Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2, 657-669
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i2.4564

Towards the evaluation of cybersecurity threats and challenges in higher education institutions in Saudi Arabia

Muhammad Asif Khan[1*], Abdelrahman Abdelaziz Almulhim[2], Safiullah Salem Alkati[3]
[1]College of Computer Science and Engineering Taibah University, Madina al Munawwara, Saudi Arabia; asifkhan2k@yahoo.com (M.A.K.)
[2]College of Computer Science and Information Technology King Faisal University, Al Ahsa, Saudi Arabia; a.almulhim190@gmail.com (A.A.A.)
[3]College of Computer Science and Information Science Imam University, Riyadh, Saudi Arabia; safik01@hotmail.com (S.S.A.)

Abstract: Digital technologies have become an integral part of the higher education domain, and various platforms are available for students, faculty, and staff to interact with each other. The growth of cyberspace has also increased the threats and challenges of cybersecurity in higher education institutions. Cybersecurity criminals target these institutions for personal gain and compromise sensitive data. Most universities, especially in Saudi Arabia, consider their technology infrastructure secure from hackers without understanding the extent of their vulnerability. The current study aims to investigate the issues, threats, and challenges of cybersecurity faced by universities in Saudi Arabia. The assessment of cybersecurity has been evaluated based on the NIST cybersecurity framework, which is the most widely used cybersecurity framework in the industry. The study employed a descriptive research design and a mixed methodology of qualitative and quantitative methods to elicit data from various sources. The findings of the study will help universities strengthen their cybersecurity and address the issues and challenges they are facing. Finally, some recommendations have been provided to assist universities in maintaining data integrity and confidentiality.

Keywords: *Cybersecurity assessment, Cybersecurity framework, Cybersecurity, Cybersecurity threats, Saudi universities.*

1. Introduction

The increasing growth of internet has transformed the way we do business and communicate with each other. Internet has become an integral part of every walk of life such as financial institutions, government agencies, health sectors, educational institutions, manufacturing companies, supply chain management systems etc. [1]. The exponential growth of internet and new emerging technologies have increased cybersecurity threats in organizations. A cybersecurity is to secure digital data available over the networked devices which can be processed and stored in information systems [2]. A cybersecurity is an art that prevents devices, networks and data from illegal access and ensures integrity, confidentiality and accessibility of information [3]. Today, rapid growth of internet and information technologies have created a cyberspace analogous to the physical world facilitating communication and transfer of information among users around the world [4]. Cyberspace has revolutionized human life which impacted every walk of life.

Now business organizations, government agencies and individuals are using cyberspace to make business transactions, to do effective governance and to exchange data from one region to another worldwide. Cyberspace provides an environment that helps users to accomplish the tasks that could not be thought few decades ago due to limitations in physical world. In result of growing use of cyberspace, cybersecurity has emerged which ensures the security of information and organizational infrastructure,

History: Received: 3 December 2024; Revised: 22 January 2025; Accepted: 24 January 2025; Published: 3 February 2025
* Correspondence: asifkhan2k@yahoo.com

maintenance and availability of computer resources. The automation of devices and subsystems has attracted cyber attackers and cyber criminals which underscored the need of cybersecurity measures [5]. Cyber criminals can destroy organizational reputation by stealing and compromising data of the organization, therefore, cybersecurity is essential to protect valuable data and it warrants security of organizational infrastructure and integrity of information. As stated earlier the exponential growth of internet has revolutionized the human lives and internet of things (IoT) has emerged a new paradigm in which billions of devices are connected via internet. The communication of such devices is IP-based via internet and helps monitoring smart homes, smart appliances, smart buildings and smart vehicles [6]. Such cyber-physical system comprises of physical elements including hardware, software and networking devices. These devices communicate through built-in sensors, processes, networking and control mechanical movement [7]. In order to protect cyberspace and cyber environment, many organizations have developed security mechanisms against the security threats and vulnerabilities but all proved to be insufficient. In wake of increased cybersecurity incidents organizations consider protection of internet users as a prime issue throughout the world [8]. The prevailing shortage of skilled cybersecurity professionals compels organizations to unearth other means of enhancing security measures to prevent from data breaches and security incidents.

With the increasing trend of using new technologies our everyday lives rely on technologies and at present, most of the businesses and social activities are carried out in cyberspace. As a result, cyberattacks have increasingly become common in cyberspace and any anomaly, vulnerability or insecurity in the cyberspace directly impacts the users [9]. Cybercrimes cannot be eliminated merely placing cybersecurity technical measures alone, but there is a need to draw and implement strategic decisions. In organizations the decision makers should heed to the nature of cyberattacks and assess impact of the attacks. Organizations are heavily investing on cybersecurity and they must keep and maintain the security beyond the reach of hackers especially web applications which are main target of hackers. Organizations regardless the type of business are using cyberspace for the business growth and, in turn, generation of huge amount of data causes security issues.

