Cyber Threat Intelligence in Risk Management

A Survey of the Impact of Cyber Threat Intelligence on Saudi Higher Education Risk Management

Amira M. Aljuhami, Doaa M. Bamasoud
Dept. of IS
College of Computing and Information Technology
University of Bisha, Bisha
Saudi Arabia

***Abstract*—Cyber Threat Information (CTI) has emerged to help cybersecurity professionals keep abreast of and respond to rising cyber threats (CT) in real-time. This paper aims to study the impact of cyber threat intelligence on risk management in Saudi universities in mitigating cyber risks. In this survey, a comprehensive review of CTI concepts and challenges, as well as risk management and practices in higher education, is presented. Previous literature was reviewed from theses, reviews, and books on the factors influencing the increase of cyber threats and CTI as well as risk management in higher education. A brief discussion of previous studies and their contribution to the current paper and the impact of CTI on risk management to reduce risk. An extensive search of more than 65 research papers was conducted and 28 were cited in this survey. Cyber threats are changing in addition to the huge flow of information about them and dealing with these threats on time requires advance and deep information about the nature of these threats and how to take appropriate defensive measures, and this is what defines the concept of CTI. The use of cyber threat information in risk management enhances the ability of defenders to mitigate growing cyber threats.**

Keywords—Cyber threat intelligence; risk management; cyberthreat; cyber security

I. Introduction

In the twenty-first century, the world is witnessing a technological revolution and a qualitative shift in the field of cybersecurity significantly. From here emerged the awareness of the Kingdom of Saudi Arabia and its interaction with these changes and developments with what appears in this era. Therefore, the royal order was issued to establish the National Cybersecurity Authority and its relationship with the King, may God protect him, in line with Vision 2030, to be specialized in cybersecurity and its affairs, and it is considered the main reference for the Kingdom [1]. Rania in [2] assumed that despite this development in the Kingdom, the Kingdom is considered more vulnerable to cyber threats in the Middle East as organization face a new generation of cyber threats. It is distinguished by its ability to easily bypass traditional defenses, such as intrusion prevention systems or firewalls, etc. It has been considered effective for the previous generation of threats. The authors in [3] hypothesize that the old approach renders traditional defenses vulnerable to complex threats because they exploit unknown vulnerabilities. This requires the need to prepare for these threats through cyber threat intelligence. With this technological revolution, systems have become more complex, resulting in lower levels of security. Because of the changing forms and functions of cyber threats targeting individuals, businesses, and government agencies, cyber threats are not limited to online attackers and hackers. Instead, the authors add in [3] it has grown into threats and funds that are financed and organized for financial gain or political ends.

The authors define in [4] CTI as a means of gathering knowledge to understand what the attacker wants and predict future attacks. CTI is used to achieve appropriate awareness of conditions and cyber threats can be countered by including CTI in defense systems. Threats are analyzed based on historical information about actual incidents in the past, and as one of the advantages of information about security threats, operations are improved effectiveness and efficiency in terms of preventative capabilities and investigations. The authors argue in [5] that the purpose of the CTI is to obtain evidence to aid decision-making because what determine the ability of the security team to produce accurate and actionable threat information is the maturity, skills, and resources of the CTI.

Although technology and information continue to grow in cyberspace, it becomes difficult to identify and respond to threats on time. Therefore, CTI management is needed to reduce cybersecurity risks. This paper aims to identify the role of CTI applications in risk management in the Kingdom of Saudi Arabia.

This paper is organized into six sections. Section 2 provides a deep explanation of the concept of CTI, where its types, main challenges, and characteristics are mentioned. Section 3 explains the concept of risk and its types. It also discusses the concept of risk management, its processes, and the most prominent practices of risk management in higher education. In section 4, the most prominent previous literature that discussed the reasons for the increase of cyber threats in addition to the importance of CTI and risk management in higher education was highlighted. In Section 5 discusses the relationship of previous studies to the current paper and the extent of its support and disagreement with it is. Section 6 provides concluding observations with suggestions for some future directions.

