awareness Course Topics

Each academic department in a faculty/school selects courses from its first, second, and third years to become targets for infusing specific cybersecurity awareness topics. For example, in an English department, courses like "Active Reading" (Levels 1 and 2), and Academic Writing Skills" (Level 3) might be elected to become infused with cybersecurity awareness topic(s). In such English courses, the infusion will come in the form of reading/writing tasks. In contrast, the Math department may choose "Discrete Math" (Level 1), "Number Theory" (Level 2), and "Numerical Analysis" (Level 3) for infusing cybersecurity awareness topics. In a Math course, the infusion could come in the form of an applied subject. The coverage of major-based cybersecurity awareness course topics in a course

associated with a CATM-$x_{(S)}$ might consume 1 to 1.5 contact hours. The allocated time may vary according to institutions and/or courses.

Each academic department would maintain records indicating which required courses corresponds to which CATM-$x_{(S)}$ (Table 2). The educators of courses associated with a CATM-$x_{(S)}$ would work with, or be a member of, the CAC constituent to create scenario-based and gamified questions for the cybersecurity awareness-infused topics. Scenario-based and gamified questions coming from infused cybersecurity topics in a specific major will be available only to students in that major during the assessment of a CATM-$x_{(S)}$.

Table 2. Examples of three major-required Math and English courses for the CATM-$x_{(S)}$.

CATM-$x_{(S)}$	**Math Major**	**English Major**
CATM-$1_{(S)}$	Discrete Math	Active Reading 1
CATM-$2_{(S)}$	Number Theory	Active Reading 2
CATM-$3_{(S)}$	Numerical Analysis	Academic Writing Skills

Departments/programs like information technology, computer science, computer engineering, and other technology-concentrated programs may include cybersecurity as an expected learning outcome of the program and infuse cybersecurity into every core course. Students in such programs should not be required to participate in the CATM-$x_{(G+S)}$.

4.1.3. Phase 1/Activity 3: Define/Adjust Scenario-Based Gamified Assessments in Training Modules

Faculty members define or adjust the scenario-based gamified assessments using the topics decided for each training module (for example, in CATM-$x_{(G)}$ and CATM-$x_{(S)}$).

Scenario-Based Questions—Gamified

Scenario-based training is an engaging training environment in which students face practical work challenges and receive realistic feedback as they advance; the results are based on the learner's choices. Unlike traditional training in which students passively learn knowledge by reading a text and then taking a test, students in scenario-based training actively engage in the process from start to end. This kind of training allows students to learn from failures and successes; if they do not correctly resolve a question or situation, students can adjust their approaches until they succeed. The following is an example of a phishing (Table 1) topic that is used to build a scenario-based question:

You received an email from a Facebook administrator asking you to urgently press a link to send the activation code you received in your mobile device within an hour, or you will lose your account:

A You should press the link and make sure the website belongs to Facebook.
B You should verify the email sender and make sure the email is sent from Facebook.
C You should try to find misspelling mistakes in the email to make sure the email is not phishing.
D This is considered a phishing email and you should not press the link as you did not sign up to any website that sent you a verification code.

The correct answer is D. Because you did not register to any website using your Facebook account, this is a type of phishing. The next question is automatically determined based on the student's choice.

Such scenario-based questions related to the cybersecurity awareness topics of a CATM- $x_{(G)}$ are then gamified using gamification engines or plugins like Kahoot, H5P, and so on. Gamifying the scenario-based questions requires game-like elements, including interactivity, instant feedback, progress indicators, time-limits, repetition, unveiling of levels, scoreboards, and badges and awards. For each CATM-x(G), the cybersecurity awareness topics, scenario-based questions, and their gamification are managed by CAC.

4.2. Phase 2—Populate Test Banks Associated with the Training Modules on LMS

Like most courses in an academic institution, the CATM-x will be created by the ICTS constituent every academic year on the academic institution's LMS (Moodle, for example). As depicted in Figure 3, there are two level-appropriate test banks associated with each CATM-x: one test bank for CATM-$x_{(G)}$, where $_G$ is for general, and another for CATM-$x_{(S)}$, where $_S$ is for specialized.