In order to protect data and implementation of effective cybersecurity in organizations, it is important to evaluate cybersecurity knowledge among employees. Organization should know the capability of managing knowledge within the firms. The capability of knowledge management refers to the utilization of knowledge acquired by employees in result of mutual interaction, exchange of information, training and sharing knowledge within organization. The management of knowledge helps organizations to identify gaps in knowledge and experience in the context of cybersecurity. There are many studies conducted to evaluate employee skills, knowledge, awareness and continuous skill development of cybersecurity in organizations [10-13]. Typically, cybersecurity incidents occur within organizations due to employees who unintentionally get involved in breach of data integrity and cybersecurity [14]. These incidents occur due to lack of cyber security awareness (CSA); and organizations have started implementation of cybersecurity strategies and CSA programs, but limited understanding about CSA causes failure most of the programs [15]. A study reported by Marousis [16] found that despite of security training provided to employees in an organization, more than half of the employees were failed in a basic test of security. This shows there are other factors which contribute to the awareness of cybersecurity such as security interest and active engagement of participants in a training program [17].

Organizations including educational institutions are investing huge amount of money to secure information assets, but despite of heavy investment cybersecurity issues and challenges could not be eradicated. The security issues, continuous cyberattacks and data breach incidents motivated us to assess whether higher education institutions (HEIs) have effective implementation of security functions and security controls. To do this we selected NIST Cybersecurity Framework (CSF) 2.0 which is the latest and most widely used cybersecurity framework. For this study we formulated following research question:

RQ: How well the universities in Saudi Arabia are prepared to meet the challenges of cybersecurity?

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

The article proceeds with the following sections. In the next section II, a review of related literature including different cybersecurity frameworks is presented. In section III, we discuss research methodology. Section IV presents results and discussion and in section V conclusion is presented.

2. Literature Review

Cybersecurity has become a major concern to all businesses as the rapid growth in technologies has increased threats and vulnerabilities in all domains. The post-pandemic caused generation of massive amount of data in all walks of life due to online activities. The activities include education sector where universities and colleges started offering online courses to wide range of students. HEIs are offering either hybrid (in-person and online) degree programs or completely online programs which create high volume of students and faculty data. The high volume of diverse data in HEIs entails research results, publications, patents, faculty and student personal information, academic records, institutional policies and business rules etc. Although, education systems, applications, training, content delivery, assessments, data storage etc. have been online for decades, but following the pandemic Covid-19 the world notice a boom in online education, now online education is sprawling in societies and students, faculty members, staff connect their devices over networks which, sometimes are connected with poorly and insecure wireless network. Therefore, HEIs have become attractive targets for hackers and cybercriminals who hack relatively insecure network of HEIs.

The University of Hawaii system was breached and in turn, data of 2400 faculty members and students was compromised in a spear phishing attack [18]. Similarly, another incident of data breach was reported by University of Hawaii Maui College in which the cyber attackers compromised students' data [19]. In Yale University, the cyberattack compromised personal data of 119000 students and staff including their social security numbers and addresses [20].

Universities also faced financial losses due to cyberattacks, for example, University of California paid $1.14 million in lieu of ransomware attack [21]. In 2023, it was reported that cybercriminals hacked the systems of University of Minnesota, University of Georgia, Indian University in different times and accessed student financial applications data, personal information from MOVEit software and data from unprotected Azure storage blogs; and demanded big ransoms [22]. In University of Portsmouth, UK a ransomware attack by cybercriminals closed the entire campus for few days and delayed inception of the term [23]. In HEIs ransomware threat has become an increasing threat due to diversified sensitive data. The attackers install ransomware software on computer or network system which denies to access data without paying a ransom [24, 25]. In 2022, the National Cyber Security Center (NSC), UK reported 93% increase in cyberattacks targeting education sector in 12 months and 62% HEIs experienced cyberattacks weekly. The report further mentioned the cyberattacks resulted 71% HEIs negatively i.e. either loss of data or money [26].

2.1. Cybersecurity Threats in HEIs

In result of increasing digitization education sector is facing cybersecurity threats and following we describe some most common threats found in HEIs.

2.1.1. Phishing

Cybercriminals use this technique to allure users to respond to their request for collecting personal information and as soon as hackers access to the user account, an incident of either money loss or data loss occurs. The main objective of this technique is to illegally access user credit card and login information [27].

2.1.2. Spam

Cyber attackers send unwanted emails to students and faculty for updating their information and instruct users to click on a link provided with the message. Sometimes a virus file is attached with the message spreads viruses in the system.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

2.1.3. Ransomware

It is a used by cybercriminals to encrypt data and files in system until a ransom is paid before decrypting data and files. In 2017, there were 23,000 companies around the world were infected by ransomware and Bitcoin ransom was demanded in lieu of unlocking and returning data [28].

2.1.4. Denial of Service

Cyber attackers bombarded a website with huge number of fake requests to make website unavailable to respond actual users. The server behind the website does not function properly and service is denied to users. Recently in a denial-of-service attack Cambridge University, UK was attacked by cyber criminals and disrupted the internet and educational platform services [29].

2.1.5. SQL Injection

Cybercriminals insert a malicious code into SQL query though the input data filed to a web application in order to manipulate data stored in database. In HEIs cyber attackers gain access to the database and can manipulate sensitive information such as student, staff, faculty, financial and business processes information exist.

2.2. Cybersecurity Vulnerabilities in HEIs

A vulnerability is a hidden risk that is not exploited advertently or accidentally by a cyber attacker or a normal user. Following are some common vulnerabilities found in HEIs.

2.2.1. Obsolete Infrastructure

When technology infrastructure has a lack of security updates it becomes target of cyber attackers who gain illegal access to assets, interccept packets passing through the weak network.