II. Cyber Threat Intelligence

A. *Threat Intelligence (TI)*

The author in [6] defines TI as the process of understanding enterprise threats based on available data points that go beyond just collecting data points. The data must also be relevant to the organization as a whole [6]. In [7] the authors define TI as any evidence-based knowledge about threats, intending to prevent an attack or shorten the period between penetration and detection. The author explained in [6] that TI can also refer to evidence-based information, such as context, mechanisms, indicators, implications, and actionable advice for a topic regarding an existing or emerging risk or risk on an asset that can be used to make informed decisions about the response to risk or risk. TI can be information collected from a variety of technical sources (for example, local sensors) or human sources (for example, observed discussions in secret forums, communication with peers). Thus, the authors stated in [3] that threat information includes technical indicators, context, mechanisms, implications, and actionable advice about current or emerging threats.

SysAdmin Audit, Network, and Security (SANS) defines a CTI as the collection, classification, and eventual use of information about adversaries, specifical information about their tactics, to discover or block them. As mentioned by one of the authors, CTI is used to determine opponent intent [8].

The study in [9] provided several definitions of CTI that are based on processes, analysis, and domain. Hence, in [9] CTIs are defined by the authors as actions taken in cyberspace to compromise and defend protected information and capabilities in the field.

The researchers proposed in [10] the definition of CTI: as “the process and product resulting from the interpretation of raw data into information that satisfies a requirement as it relates to adversaries who have the intent, opportunity, and ability to cause harm.” The research conducted in [10] claimed that Threat Intelligence (TI) involved the process of converting data into information about the adversary.

CTI can easily become an uncontrollable alert stream. The context allows the security analyst to understand the type of threat or actor they are dealing with so that they can formulate an appropriate response plan. The three main components of a CTI are relevant, timely, and actionable. A complete CTI definition needs to cover these three elements to ensure that relevant threat data is collected, analyzed, and processed on time, and the outcome can produce actionable intelligence to aid decision-making [11].

B. *Cyber Threat Intelligence Challenges*

In [12] the authors discuss that cybercriminals use a variety of methods to attack their victims to:

- Steal their sensitive personal information (such as financial information).
- Accessing and controlling the victim’s device to commit other malicious acts such as ransomware which can provide malware (in case of Botnet) and lock/encrypt the victim’s device (in case of Botnet).

The authors argue in [12] that although different types of cyber-attacks use a variety of infection methods, in essence, they follow a similar life cycle: beginning with victim reconnaissance and ending with malicious activities on the victim's device/network.

1) Vector reconnaissance attack: Identifying the attack point and system vulnerabilities that cybercriminals can exploit is a challenge in defending against cyberattacks. In addition to the common methods that have always been used to deceive victims (for example, phishing) into performing the actions desired by the attackers, the attackers have used more intelligent and innovative methods in recent years [12]. The authors hypothesize in [12] that methods range from delivering malicious software (malware) in an unexpected format (e.g. Word documents or PDF files) to one-day exploits of vulnerabilities, to infringing anonymous communications to contact threat actors. New families of ransomware, which have worm-like behaviors, have infected tens of hundreds of individuals, organizations, and important systems with such advanced attacks. These advances in attack techniques make it very difficult to determine the point of origin of the attack as well as to identify the attacker.

2) Attack indicator poll: The authors report in [12] that cybercriminals also use sophisticated methods to combat forensics and evasion in their malicious code, making standard security assessment methods, for example, CVSS (Common Vulnerability Scoring System), or persistent malware and traffic analysis, less efficient. Models, such as Software Defined Networking (SDN), Internet of Things (IoT), and cloud computing, and their widespread adoption by organizations (e.g. using cloud resources to process and store big data) require modern forensic techniques such as Well [12].

C. *Types of Cyber Threat Intelligence*

In [13] the authors discussed that CTI can be classified into four types based on their features and the role of the consumer in the organization as shown in Fig. 1:

- Strategic Threat Intelligence.
- Operational Threat Intelligence.
- Tactical Threat Intelligence.
- Technical Threat Intelligence.