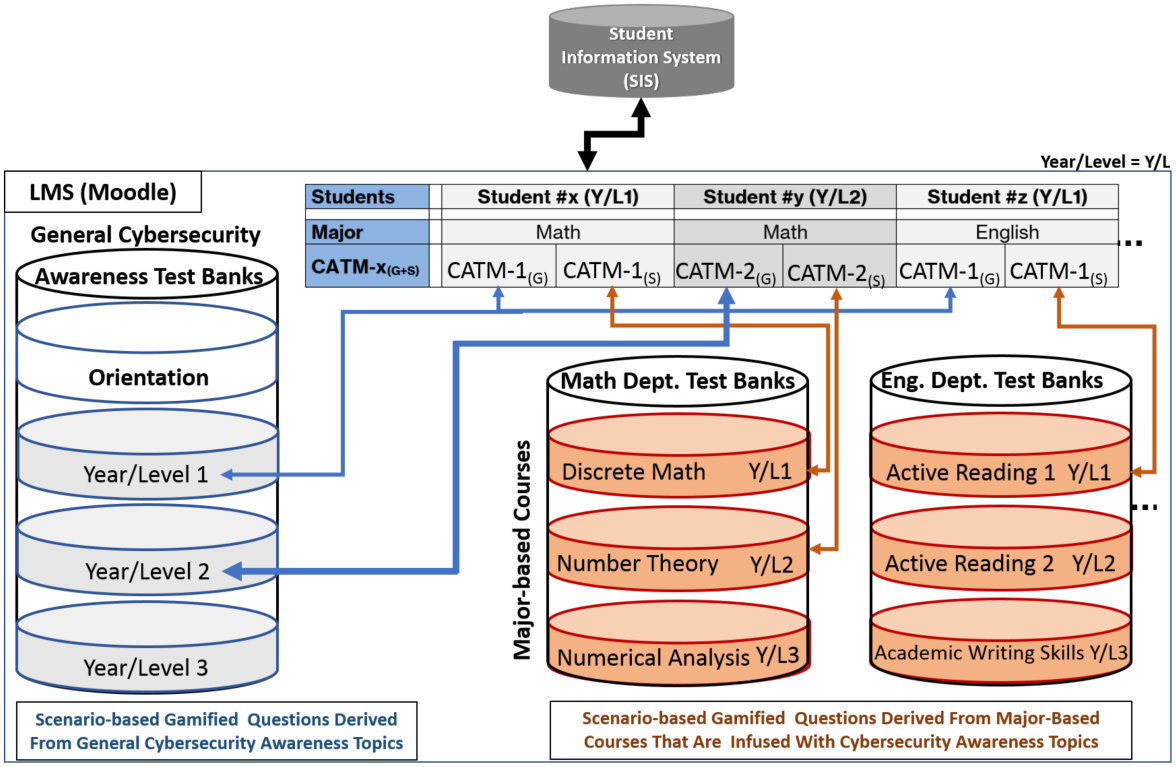

Figure 3. Populating test banks for training modules.

The test bank associated with CATM-$x_{(G)}$ contains scenario-based gamified questions derived from general cybersecurity awareness topics that are level-appropriate. For example, in Figure 3, CATM-$1_{(G)}$ is associated with the general cybersecurity awareness test bank of Level 1. The test bank associated with CATM-$x_{(S)}$ contains level-appropriate scenario-based gamified questions derived from major-based courses infused with cybersecurity awareness topics. For example, in Figure 3, CATM-$1_{(S)}$ for the English major is associated with the cybersecurity awareness test bank of Level 1 (Active Reading 1), whereas CATM-$2_{(S)}$ for the Math major is associated with the cybersecurity awareness test bank of Level 2 (Number Theory). It should be noted that students in one major taking courses in another major, for example, computer science students taking Active Reading 1, would also experience the training module from the other major. This is an advantage as students would be exposed to similar concepts from the points of views of different disciplines.