2.2.2. Software Misconfiguration

Due to some misconfiguration of a software, security functions are disabled which causes cyber attackers to gain illegal access to the system.

2.2.3. Exposure to Data

Faculty, student or other staff are given access and different extra privileges to data which attackers could access or even employees could misuse the given access and compromise data.

2.2.4. Poor Encryption

A weak network may cause poor data encryption or no encryption which hackers may take benefit and compromise critical data including student information, faculty and staff data and university policies on server.

In HEIs the security challenges stem largely due to the culture of information sharing and collaboration among faculty, students, researchers and staff [30]. Unlike most industries, HEIs are recognized by their transparency and openness. The networks of HEIs are accessible to public who connects personal devices with the universities networks and systems, in turn, cause security vulnerabilities. The security threats and vulnerabilities usually are managed by strengthening technology infrastructure and business strategies aligned with technologies. However, most of the cybersecurity incidents occur due to human mistakes and ignorance of security policy [31]. In order to monitor organizational performance, there are key performance indicators (KPIs) which evaluate the security performance in organizations. There were three types of cybersecurity KPIs described by Aven [32] which help to assess technical activities, effectiveness of security training programs and employee awareness, and to build security scorecard. But with advancement of technology and passing time the KPIs are no more effective and could not provide useful information to organizations. Usually, KPIs are developed based on the best practices in organizations which vary from one organization to another.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

Therefore, HEIs need some other tools to measure and protect their assets from cybersecurity risks and threats. There are various frameworks developed for different stakeholders to evaluate and monitor the effectiveness of cybersecurity.

2.3. Cybersecurity Frameworks

Cybersecurity frameworks are usually collection of best practices and standards that guide organizations to evaluate security threats and vulnerabilities in an organization. These frameworks help organizations to develop a security ecosystem against landscape of threats and vulnerabilities to protect their assets.

We provide a brief description of only few frameworks that are known and operative in education sector especially HEIs.

2.3.1. National Initiative for Cybersecurity Education (NICE)

This framework is designed to craft curriculum in HEIs to be aligned with the cybersecurity requirements in the industry and to ensure learners acquire the required skills in cybersecurity ambit. The framework consists of main components as knowledge, skills, tasks, work roles, work role categories and competency measure which facilitate HEIs to systematize their approach to learners. The framework encourages student retention and application of knowledge [33]. This framework facilitates HEIs to align curriculum with the industry requirements so that students are equipped with the knowledge and tools need to the industry and they could be a part of cybersecurity workforce.

2.3.2. Critical Security Controls (CSC)

This framework is developed by Center for Internet Security (CIS) consisting of 153 best practices, 18 categories grouped into 3 implementation groups (IGs). Usually, organizations in education sector are related to IG1 and IG2 groups; and in IG1 cybersecurity and technology experts are limited and main focus is on operational continuity and protection of data. However, in IG2 cybersecurity experts and experienced management teams meet with the compliance of cybersecurity requirements [34].

2.3.3. European Cybersecurity Skills Framework

European Cybersecurity Skills (ECS) framework developed by European Union Agency for Cybersecurity (ENISA) aims to standardize training and education programs related to cybersecurity across Europe [35]. The framework helps learners to explore opportunities to link with cybersecurity industry in order to prepare cybersecurity workforce to fill the gap in the field. The framework emphasizes the need of student immersion in cybersecurity and assists in monitoring student progress.

In HEIs, this framework ensures that institutions have clear insights of career paths in their cybersecurity programs.

There are various frameworks which are used by different stakeholders including education sector. In a study conducted by Toussaint, et al. [36] different 36 cybersecurity frameworks were evaluated based on criteria set as cybersecurity compliance, comprehensiveness, standards-based and implementation guidelines. The study found only four frameworks which fulfilled the criteria, but it notable all the frameworks failed to support data integrity, in turn, a new criterion 'customizability' was included in the criteria. Thereafter, NIST cybersecurity framework turned out to be the most popular among companies and HEIs; also flexible which aids to identify risks and fills gap in security.

2.3.4. NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework 2.0 (CF 2.0) is the latest framework which provides guidelines to all types of organizations to manage cybersecurity risks. The implementation of the framework varies from one organization to another depending on type, size, level of risks, mission and objectives etc. The framework illustrates the preferred outcomes that people within an organization at all levels should understand without having any specific knowledge of cybersecurity. The outcomes are mapped to

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

security controls in order for considering to mitigate cybersecurity risks. The CF 2.0 is the latest version of cybersecurity framework in which a new function Governance and a category Cybersecurity Supply Chain Risk Management have been included.