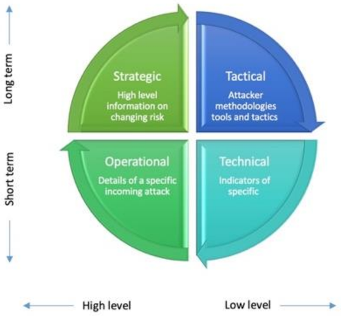
Long term
Short term
Strategic
High level information on changing risk
Tactical
Attacker methodologies tools and tactics
Operational
Details of a specific incoming attack
Technical
Indicators of specific
High level
Low level

Fig. 1. Types of CTI.

The author hypothesizes in [13] that the purpose of strategic intelligence is to provide management personnel with high-quality information about attack trends and threats that can influence high-level business decisions. TI's operational information provides information about specialized and technically focused intelligence (mostly from campaigns, malware, forensic reports, and/or tools) of an organization's specific security incident and is consumed by security managers and the organization; Tactical TI deals with the tactics, techniques, and procedures (TTPS) used by various threat actors, IOCS (Indicators of Settlement) to advocate for signature-based settlements. The author mentioned in [13] that threat intelligence is consumed by incident response teams, and technical threat intelligence is consumed through information feeds, which are often automatically consumed by enforcement or monitoring and analysis systems such as firewalls.

D. Cyber Threat Intelligence Characteristics

The ability to perceive and capture the enemy's attention during the reconnaissance, armament and transmission phases of the cyberattack lifecycle provides the opportunity to take appropriate action to protect the network and prevent attacks. Effective recovery and response strategies can also be created in this way. In [14] the authors claimed that conditioning the following characteristics would result in greater efficacy in TI:

- Timely: For effective threat intelligence, time plays a critical role. Intelligence must be conveyed quickly with petty frivolity.
- Relevant: Threat information must be applied to the relevant environment.
- Accurate: To be able to take more reasonable and effective action against attacks, it is necessary to have more accurate intelligence. Therefore, the information provided through Threat Information must be true, complete, and frank.
- Specific: More detailed and more specific threat information can allow defenders to choose appropriate countermeasures.
- Actionability: Actions need to be defined by threat information to ensure the data necessary to respond to threats.
- The author mentioned in [14] that understanding these four aspects of the model, finding the data that corresponds to each of them, and knowing where the attacker's killing chain occurs, gives insight to the attackers and facilitates the production of threat intelligence. Both fuel the active cyber defense cycle.

III. Risk Management

A. Classification of Risks

In [15] the authors discussed the classifications that determine the nature of the operations generated by the types of risks that have an impact on achieving goals at the level of the economic organization, as shown in Fig. 2, which are:

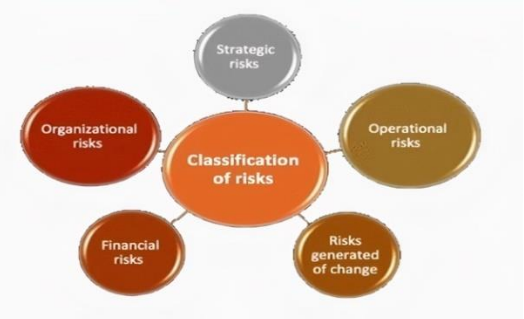

Fig. 2. Classification of Risks.

- Strategic risk relates directly to the development strategy of the organization and is associated with its strategic goals.
- Organizational risks are related to organizational processes, operational activities, and procedures.
- Financing risks are caused by interest rates, inflation, insurance, taxes, protectionist policy, regional policy, and the necessity to minimize losses.
- Risks of change are caused by legislative changes, professional ethics, levels of culture and training, the diversity of needs and requirements, staff fluctuations, and the issues of turnover.
- Operational risks have a direct relationship to the functional compartments within an organization and are linked to the specific objectives defined at the level of functional groups.