4.2.1. Phase 2/Activity 1: Create/Adjust Scenario-Based Gamified Questions on LMS Test Banks

Based on Phase 1, faculty members experienced in using the scenario-based gamification tools of an LMS (Like H5P) will compile questions in the appropriate test banks. For example, in the test banks related to the Math department, questions related to courses at various levels would be created/adjusted.

4.2.2. Phase 2/Activity 2: Populate Each Training Module with Assessments from Test Banks

Based on the recommendations/results from Phase 3 of CAC, faculty members populate each CATM-$x_{(G+S)}$ training module with questions from the appropriate test bank and levels. Scenario-based gamified assessment questions related to a CATM-$x_{(G)}$ are derived from the appropriate test bank and are common to all students enrolled in that CATM-$x_{(G)}$ (Figure 3). In contrast, scenario-based gamified assessment questions related to a CATM-$x_{(S)}$ are derived from the appropriate test bank related to a department's courses that are infused with cybersecurity awareness topics (Figure 3). For example, game-based assessment questions for CATM-$1_{(S)}$ for a Math major are populated from the test bank related to the cybersecurity awareness topics that are infused into Discrete Math.

4.3. Phase 3—Report on Assessment Results and Recommend Actions

In this phase, reports of assessment results are generated to the Student Information System (SIS); these reports are analyzed and recommend actions are generated for improvement in the overall design of cybersecurity awareness topics and their related scenario-based gamified assessments. It is recommended that courses that are infused with training modules include cybersecurity-related outcome(s) in their course learning outcomes; the results on these outcome(s) could serve as elements of the evaluation of the effectiveness of the training module.

4.3.1. Phase 3/Activity 1: Report Assessment Results to the Student Information System (SIS)

As depicted in Figure 1, the results of the assessment of a CATM-x will be reported to the SIS for the entry of grades. However, it is recommended that courses that are infused with training modules include cybersecurity-related outcome(s) in their course learning outcomes; the results on these outcome(s) could serve as elements of the evaluation of the effectiveness of the training module.

4.3.2. Phase 3/Activity 2: Analyze Results for Each CATM-$x_{(G+S)}$ and Report for Actions

The results of the training modules are reported to the Student Information System (SIS). These results are then analyzed by the CAC for improvement, which could include changes to the design of the assessment instruments' content.

5. Information and Communication Technology Support (ICTS)

The information and communication technology support (ICTS) constituent of the CAFA in Figure 1 includes two phases. The phases have sequential activities that are depicted in Figure 4.

5.1. Phase 1—Create Logistics for Training Modules on LMS

The first phase of the ICTS encapsulates the logistics required to create, manage, and support the cybersecurity awareness training modules CATM-$x_{(G+S)}$ on the LMS of the academic institution. The second phase provides the technical support to faculty members in charge of designing and managing cybersecurity awareness training modules.

5.1.1. Phase 1/Activity 1: Set up Training Modules on LMS

Aside from CATM-0, which students are required to take, and at orientation, the ICTS establishes all three CATM-x modules on the university's learning management system (LMS) as courses based on the Student Information System (SIS). The ICTS then communicates with the CAC constituent to receive the updated/revised topics and assessment questions related to all the CATM-$x_{(G)}$ and CATM-$x_{(S)}$ modules.

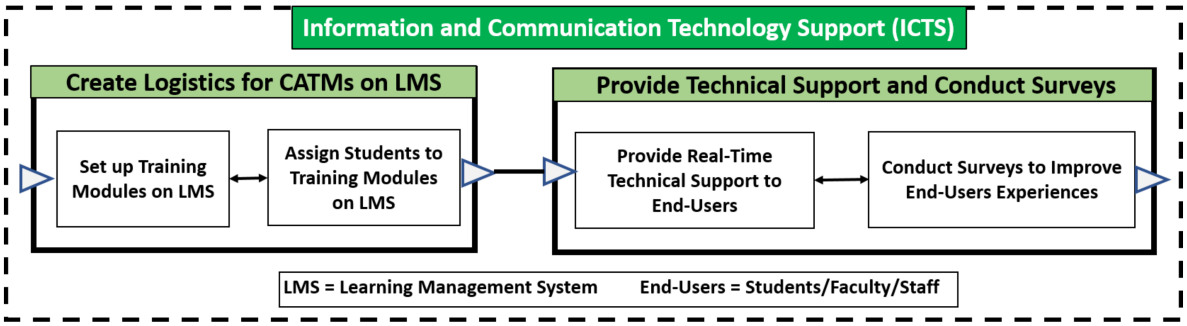

Figure 4. Information and communication technology support (ICTS) constituent of the Cybersecurity Awareness Framework.