The CF 2.0 consists of six core functions and four tiers. Each core function comprises of different categories that are preferred outcomes and each category is divided into sub categories with more specific outcomes. Each tier characterizes the compliance of cybersecurity practices in an organization. Since we intended to use CF to evaluate cybersecurity issues and challenges during the cybersecurity practices in HEIs, we developed a tool shown in Figure 1 that may help to map organizational practices to the CF functions and corresponding outcomes

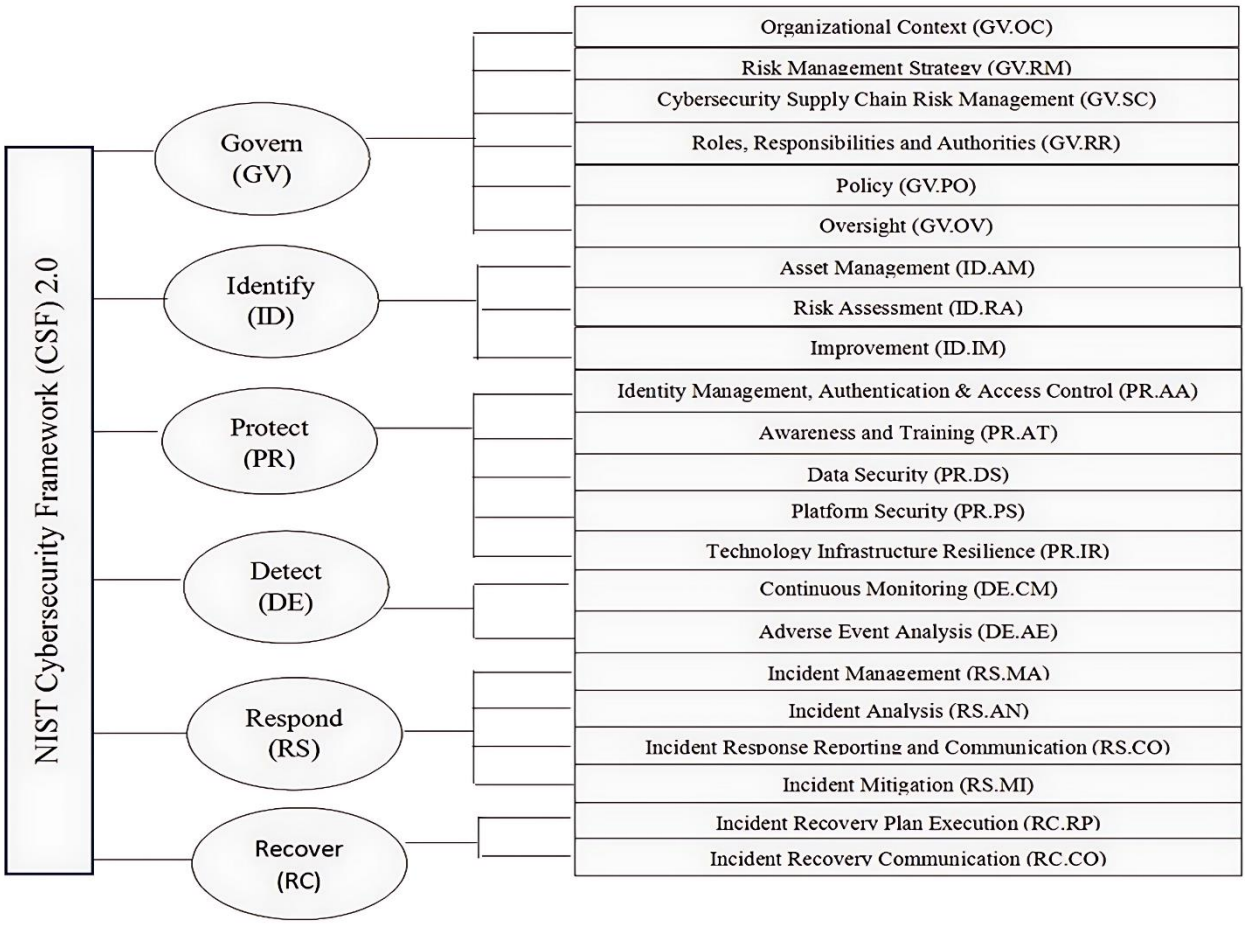

Figure 1.
Cybersecurity framework 2.0 functions and outcomes.

3. Methodology

We used a descriptive research methodology and deployed both quantitative and qualitative methods in HEIs for data collection to determine the effectiveness of their security functions using NIST CF 2.0.

We developed a survey instrument focusing on CF 2.0 in order to collect data about implementation of security functions in HEIs. The questionnaire consisted of 18 items aimed at assessing implementation of CF 2.0 functions in HEIs in Saudi Arabia. The survey was made available online for three weeks to elicit data from five different Saudi universities (three universities in Eastern province and two in Western region). However, in response to some requests one week was extended; hence data

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

collection period spans a month. The questionnaire was based on the core functions of CF 2.0 and each item was measured on five-point Likert's scale ranging from Strongly disagree-SD=1, Disagree-D=2, Agree-A=3 and Strongly agree-SA=4. We communicated to various Saudi universities using different means of communication and requested them to participate in this study and in turn five universities participated in the study. In addition to the survey, requests were made to faculty and staff of three universities to conduct interviews in order to collect data about cybersecurity issues, challenges and threats. There were 21 interviews successfully conducted with professionals at different levels which include faculty, technical and managerial staff in the universities.

4. Results and Discussion

The respondents participated in the survey voluntarily and their voluntarily participation was agreed before beginning of the survey. We received 143 surveys but after scrutiny we selected data of 138 surveys suitable for the study. Table 1 shows the demographic data of the participants. Most of the participants (51%) holds the Masters degrees in their field followed by Doctorate degree (30%) which implies the participants were experts, professionals and knowledgeable in cybersecurity field.

Table 1.
Demographic information of participants.