B. Types of Risks

The author stated in [15] that the identification of risks to which the organization is exposed may be divided into two categories, namely, inherent risks, and residual risks as shown in Fig. 3, and the risks inherent in any business are those that usually exist before applying internal control measures to reduce risks, or the overall The risks that lie with the entity or organization, whether internal or external, measurable or not. In this way, the inherent risk is the possibility that the administrative and financial statements contain errors or inconsistencies before the implementation of internal control measures.

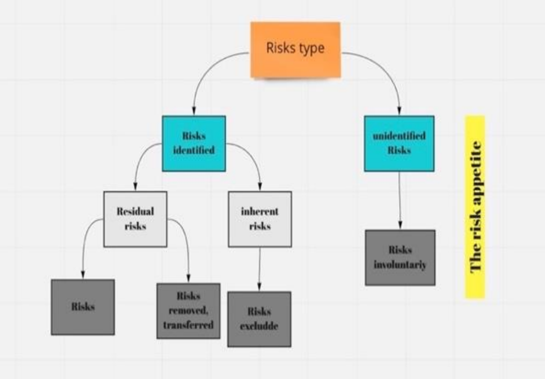

Fig. 3. The Risks Type.

- The author assumed in [15] that the residual risk is the risk that remains after taking measures to mitigate it, the risk-mitigating measure is part of the internal control, and the residual risk is a measure of the effectiveness of the internal control, which is why some countries have replaced the term residual risk with the term "residual risk." Control, therefore, the residual risk is the residual risk after the implementation of internal control measures, the internal control measures must have the effect of reducing the inherent risks at reasonable levels for the organization, and the inherent and residual risks can be considered as illusions of the same risks. As a result, there were inherent risks before the internal controls were introduced, and residual risks emerged after they were introduced.

- Besides inherent and residual risks, there are also control risks and undetected risks that occur at the enterprise level, and there are control risks when the internal control system of the enterprise fails to prevent or detect errors, irregularities, or fraud on time, there may be individual risks associated with the account balance or a class of transactions or both, and risks can be aggregated [15]. In other words, undetectable is the risk that a particular threat cannot be identified and managed, experts in this field believe that economic organizations should focus on assessing risks and keeping them within the limits that they can accept and tolerate because risks cannot be avoided or eliminated.

C. *Risk Management*

The author defined in [15] the risk management process as a plan developed by the leaders of economic organizations and implemented by all employees, and the process includes risk assessment, identification of risk tolerance, and treatment of uncontrollable risks.

Risk management at the level has become necessary due to the uncertainty like threats that may affect the achievement of organizational goals and the environment in which the organization operates, as part of risk management, and the goal is to manage risks in such a way that it can ensure the protection of resources and the protection of employees.

The author argued in [15] that risk management is continuous, and the results arise from decisions made regarding accepting, reducing, or eliminating risks that affect the achievement of objectives, and to prevent losses, avoid threats and take advantage of opportunities, exposure to risks must be optimal.

D. *The Risk Management Process*

The author mentioned in [16] that it is the manager and project team members at different levels who identify and manage risks in several ways, but without a unified framework for risk assessment, this is ineffective, as there will be no full impact assessment.

Risk management is an iterative process, and every aspect of risk management must be planned and implemented at every stage [16]. The risk management process consists of four steps as shown in Fig. 4: Identifying, analyzing, evaluating, and controlling risks.

1) Risks management plan: Risk management frameworks are reviewed and adapted to define project risk management plans at project initiation. The author assumes in [16] that risk management plans include the following guidelines:

- List of possible sources and categories of risk.
- Impact and probability matrix.
- Risk reduction and action plan.
- Intervention plan.
- Threshold and risk values.

2) Identification of risks: The author stated in [16] that risks should be identified and addressed as early in the project as possible. Risks are identified throughout the project life cycle, focusing on key stages. Risk identification is an important topic in the project landscape and the reporting sessions. Some risks emerge easily to the team (known risks), while others may take longer to identify. Risks are identified in a disciplined and systematic way, ensuring that no significant threats are overlooked:

- Risk log: list of risks from history (other projects)
  - List of potential risks
- Expert judgment, using brainstorming.
  - Project status, which includes progress reports.
  - Classification of risks by categories.