5.1.2. Phase 1/Activity 2: Assign Students to Training Modules on LMS

At the beginning of each academic year, the ICTS adds university students to the appropriate CATM-$x_{(G+S)}$ based on the Student Information System (SIS). Students who fail a CATM-$x_{(G+S)}$ are assigned an "NP" or "No Pass" grade, but are registered in CATM-$x+1_{(G+S)}$ by the SIS. Registering in CATM-$x+2_{(G+S)}$ requires that a student passes CATM-$x_{(G+S)}$ or CATM-$x+1_{(G+S)}$. This way, students are not hindered by the failure of a training module.

5.2. Phase 2—Provide Technical Support and Conduct Surveys

The second phase of the ICTS encapsulates the logistics required to provide real-time technical support to CAC/CAM end-users. The second phase provides the technical support to conduct usability and other surveys to improve the execution of phases by the CAC constituent.

5.2.1. Phase 2/Activity 1: Provide Real-Time Technical Support to End-Users

The ICTS second phase plays a major role in supporting the end-users. Both synchronous and asynchronous support should be readily available to end-users to ensure that the experience is both enjoyable and effective.

5.2.2. Phase 2/Activity 2: Conduct Usability Surveys to Improve End-Users Experiences

To improve the various phases in the CAC constituents, the ICTS could deploy surveys whose aim is to identify ways to improve the processes. These surveys will attempt to (a) identify novel cybersecurity attack trends; (b) best infuse cybersecurity awareness topics in selected major courses; (c) design and deliver scenario-based gamified assessments; and (d) improve the usability of the assessment platform and interface. User satisfaction surveys are also deployed by ICTS to improve the overall experience of the end-users.

6. Discussion

This work proposes a Cybersecurity Awareness Framework for Academia (CAFA) that focuses on the implementation, assessment, and continuous improvement of cybersecurity training modules. It comprises two constituents: the cybersecurity awareness center (CAC) and information and communication technology support (ICTS). This CAFA can be adjusted based on the capabilities and goals of an academic institution. For example, the CAC constituent may be a formal, funded unit in an institution, or a specialized unit in the teaching and learning center (which most universities have); alternatively, it can engender the training of a few faculty members who would provide this service to the rest of the academic departments. The CAFA defines the cybersecurity awareness training modules and operational structure. This framework is thus an essential component of an institutional quality assurance system (IQAS) that guides the design of policies and procedures and ensures continuous improvement of operations and of the CAFA itself.

To ensure continuous improvement, at both the macro level (policy, procedures, and CAFA design) and the micro level (implementation of procedures by various academic

and non-academic units), an IQAS that incorporates a continuous improving cycle with proper assessment and feedback is required (Figure 5). The continuous improvement cycle of the IQAS that is outlined below can be used by most educational institutions, albeit with some adjustments. In the context of IQAS, these adjustments may be related to the culture and mission of the educational institution. The IQAS comprises four units that are briefly discussed below in the context of CAFA.

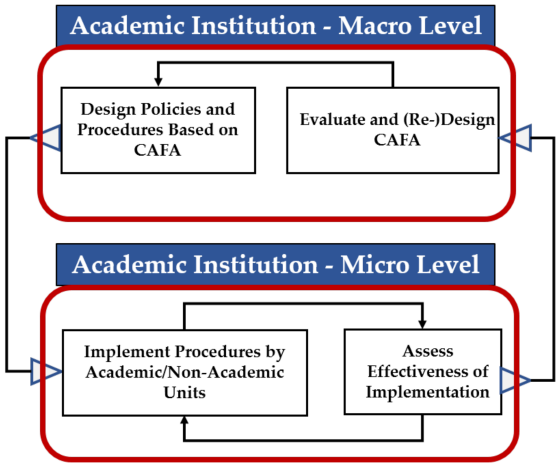

Figure 5. The IQAS and its continuous improvement cycle.