	No. of responses	% of participants
Gender		
Male	73	53
Female	65	47
Education		
PhD	42	30
Masters	71	51
Bachelor	18	13
Diploma	7	5
Age		
<25	11	8
25-35	48	35
36-45	37	27
46-55	28	20
>55	14	10

The majority of respondents (53%) was male as compare to female participants (47%). The slight difference of 6% shows growing number of females in information technology specially in cybersecurity field. A large number of respondents found to be in the age group of 25-35 years which shows that young participants who are highly qualified engage in cybersecurity work and have sound knowledge of cybersecurity. Another reason is that more doctorate and master candidates are completing education and joining the workforce including cybersecurity. Bachelor and diploma participants work in technical department and deal with technical issues and solve user problems.

Table 2 shows the extent of implementation CF 2.0 functions and the anticipated outputs. All universities seem to have implemented most of the functions and controls. The results depicted that low scale was 1-18, the average scale was 19-37 and high scale was 38-56. The overall mean for the implementation of CSF 2.0 in the HEIs is $\bar{x}$= 47.2 which is in the high scale and indicates that most of the functions of CSF 2.0 are implemented in HEIs. This also shows the HEIs in Saudi Arabia have adopted the cybersecurity framework and security controls are in place. However, items 5 and 16 indicate that some universities do not have effective monitoring mechanism of cybersecurity which in turn, causes cybersecurity incidents and staff remain unaware of the reasons of such incidents.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

In a study conducted by Zwilling, et al. [37] it is mentioned that most users at internet merely install antiviruses to protect themselves rather than studying reasons of cyberattacks and take concrete measures to protect from such incidents. In the universities different antiviruses, firewalls are procured and updated with patches. But the data items 5 and 16 indicate the lack of a mechanism in the universities exists to identify cybersecurity risks and to know reasons of the risks in the institutions causes failure the procurement of antiviruses. The data is evident that some universities have a lack of implementation of the CSF 2.0 functions i.e. Govern and Detect functions need to implemented completely in order to protect assets. Similarly, in order to manage assets properly and to protect them an automated process to identify flaws to assets is necessary. Therefore, the function Identify of CSF 2.0 is required to be implemented in the universities.

Following the analysis of the data we found answer of our research question that based on cybersecurity framework 2.0 functions, we argue HEIs are not fully secure and security functions such as Govern, Respond and Recovery are implemented to an extent, but Identity, Protect and Detect functions need to be implemented completely. The data depicts infrastructure is not resilient, monitoring mechanism is not effective and process to find reasons for any cyber incident cannot be found. The data shows there is a need for HEIs to monitor security functions regularly and follow the CSF 2.0 functions.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

Table 2.
The framework functions and implementation in HEIs.

S/N	Items	SD	D	A	SA	Mean	StdD
1	Cybersecurity risk management strategy and policy are communicated throughout university IT deanship	13(9.4%)	29(21%)	74(53.6%)	22(15.9%)	2.76	0.825
2	Risk management strategy incorporates supply chain risk strategy	10(7.2%)	75(54.3%)	51(36.9%)	2(1.4%)	2.33	0.623
3	Managers communicate cybersecurity priorities, accountability and resources as needs arise	12(8.6%)	36(26.0%)	57(41.3%)	33(23.9%)	2.80	0.896
4	I communicate any potential risks to my manager for appropriate action	1(0.72%)	13(9.4%)	85(61.5%)	39(28.2%)	3.17	0.608
5	We have a mechanism to monitor cybersecurity in our organization	35(25.3%)	85(61.5%)	17(12.3%)	1(0.72%)	1.88	0.625
6	Managers always focus on achieving the risk targets by controls and services stated in action plan	5(3.6%)	35(25.3%)	77(55.7%)	21(15.2%)	2.83	0.707
7	An automated process exists to identify, assess and manage any flaws in assets for their protection	25(18.1%)	72(52.1%)	40(28.9%)	1(0.72%)	2.12	0.695
8	There is a systematic process to identify vulnerabilities and threats in our IT environment	3(2.1%)	39(28.2%)	82(59.4%)	14(10.1%)	2.78	0.661
9	Implementation of appropriate controls allow access to IT resources	8(5.7%)	20(14.4%)	87(63.0%)	23(16.6%)	2.91	0.728
10	Critical data cannot be accessed without digital identification	4(2.8%)	37(26.8%)	77(55.7%)	20(14.4%)	2.82	0.714
11	Attended cybersecurity awareness training program organized by the university	8(5.7%)	26(18.8%)	94(68.1%)	10(7.2%)	2.77	0.661
12	We have a centralized platform and controls to protect data and network	17(12.3%)	42(30.4%)	56(40.5%)	23(16.6%)	2.62	0.896
13	Our organization's infrastructure is resilient to prevent from cybersecurity incidents	1(0.72%)	81(58.6%)	52(37.6%)	4(2.8%)	2.43	0.573
14	We all keep ourselves well aware of cybersecurity, threats and vulnerabilities1	21(15.2%)	45(32.6%)	37(26.8%)	35(25.3%)	2.62	1.022
15	We analyze any anomalous event to detect any cybersecurity incident	3(2.1%)	22(15.9%)	78(56.5%)	35(25.3%)	3.05	0.707
16	We have a process to identify the reasons of any cybersecurity incident and possible measures to protect from such incidents	37(26.8%)	80(59.2%)	18(13.0%)	3(2.1%)	1.91	0.687
17	We are capable to restore business activities following a cybersecurity incident	5(3.6%)	30(21.7%)	66(47.8%)	37(26.8%)	2.98	0.796
18	We communicate with partners within and outside of the organization	26(18.8%)	40(28.9%)	59(42.7%)	13(9.4%)	2.43	0.914