3) Risk analyses: Risk analysis or risk assessment involves examining how project outcomes and objectives may change because of the risk event [16]. The risks are identified and then analyzed to determine the qualitative and quantitative impact of the risks on the project so that appropriate mitigation measures can be taken. In general, the author advises in [16] a risk analysis based on these guidelines: the likelihood of occurrence, the extent to which the risk will occur, the exposure to the risk, and the period during which the risk will occur.

4) Risk management: The author mentioned in [16] that risk management includes planning the response to risks, identifying risk drivers, and identifying the person responsible for solving the risks.

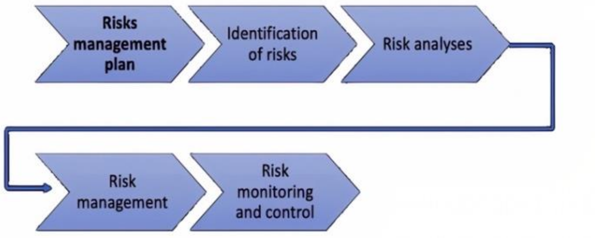

Fig. 4. Risk Management Process.

- Planning the risk response

It may not be possible to eliminate or reduce all the risks associated with a project seamlessly. Managing some risks over longer periods may be necessary and strategically beneficial. To reduce these risks, action plans should be developed [16].

- Risk triggers

In the risk log, the trigger must be recorded for each risk.

The author mentioned in [16] that the triggers are symptoms or warning signs that indicate danger. Risk triggers also indicate when a particular risk is expected to occur, after the implementation of response plans, the degree of risk will be reduced once stakeholder consultation has taken place.

- Risk responsibility

As a basic principle, it is the responsibility of the project manager to manage all risks. The risk owner (who does not necessarily have to be the project manager) must be identified and named in the risk register [16]. The risk owner may be best suited to monitor the risk catalyst but may also be the best suited to implementing and managing the metrics identified, the author assumes in [16] that it is the responsibility of the risk owner to promptly report any change in the risk release status, as well as implement countermeasures specified.

5) *Risk monitoring and control*

In [16] the authors note that risk monitoring and control include:

- Identifying new risks and planning for them.
- Track existing risks to verify that:
  - Reassessment of risks is necessary.
  - Any risk conditions have been triggered.
- Monitor any risks that may become more critical over time.
- Addressing other risks that require a long-term, planned, and managed approach with risk action plans.

E. Risk Management Principles in Higher Education Institutions

It is very important for higher education institutions that they prevent events that could lead to risk in their processes, projects, and other activities, thereby preventing harm from occurring. As well as the above principles, there are other factors to consider [17]:

- Institutions of higher education should integrate risk management into their process maps with defined process features that work in tandem with their main, ancillary, and management processes.
- They must be a key part of decision-making at all levels of management and raise awareness of their importance to the training and business processes among all stakeholders.
- Risk management is the systematic, structured, and timely activity of all institutions' leaders and processes.
- Risk management always adapts to specific situations.
- Risk management is dynamic, repeatable, and sensitive to change.
- Risk management explicitly addresses all types of uncertainty in training processes.
- Risk management is beneficial to the improvement of quality education, processes, and the whole institution.

IV. Literature Review

A. Influencing Factors of Cyber Threats

The study of [18] discussed that risk management has emerged and evolved since the emergence of human societies and has improved greatly over time, including identifying, accepting, evaluating, and controlling undesirable events, and preventing the exploitation of opportunities and threats through risk management actions. The primary function of cybersecurity research is to focus efforts on those circumstances and metrics in which the people involved gain an understanding of how to perceive and respond to specific cybersecurity challenges, bearing in mind that cybersecurity is rapidly evolving from technical specialization into a strategic concept, concluding that most security incidents Caused by inadequate management and regulation with the unpredictability of attacks and insecurity, a lack of attention to security concerns may threaten the future of the organization, so it is important to categorize and prioritize risks [18]. The study of [18] is based on the identification of necessary measures to be taken to protect the information, resources, and resources based on an assessment of threats and vulnerabilities and aim to assist governments and organizations in making decisions about security measures against threats.