6.1. Academic Institution Macro Level

6.1.1. Unit—Evaluate and (Re-)Design CAFA

A CAFA is an essential tool for starting academic institutions as it guides the development of cybersecurity awareness educational policies and procedures; it can also be an effective tool for established academic institutions who wish to refine their educational goals and adjust their policies and procedures. However, the CAFA itself needs to be systematically adjusted and improved. The feedback received from the "assess effectiveness of implementation" unit in the IQAS is used to evaluate the effectiveness of the CAFA. This evaluation may result in the amelioration of the CAFA and/or its associated policies and procedures.

6.1.2. Unit—Design Policies and Procedures Based on CAFA

The CAFA guides the development of policies (laws) and procedures (implementation details) that regulate and guide the implementation of the CAFA. Indeed, the policies and procedures of the cybersecurity awareness center (CAC) and the information and communication technology support (ICTS) constituents must be coordinately developed and implemented to ensure the overall operational success. In addition, academic institutions should be aware of the requirements of their targeted accreditation bodies when constructing their CAFA and their associated policies and procedures. Procedures provide detailed instructions with forms, templates, and checklists on how to accomplish rules established in policies.

6.2. Educational Institution Micro Level

6.2.1. Module—Implement Procedures by Academic/Non-Academic Units

The established procedures are used by faculty members and formal entities, such as departments and/or faculties, to efficiently and effectively engage students with the training modules; feedback from faculty members, students, and entities should be used to evaluate the feasibility of the implementation plan and can be mechanisms for strategic institutional improvement. For example, some scenario-based gamification and relevant assessment may not be implementable in the current LMS, so the LMS capabilities may be upgraded.

6.2.2. Unit—Assess Effectiveness of Implementation

To assess the educational experience, the IQAS requires operational assessment instruments that evaluate compliance with policies and procedures designed based on the CAFA; for example, operational assessment instruments could be incorporated into the cybersecurity awareness training modules. These instruments determine whether the CAFA adopted by the institution can function/is functioning effectively. Furthermore, the cybersecurity awareness topics infused into selected major-based courses outlined in this work would be assessed at the micro level to improve the cybersecurity awareness educational experience. For example, using feedback mechanisms outlined in this work (Figure 5). Data from the operational and training modules assessment instruments could be used to adjust the CAFA and/or its associated policies and procedures.

The complete CAFA with its well-developed constituents should clearly delineate its stakeholders. Indeed, this article refers to faculty members as the primary stakeholders in all aspects of the CAC constituent; however, it may be staffed by expert faculty members as well as expert staff members from the ICT or information and communication department. While several of the cybersecurity training module activities rely primarily on faculty members responsible for the training modules, the faculty member's academic units (for example, departments) should be integral to managing training modules and interactions/accountability with other constituent (ICTS). Thus, feedback from assessments can be used to ameliorate the CATM-x design, delivery, training modules, and/or the CAFA and its associated policies and procedures.

7. Conclusions

Incorporating cybersecurity into academia, irrespective of major, and making it part of the required skills to graduate (with a certificate) is challenging, especially if there is a desire to systematically maintain and continuously improve the awareness among graduates of academic institutions. The CAFA introduced in this work can serve as a starting point for academic institutions to establish new, or amend existing, policies and procedures; the proposed framework itself would first have to be adjusted to be compatible with the missions of institutions and their available resources.

Institutions have their own missions, modes of operations, infrastructures, facilities, and budgets. All of these are factors that may influence the structures of their CAFAs. For example, budgetary constraints may require managing, adapting, or innovating scenario-based gamification practices that can be implemented using technologies that are already available in the institution. Institutions that are being founded may decide to first generate a CAFA and subsequently establish some of their formal entities on its basis. For example, the CAC may be an "office of teaching and learning" whose duties include the ones listed in their CAFA; similarly, the ICTS may be an "office of information and communication technology". Established institutions may use a CAFA to review the effectiveness of their existing training modules operations and, correspondingly, establish new formal entities or assign new duties to existing ones.