In order to determine the cybersecurity threats, challenges and issues in universities, we conducted 21 interviews with faculty, technical and managerial staff in three Saudi universities on the condition to maintain privacy and anonymity. We asked 15 open and close ended questions during the interviews to each of the interviewees. The interviewees described different cyberattacks and threats in the respective institution.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

We used Likert's scale to place their responses as (Strongly disagree-SD=1, Disagree-D=2, Agree-A=3, Strongly agree-SA=4) against each of the items. Table 3 shows the items we investigated during the interviews. The interviewees responded that the institutions were subjected to different cyberattacks and threats. This data depicts more than 50% of the interviewees replied positively that the universities have been subjected to various cyberattacks. The data shows 57% interviewees considered themselves to have incapability of managing cybersecurity threats and risks as the main challenge. One of the challenges HEIs found that cybercriminals use various techniques which cannot be identified by the detection systems. These challenges were mentioned by Nadir et al. [38] in a research study. It depicts from the data that 80% respondents have awareness of cybersecurity and most of the respondents i.e. 75% have good communication with each other, but still unable to manage cyber threats and risks. The results showed the low scale is 1-14, average scale is 15-29 and high scale is 30-44. The overall mean of cyber threats, issues and challenges is $\bar{x} = 40.6$ which depicts the cyberattacks and threats to HEIs.

Table 3.
Cyberattacks, threats and issues in HEIs.

S/N	Items	SD	D	A	SA	Mean	StdD
1	Implementation of cybersecurity strategy and policy in place	3(14.3%)	8(38.1%)	8(38.1%)	2(9.5%)	2.4	0.87
2	A proper protection of devices is implemented	2(9.5%)	2(9.5%)	11(52%)	6(28.6%)	3.0	0.90
3	Ransomware attacks occurred in institution	4(19%)	7(33%)	9(43%)	1(4.8)	2.3	0.90
4	Access control attacks occurred	2(9.5%)	9(42.9%)	6(28.6%)	4(19%)	2.5	0.93
5	Experienced phishing attack	2(9.5%)	6(28.6%)	12(57.1%)	1(4.8%)	2.5	0.75
6	Denial of service attacks happened	2(9.5%)	6(28.6%)	10(47.6%)	3(14.3%)	2.6	0.86
7	Experience of spyware	2(9.5%)	3(14.3%)	10(47.6%)	6(28.6%)	3.0	0.90
8	Malware attacks happened	1(4.8%)	6(28.6%)	11(52.4%)	3(14.3%)	2.8	0.80
9	Implementation of intrusion detection systems	2(9.5%)	6(28.6%)	6(28.6%)	7(33.3%)	2.8	1.01
10	Cybersecurity knowledge & awareness	2(9.5%)	2(9.5%)	11(52.4%)	6(28.6%)	3.0	0.89
11	Communicate risks to higher level	4(19%)	2(9.5%)	13(61.9%)	2(9.5%)	2.6	0.92
12	Digital identification to access assets	3(14.3%)	2(9.5%)	12(57.1%)	4(19%)	2.8	0.93
13	Communication among partners	2(9.5%)	3(14.3%)	13(61.9%)	3(14.3%)	2.8	0.81
14	Occurrence of cyber incidents	1(4.8%)	5(9.5%)	10(47.6%)	5(9.5%)	2.9	0.83
15	Capability to manage security threats and risks	2(9.5%)	10(47.6%)	8(38.1%)	1(4.8%)	2.3	0.74

In order to figure out the number of occurrences of cyberattacks, threats, vulnerabilities and challenges we synthesized the interviews data and discovered the average frequency of different attacks, threats and challenges was 10. The majority of the interviewees responded positively that their institutions experienced cyberattacks in different timings. Table 4 depicts the frequency of threats and vulnerabilities with the preventive measures taken by the institutions.

It is evident from the data that most common attack among the institutions is malware attack which has high frequency of attacks. There also have been attacks and threats of illegitimate access of data by device tampering or otherwise. Phishing attacks are also considered a significant challenge for the higher education institutions and a number of preventive measures have been taken by the institutions.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564

Table 4.
Cybersecurity threats, vulnerabilities and challenges in HEIs.