The study of [19] discusses the growing popularity of information and communication technology that has led to the rapid increase in cybercrime. In addition, many countries around the world are making the necessary interventions to ensure cybersecurity. It also reported that Saudi Arabia was the worst victim of cybercrime in the Gulf region. The study [19] deals with the extent of Saudi Arabia's readiness to confront and defend cyber threats. The carried work in [19] concluded that despite the existence of an anti-cybercrime law that covers the basic areas of combating cybercrime, it is flawed in the protection against identity theft in addition to the violation of privacy and cyberbullying. Therefore, the Kingdom of Saudi Arabia needs to strengthen the cybercrime law, cybersecurity systems, and the National Cyber Security Authority, and it also needs to develop a strategy and standards for cybersecurity [19].

The study of [20] indicates that the twenty-first century has witnessed a new dimension of security known as cybersecurity. With this development, there has been an exploitation of vulnerabilities in cybersecurity, especially between countries to compete. Over time, malware has become a security threat that cannot be underestimated in cybersecurity. And the Kingdom of Saudi Arabia is a prime target for cyber-attacks due to its economic activity and the high rate of technology use with digital transformation. The study [20] also presented a case study on attacks against Saudi Arabia and focused on two types of malwares: ransomware and Shamoon. The study of [20] suggested some best practices that can be followed to curb attacks, including restricting access, following correct password policies, developing a strong team to respond to incidents in real-time, and providing them with appropriate tools and procedures. The study of [20] showed a lack of scientific studies and investigations dealing with attacks in the Kingdom of Saudi Arabia.

The study of [21] discusses that the technological development of cyber security and the increasing dependence of individuals, societies, and states on it was the reason for the emergence of new and constantly changing threats, where the rapidly developing threats are much more than what can be assessed. The study of [21] showed that defense organizations against attacks in nation-states are considered lagging behind the rapid development of these threats, and this calls for the need to respond to threats in real-time. The study of [21] aims to provide an overview of the most prominent cyber threats and their trends. The study of [21] concluded that it is necessary to increase the capabilities of cyber-threat intelligence in addition to training because it is late and limited compared to the threats.

Cyber security is witnessing the growth and spread of data in information communication technologies, it will be difficult to obtain valid and actionable data from big data to detect and respond to an attack in real-time [22]. the study of [22] suggests a way to organize a large amount of data from different sources, they adopted a pilot approach and reviewed the methodologies for an extensive study on platforms for exchanging information about CTI, implement an online CTI platform, it works to exchange intelligence to reduce the risks of cyber security [22].

B. Leveraging the Cyber Threat Intelligence in Risk Management

Real-time risk assessment is very important, given the nature of the evolving threats that arise from attackers and electronic criminal groups. The study of [23] describes the Polish national platform for cyber security for analyzing cyber risks using CTI, The approach presented came to meet the needs for numerical risk assessment at the national level, to assess risks in real-time, they aim to provide a broad and comprehensive view of cyber threats at the country level And monitor the current situation of the various technical services, Where the proposed approach on the platform is to achieve several goals: From monitoring the cyber security space, detecting threats early, and preparing for measures against hazards in advance, This is the first approach at the national level that uses smart threats, as one of its results is that it leads to building awareness and avoiding the situation.

In [3] the authors discuss that given today's cyber threats and attacks, this requires a new approach to security defenses, since traditional defenses are incompatible with the new generation of more complex threats, any organization needs to collect and share information about cyber threats and turn it into intelligence about Threats and thus contribute to preventing attacks or at least implementing timely disaster recovery. A study by [3] found a classification of types of CTI, providing reliable strategies for sharing information about CTI and some research and criteria to mitigate threat intelligence problems Technical (TTI) and evaluation of most-sourced tools were surveyed [3].