Just as this work has focused on the "cybersecurity awareness center" constituent of the CAFA, future work will develop the modules in the other constituent, "information and communication technology support". The CAFA will then be used to develop other components of the IQAS; this system includes continuous improvement mechanisms that are necessary for institutions to adapt to the constantly evolving cybersecurity and technological landscapes.

Author Contributions: The authors equally contributed to this work; the conceptual framework was developed by all three authors; the literature review was conducted by M.K. (Mohammed Khader); the original draft was prepared by M.K. (Mohammed Khader), and edited by M.K. (Marcel Karam) and H.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are grateful to the Applied Science Private University, Amman, Jordan, for the full financial support granted to cover the publication fee of this research article.

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

References

1. McCrohan, K.F.; Engel, K.; Harvey, J.W. Influence of Awareness and Training on Cyber Security. *J. Internet Commer.* **2010**, *9*, 23–41. [CrossRef]
2. Troia, V. The Cybersecurity Framework as an Effective Information Security Baseline: A Qualitative Exploration. *ProQuest Diss. Theses* **2018**, 10933040.
3. Siddiqui, Z.; Zeeshan, N. A Survey on Cybersecurity Challenges and Awareness for Children of all Ages. In Proceedings of the 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 17–18 August 2020; pp. 131–136. [CrossRef]
4. Alharbi, T.; Tassaddiq, A. Assessment of Cybersecurity Awareness Among Students of Majmaah University. *Big Data Cogn. Comput.* **2021**, *5*, 23. [CrossRef]
5. Garba, A.; Sirat, M.B.; Hajar, S.; Dauda, I.B. Cyber Security Awareness Among University Students: A Case Study. *Sci. Proc. Ser.* **2020**, *2*, 82–86. [CrossRef]
6. Moallem, A. Cyber Security Awareness Among College Students. In *Advances in Intelligent Systems and Computing*; Springer: Berlin/Heidelberg, Germany, 2019; Volume 782, pp. 79–87. [CrossRef]
7. Garba, A.A.; Jeribi, F.; Al-Shourbaji, I.; Alhameed, M.; Reegu, F.; Alim, S. An Approach to Weigh Cybersecurity Awareness Questions in Academic Institutions Based on Principle Component Analysis: A Case Study of Saudi Arabia. *Int. J. Sci. Technol. Res.* **2021**, *10*, 319–326.
8. Slusky, L.; Partow-Navid, P. Students Information Security Practices and Awareness. *J. Inf. Priv. Secur.* **2012**, *8*, 3–26. [CrossRef]
9. Ahlan, A.R.; Lubis, M.; Lubis, A.R. Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Proc. Comput. Sci.* **2015**, *72*, 361–373. [CrossRef]
10. Al-Alawi, A.I.; Al-Kandari, S.M.H.; Abdel-Razek, R.H. Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University. *J. Innov. Bus. Best Pract.* **2016**, 1–24. [CrossRef]
11. Taha, N.; Dahabiyeh, L. College Students Information Security Awareness: A Comparison Between Smartphones and Computers. *Educ. Inf. Technol.* **2021**, *26*, 1721–1736. [CrossRef]
12. Aloul, F.A. The Need for Effective Information Security Awareness. *J. Adv. Inf. Technol.* **2012**, *3*, 176–183. [CrossRef]
13. Garba, A.A.; Siraj, M.M.; Othman, S.H.; Musa, M.A. A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach. *Int. J. Emerg. Technol.* **2020**, *11*, 41–49.
14. Aliyu, M.; Abdallah, N.A.O.; Lasisi, N.A.; Diyar, D.; Zeki, A.M. Computer Security and Ethics Awareness Among IIUM Students: An Empirical Study. In Proceedings of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M), Jakarta, Indonesia, 13–14 December 2010. [CrossRef]
15. Senthilkumar, K.; Easwaramoorthy, S. A Survey on Cyber Security Awareness Among College Students in Tamil Nadu. *IOP Conf. Ser. Mater. Sci. Eng.* **2017**, *263*, 042043. [CrossRef]
16. Chandarman, R.; van Niekerk, B. Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *Afr. J. Inf. Commun.* **2017**, *20*, 133–155. [CrossRef]
17. ALArifi, P.A.L.; Tootell, A.; Hyland, P. Information Security Awareness in Saudi Arabia. In Proceedings of the 2012 International Conference on Information Resources Management (CONF-IRM), Linz, Austria, 21–23 May 2020; Volume 57.
18. Alotaibi, M.; Furnell, F.; Stengel, S.; Papadaki, I. A Survey of Cyber-Security Awareness in Saudi Arabia. In Proceedings of the 11th International Conference for Internet Technology and Secured Transactions, Barcelona, Spain, 5–7 December 2016; pp. 154–158.
19. Al-Janabi, S.; Al-Shourbaji, I. A Study of Cyber Security Awareness in Educational Environment in the Middle East. *J. Inf. Knowl. Manag.* **2016**, *15*, 1650007. [CrossRef]
20. NIST-USA. National Initiative for Cybersecurity Education. Available online: https://www.nist.gov/itl/applied-cybersecurity/nice (accessed on 27 September 2021).
21. UK Government. The UK Cyber Security Strategy—Protecting and Promoting the UK in a Digital World. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (accessed on 27 September 2021).
22. Ali, W.N.A.W.; Ni, T.Q.; Idrus, S.Z.S. Social Media Cyberbullying: Awareness and Prevention through Anti Cyberbully Interactive Video (ACIV). *J. Phys. Conf. Ser.* **2020**, *1529*, 032071. [CrossRef]
23. Valcke, T.; Keer, M.W.; Schellens, H. Long-term Study of Safe Internet Use of Young Children. *Comput. Educ.* **2011**, *57*, 1292–1305. [CrossRef]
24. Al Shamsi, A.A. Effectiveness of Cyber Security Awareness Program for Young Children: A Case Study in UAE. *Int. J. Inf. Technol. Lang. Stud.* **2019**, *3*, 8–29. [CrossRef]