Threat/Vulnerability/ Challenge	Incident frequency (Mean)	Number of participants	Preventive measures taken
Denial of service	<10	13(62%)	-Virtual network - Distribution of traffic - Blocking unknown source - Limiting rate of traffic - Traffic monitoring - Awareness training
	>=10	8(38%)	
Tampering of hardware	<10	12(57%)	-Verifying firmware -Using sensors to protect from device tampering -Monitoring integrity of firmware -Hardware-linked boot
	>=10	9(43%)	
Ransomware	<10	16(76%)	-Using updated antiviruses -Backup data regularly -Never open unknown files -Install anti-ransomware software
	>=10	5(24%)	
Unauthorized access control	<10	13(62%)	-Monitoring users activities -Employing strong password strategy -Establishing strong infrastructure
	>=10	8(38%)	
Phishing	<10	12(57%)	-Awareness sessions -Blocking unknown sources -Using ant-spam filter -Never open suspicious mails
	>=10	9(43%)	
Malware	<10	7(33%)	-Implement and monitor security policy -Never download suspicious files -Update operating systems -Monitoring and analyzing network activities -Backup data regularly
	>=10	14(67%)	
Rogue user access	<10	17(81%)	-Monitor network activities -Monitor user activities -Employing strong password strategy -Keep strong infrastructure -Awareness programs
	>=10	4(19%)	
Mobile device users	<10	18(86%)	-Monitoring traffic -Multi-factor authentication -Restrictions on some websites -Restrictions on downloads -Implementation of encryption policy
	>=10	3(14%)	

The data completes the answer of our research question of the threats, vulnerabilities and challenges the HEIs are facing such as malware, phishing, denial of service, device tampering, rogue and mobile users.

The data depicts there are rogue users and staff who are legitimate users, but use their own The HEIs face many challenges as listed above, but one the main challenges is the cyber attackers use various techniques which are not identified by the detection systems. Nadir, et al. [38] conducted a study of the cyber challenges being faced by organizations.

5. Conclusion

The latest and emerging technologies have revolutionized organizations and their business processes. At one hand organizations ripe the benefits of technologies, on the other hand they strive to deal with cyber threats which arise due to technologies. Higher education institutions are also engaged in dealing with cybercrimes and growing number of cyberattacks ad threats compel them to implement security measures. Our study showed that HEIs have security controls, security policy and strategy, but the implementation of strategy does not exist to the required extent. In a study Woody and Creel [39] also mentioned that merely taking security measures in organizations cannot protect assets unless

cybersecurity strategy is implemented. In this study we elicited data using a survey instrument conducted interviews with faculty, technical and managerial staff of different universities and the interviewees elaborated various cyberattacks in their institutions. The data showed cyberattacks such as phishing, illegal access control, denial of service, malware found to be common in HEIs. Also, in some HEIs the monitoring mechanism is either ineffective or does not exist. Although, training and awareness programs of cybersecurity are organized in HEIs, but most of the interviewees suggested to include cybersecurity courses in the regular curriculum to prepare skilled and knowledgeable work force.

We recommend that HEIs should disseminate cybersecurity awareness and knowledge by introducing cybersecurity courses in their programs. Also, CSF 2.0 should be implemented completely in order to be protected from cyberattacks specially cybersecurity strategy should be implemented effectively in addition to the security measures.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Acknowledgements:

The authors would like to thank to all the participants who participated in this study and provided us valuable information.

References

[1] H. Kavak, J. Padilla, D. Vernon-Bido, S. Y. Diallo, R. Gore, and S. Shetty, "Simulation for cybersecurity: State of the art and future directions," *Journal of Cybersecurity*, vol. 7, no. 1, pp. 1-13, 2021. https://doi.org/10.1093/cybsec/tyab005

[2] B. von Solms and R. von Solms, "Cybersecurity and information security—what goes where?," *Information and Computer Security*, vol. 26, no. 1, pp. 2–9, 2018. https://doi.org/10.1108/ICS-04-2017-0025

[3] CISA, "What is cyber security. America's cyber defense agency," Retrieved: https://www.cisa.gov/news-events/news/what-cybersecurity 2024.

[4] L. De Kimpe, K. Ponnet, M. Walrave, T. Snaphaan, L. Pauwels, and W. Hardyns, "Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims," *Computers in Human Behavior*, vol. 108, p. 106310, 2020. https://doi.org/10.1016/j.chb.2020.106310

[5] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean & Coastal Management*, vol. 236, p. 106493, 2023. https://doi.org/10.1016/j.ocecoaman.2023.106493

[6] F. E. Abrahamsen, Y. Ai, and M. Cheffena, "Communication technologies for smart grid: A comprehensive survey," *Sensors*, vol. 21, no. 23, p. 8087, 2021. https://doi.org/10.3390/s21238087

[7] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, 2017. https://doi.org/10.1109/JIOT.2017.2703172

[8] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," *Electronic Research Archive*, vol. 31, no. 2, pp. 708-728, 2023. https://doi.org/10.3934/era.2023035

[9] M. Amir and T. Givargis, "Pareto optimal design space exploration of cyber-physical systems," *Internet of things*, vol. 12, p. 100308, 2020. https://doi.org/10.1016/j.iot.2020.100308

[10] M. Kianpour and S. Raza, "More than malware: Unmasking the hidden risk of cybersecurity regulations," *International Cybersecurity Law Review*, vol. 5, pp. 169–212, 2024. https://doi.org/10.1365/s43439-024-00111-7

[11] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers & Security*, vol. 95, p. 101827, 2020. https://doi.org/10.1016/j.cose.2020.101827

[12] J. Dawson and R. Thomson, "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance," *Frontiers in Psychology*, vol. 9, p. 744, 2018. https://doi.org/10.3389/fpsyg.2018.00744

[13] L. Nautiyal and A. Rashid, "A framework for mapping organisational workforce knowledge profile in cyber security," *Computers and Security*, vol. 145, p. 103925, 2024. https://doi.org/10.1016/j.cose.2024.103925

[14] J. Hancock, "The psychology of human error: Understand the mistakes that compromise your company's cybersecurity. Tessian Research," Retrieved: https://www.tessian.com/resources/psychology-of-human-error-2022/ 2022.