The rapid development of information technology has been associated with an increased risk of cyber-attacks by malicious hackers [24]. The study of [24] argues that organizations aim to develop CTI to enable effective cybersecurity decisions, and many have been interested in Major cybersecurity companies such as Anomal, FireEye, and many others are developing CTI platforms due to their many benefits, including a high ability to identify key threat actors and prioritize threats, as well as an understanding of their technologies, tools, and procedures, and identification of appropriate security controls. The study of [24] aims to provide a systematic review of the CTI platforms that exist today within the industry. This has led to potential future directions that CTI startups can explore, integrate with improved data mining capabilities, and move from CTI platforms to open-source intelligence platforms (OSINT).

The study of [25] discusses the global increase in attacks and cyber threats, and the trend of many organizations at present to CTI. The main function of CTI is to help organizations better understand and know their enemies by pre-detecting threats and responding to them on time [25]. The study of [25] clarified that prior knowledge of the nature of threats is not considered a major direction for risk management and therefore success in risk management with the massive spread of threats and their changing nature is considered low. The study of [25] proposes the work of a CTI-CM model that describes the main capabilities necessary for CTI practitioners to participate effectively in CTI activities. The study of [25] found that at present, threats spread tremendously and faster than prevention information, although this spread makes it more difficult to keep up with these threats, CTI helps to reduce these threats.

In [5] the authors claim that the success of CTI in cybersecurity requires a base that contains an error in knowledge about CTI, and in addition to a good way of representing this knowledge, classifications and sharing criteria are used to serve this purpose. The study of [5] aims to introduce the CTI model. It enables defenders to learn about their CTI capabilities and understand their behavior against changing cyber threats.

The study of [26] discussed that cyberattacks cost the global economy about $445 billion annually. To reduce attacks, many companies have relied on Cyber Threat Information (CTI). The [26] study contributed to the creation of a new framework for CTI by utilizing a web, data, and text approach. Using this framework, many freely available malicious assets, such as encryption programs and keyloggers, have been identified.

C. Risk Management in Higher Education

Higher education institutions have been exposed in recent years to an increasing number of reported security violations, which embody the importance of confidentiality, integrity, and availability of information in universities. The study of [27] aims to systematically review the literature by examining papers that have been published in the past thirteen years in the field of information security management in higher education. The study of [27] found several theoretical contributions, including highlighting the complexity of universities in the practices they apply concerning confidentiality, safety, and access to information. The study of [27] concluded that the field of research is still emerging and that there is an urgent need to increase research efforts in the field of risk management in higher education due to the increasing interest in this field.

Information is one of the most important assets of universities and must be protected from security breaches. Whereas the study of [28] aims to analyze the security threats that develop particularly in the university network environment and recommend an information security framework for the university network environment. The study of [28], evaluation addressed issues at Vikram University, such as enforcing password policies, managing remote access, and restricting mandatory account permissions. The study of [28] when applying the proposed framework to the campus network of Vikram University concluded that the current methods of securing the network are ineffective concerning the university environment and that there is a need to apply for frameworks information protection in the university network, as the proposed framework contributed to Enhancing the level of security in the campus network.