25. Kruger, H.; Drevin, L.; Steyn, T. A Vocabulary Test to Assess Information Security Awareness. *Inf. Manag. Comput. Secur.* **2010**, *18*, 316–327. [CrossRef]
26. Null, L. Integrating Security Across the Computer Science Curriculum. *J. Comput. Sci. Coll.* **2004**, *19*, 170–178.
27. Curricula, C. The Joint Task Force on Computing Curricula IEEE Computer Society Association for Computing Machinery. 2001. Available online: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2001.pdf (accessed on 25 September 2021).
28. Siraj, S.G.A.; Taylor, B.; Kaza, S. Integrating Security in the Computer Science Curriculum. *ACM Inroads* **2015**, *6*, 77–81. [CrossRef]
29. Taylor, B.; Kaza, S. Security Injections@Towson: Integrating Secure Coding into Introductory Computer Science Courses. *ACM Trans. Comput. Educ.* **2016**, *16*, 1–20. [CrossRef]
30. Weiss, M.; Richard, S.; Ambareen, M.; Jens, H.; Elizabeth, T.; Blair, K.; Sidd, L. Building and Supporting a Community of CS Educators Teaching Cybersecurity in 2017 (Abstract Only). In Proceedings of the 2017 ACM SIGCSE Technical Symposium, Seattle, WA, USA, 8–11 March 2017. [CrossRef]
31. Weiss, A.C.R.; Mache, J.; Hawthorne, E.; Siraj, A.; Taylor, B.; Kaza, S. Integrating Hands-on Cybersecurity Exercises into the Curriculum in 2021. In Proceedings of the 52nd ACM Technical Symposium on Computer Science Education, Virtual Event, 13–20 March 2021; p. 1358. [CrossRef]
32. Dai, J. Situation Awareness-Oriented Cybersecurity Education. In Proceedings of the 2018 IEEE Frontiers in Education Conference, San Jose, CA, USA, 3–6 October 2018; IEEE: Manhattan, NY, USA, 2018. [CrossRef]
33. Wang, J.; Brylow, D.; Perouli, D. Implementing cybersecurity into the Wisconsin K-12 classroom. In Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15–19 July 2019; Volume 2, pp. 312–317. [CrossRef]
34. Sobel, A.; Parrish, A.; Raj, R.K. Curricular Foundations for Cybersecurity. *Computer* **2019**, *52*, 14–17. [CrossRef]
35. Blair, J.R.S.; Chewar, C.M.; Raj, R.K.; Sobiesk, E. Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum. In Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education ITiCSE, Trondheim, Norway, 15–19 June 2020; pp. 82–88. [CrossRef]
36. Abawajy, J. User Preference of Cyber Security Awareness Delivery Methods. *Behav. Inf. Technol.* **2014**, *33*, 237–248. [CrossRef]
37. Socrative. Available online: www.socrative.com (accessed on 6 June 2021).
38. Eow, B.; Wanzah, Y.L.; Rosnaini, W.A.; Roselan, M. Computer Games Development and Appreciative Learning Approach in Enhancing Students' Creative Perception. *Comput. Educ.* **2010**, *54*, 146–161. [CrossRef]