[15] S. Chaudhary, V. Gkioulos, and S. Katsikas, "A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises," *Computer Science Review*, vol. 50, p. 100592, 2023. https://doi.org/10.1016/j.cosrev.2023.100487

[16] A. Marousis, "Cybersecurity training lags, while hackers capitalize on COVID-19. TalentLMS," Retrieved: https://www.talentlms.com/blog/cybersecurity-statistics-survey/ 2021.

[17] A. Christiano and A. Neimand, "Stop raising awareness already," *Stanford Social Innovation Review*, vol. 15, no. 2, pp. 34-41, 2017. https://doi.org/10.48558/7ma6-j918

[18] MDL, "Hawaii data breach," Retrieved: https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/university-of-hawaii-data-breach/ 2024.

[19] JDSUPRA, "University of Hawaii Maui College announces recent data breach," Retrieved: https://www.jdsupra.com/legalnews/university-of-hawaii-maui-college-7130666/ 2024.

[20] H. Fuchs, "Yale faces lawsuit for data breach. Yale Daily News," Retrieved: https://yaledailynews.com/blog/2018/08/31/yale-faces-lawsuit-for-data-breach/ 2018.

[21] J. Tidy, "How hackers extorted $1.14m from University of California, San Francisco. BBC News," Retrieved: https://www.bbc.co.uk/news/technology-53214783 2020.

[22] Z. Scott, "A recap of recent cybersecurity incidents at universities. Schellman," Retrieved: https://www.schellman.com/blog/cybersecurity/cybersecurity-incidents-at-universities-2023 2023.

[23] N. Fatkin, "University of Portsmouth beefs up its security after 'cyber incident' as campus reopens. The News," Retrieved: https://www.portsmouth.co.uk/education/university-of-portsmouth-eefsup-it-security-after-cyber-incident-as-campus-reopens-3207773 2021.

[24] T. Nusairat, M. M. Saudi, and A. B. Ahmad, "A recent assessment for the ransomware attacks against the internet of medical things (iomt): A review," in *2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE). https://doi.org/10.1109/ICCSCE56670.2023.101234*, 2023: IEEE, pp. 238-242.

[25] B. Khammas, "Ransomware detection using random forest technique," *ICT Express*, vol. 6, no. 4, pp. 325-331, 2020. https://doi.org/10.1016/j.icte.2020.04.004

[26] Moor Clearcomm, "The cyber threat to education and academy trusts in the UK," Retrieved: https://mooreks.co.uk/wp-content/uploads/2022/10/Cyber-Threat-to-Education.pdf 2022.

[27] A. Kazemi, M. Golkar, and S. Lajmiri, "Origins of cyber security: Short report," *International Journal of Reliability, Risk and Safety*, vol. 6, no. 2, pp. 77-83, 2023. https://doi.org/10.1080/23738871.2023.1009894

[28] S. Mohurle and M. Patil, "A brief study of wannacry threat: Ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938-1940, 2017.

[29] L. John, "Cambridge university hit by DDoS attack. Computing," Retrieved: https://www.computing.co.uk/news/4176168/cambridge-university-hit-ddos-attack 2024.

[30] N. S. Fouad, "Securing higher education against cyberthreats: from an institutional risk to a national policy challenge," *Journal of Cyber Policy*, vol. 6, no. 2, pp. 137-154, 2021. https://doi.org/10.1080/23738871.2021.1973526

[31] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Computers & Security*, vol. 66, pp. 40-51, 2017. https://doi.org/10.1016/j.cose.2017.01.004

[32] T. Aven, "On the allegations that small risks are treated out of proportion to their importance," *Reliability Engineering & System Safety*, vol. 140, pp. 116-121, 2015. https://doi.org/10.1016/j.ress.2015.02.017

[33] NICE, "Events, expo and conferences," Retrieved: https://niceconference.org/events/ 2024.

[34] Coro, "Three cybersecurity frameworks for school systems," Retrieved: https://www.coro.net/blog/three-cybersecurity-frameworks-for-school-systems 2024.

[35] The SANS Institute, "Cyber security skills roadmap," Retrieved: https://www.sans.org/cyber-security-skills-roadmap 2024.

[36] M. Toussaint, S. Krima, and H. Panetto, "Industry 4.0 data security: A cybersecurity frameworks review," *Journal of Industrial Information Integration*, vol. 39, p. 100604, 2024. https://doi.org/10.1016/j.jii.2024.100604

[37] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82-97, 2022. https://doi.org/10.1080/08874417.2020.1712269

[38] O. Nadir, S. Ahmad, T. Ahmed, and E. Rasha, "Cybersecurity threats detection using optimized machine learning frameworks," *Computer Systems Science & Engineering*, vol. 48, no. 1, pp. 77-95, 2024. https://doi.org/10.32604/csse.2023.039265

[39] C. Woody and R. Creel, "P21-071: Challenges in building and implementing an effective cybersecurity strategy, Software Engineering Institute, Carnegie Mellon University," Retrieved: https://apps.dtic.mil/sti/trecms/pdf/AD1126968.pdf 2021.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 2: 657-669, 2025
DOI: 10.55214/25768484.v9i2.4564