39. Laszka, A.; Felegyhazi, M.; Buttyan, L. A Survey of Interdependent Information Security Games. *ACM Comput. Surv.* **2014**, *47*, 23. [CrossRef]
40. Bente, J.; Breuer, G. Why so serious? On the Relation of Serious Games & Learning. *J. Comput. Game Cult.* **2010**, *4*, 7–24.
41. Kahoot. Available online: https://kahoot.com/ (accessed on 6 June 2021).
42. Rajendran, D.P.D.; Rangaraja, P.S. An e-ADR (elaborated action design research) Approach Towards Game-based Learning in Cybersecurity Incident Detection and Handling. In Proceedings of the Hawaii International Conference on System Sciences, Wailea, HI, USA, 7–10 January 2020. [CrossRef]
43. CyberCIEGE. Center for Cybersecurity and Cyber Operations. Available online: https://nps.edu/web/c3o/cyberciege (accessed on 5 July 2021).
44. Röpke, R.; Schroeder, U. The Problem with Teaching Defence Against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education. In Proceedings of the 11th International Conference on Computer Supported Education, Heraklion, Greece, 2–4 May 2019. [CrossRef]
45. Mio, C.; Ventura-Medina, E.; João, E. Scenario-based eLearning to Promote Active Learning in Large Cohorts: Students' Perspective. *Comput. Appl. Eng. Educ.* **2019**, *27*, 894–909. [CrossRef]
46. Lupiana, D. Development of A Framework to Leverage Knowledge Management Systems to Improve Security Awareness. 2008. Dissertations. 6. Available online: https://arrow.tudublin.ie/scschcomdis/6 (accessed on 7 September 2021).
47. Shen, L. The Nist Cybersecurity Framework: Overview and Potential Impacts. *J. Internet Law* **2014**, *18*, 3–6.
48. Kortjan, N.; von Solms, R. A Conceptual Framework for Cyber Security Awareness and Education in SA. *South Afr. Comput. J.* **2014**, *52*, 29–41. [CrossRef]
49. Katsantonis, N.M.; Kotini, I.; Fouliras, P.; Mavridis, I. Conceptual Framework for Developing Cyber Security Serious Games. In Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON), Dubai, United Arab Emirates, 8–11 April 2019; pp. 872–881. [CrossRef]
50. Tirumala, S.S.; Valluri, M.R.; Babu, G.A. A Survey On Cybersecurity Awareness Concerns, Practices and Conceptual Measures. In Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2019; pp. 1–6. [CrossRef]
51. Peker, Y.K.; Ray, L.; da Silva, S. Online Cybersecurity Awareness Modules for College and High School Students. In Proceedings of the 2018 National Cyber Summit (NCS), Huntsville, AL, USA, 5–7 June 2018; pp. 24–33. [CrossRef]
52. Schreider, T. *Building an Effective Cybersecurity Program*, 2nd ed.; Rothstein Publishing: Brookfield, CT, USA, 2019.