V. Discussion

Risk management has evolved and improved significantly over time and includes identifying, accepting, evaluating, and controlling undesirable events and preventing the exploitation of opportunities and threats through risk management procedures. A study [18] concluded that one of the main reasons that led to the failure to address threats on time is the insufficient management and organization with the inability to anticipate attacks and insecurity, and thus threatens the future of the organization. This confirms the position of the current study in the importance of CTI in enhancing the role of risk management to respond to attacks on time. A study [19] also discussed that one of the reasons for the increase in threats and electronic attacks is the increasing reliance on information and communication technology. Also, many countries around the world have taken the necessary measures to ensure that cybersecurity is so important at present. A study [19] also mentioned that the Kingdom of Saudi Arabia is the worst victim of cybercrime in the Gulf. This reinforces the need to prepare in advance for these threats and to govern the vast amount of information about threats to address them. A study [20] confirmed that, despite the paradigm shift in cyber security in the twenty-first century, there is an increase in cyber threats and their degree of complexity and has even become a subject of competition between countries, and this is something that cannot be underestimated. In addition, the study [21] discussed the increasing adoption of technology by individuals, societies, and countries, which led to the emergence of new and constantly changing threats. This underlines the need to keep pace with these changes by using CTI and training risk response teams on it to reduce risks. In addition, the study [22] discussed a way to organize a large amount of data from various sources, in addition to it focused on the importance of information exchange platforms about cyberthreat intelligence, as it works to reduce cybersecurity risks by exchanging information. A study [23] was based on the work of a Polish national platform for cybersecurity. This platform analyzes cyber risks using CTI. One of the most important and most prominent results of this platform was to achieve awareness and avoid risks, in addition to the fact that there was early detection of threats, and this is one of the most prominent benefits of the intelligence of cyber threats. Moreover, in [3] it is also found that organizations with the new generation of cyber threats need to strengthen defenses through the exchange of CTI information, which effectively contributes to preventing attacks or at least recovering from disasters on time. In [24], the study emphasized that many major companies in the field of cyber security have tended to develop CTI platforms due to their multiple benefits. This illustrates the current awareness of the importance of the CTI and its ability to identify the main actors of the threat and the priority of threats, as well as the ability through the CTI to determine the measures necessary to confront the threats. The study [25] concluded that prior knowledge of the nature of threats is not a major trend for risk management, and this makes managing risks at present with the massive spread of threats considered difficult. Therefore, to enhance risk management and keep it up to date with this development in cyber threats, the capabilities of CTI must be used. The study [5] aimed to present a CTI model characterized by this model in working on the capabilities of defenders in CTI and knowing their behavior against cyber threats. Strengthening the capabilities of defenders through CTI is one of the most important reasons that help reduce risks and make maximum use of CTI capabilities. A study [26] benefiting from the web, data, and text approach contributed to the creation of a new framework for CTI. This framework helped identify malicious assets free of charge. This indicates the multiplicity of ways to take advantage of CTI. A study [27] focuses on the increase in threats with the development in cybersecurity, including higher education, and in recent years it has had an increasing number of security violations. Maintaining the confidentiality of information in the university network is a very important matter that cannot be underestimated. Therefore, it is necessary to increase the security of the university network and to highlight the importance of protecting information and reducing the risks to which higher education institutions are exposed. In addition, the study [28] also discussed the importance of information, as it is one of the most important assets of universities that must be protected from security violations. Due to the great dependence of universities on technology, especially with the digital transformation that we are witnessing in the 21st century, and despite the importance of protecting information on the university network, there is not enough focus on this topic by another research.

Previous studies that were mentioned earlier discussed the reasons for the increase in cyber threats, in addition to the role of CTI in reducing risks, as well as the need for risk management to address threats on time and discussed the need for higher education to focus on protecting information and raising the level of security in the university network. The applications of previous studies for CTI and ways to benefit from it differed. However, previous studies did not discuss the idea of using CTI to improve the ability of risk management to address threats promptly; although she discussed the inability to manage risks to deter threats. In addition to the lack of studies that discuss the need for higher education to enhance security despite its importance. The present paper highlights the utilization of CTI's capabilities in enhancing risk management to reduce threats in higher education.

VI. Conclusion and Future Work

Today, with the increasing adoption of information technology and the emergence of new opportunities and possibilities, but the rapid and continuous progress and development of information technology have increased the complexity of digital systems, which makes these systems less secure and thus leads to the complexity and change of forms and functions of cyber threats. Despite the current development in cybersecurity, there is a new generation of advanced threats that can easily bypass traditional defenses as these defenses were designed to combat a previous generation of attacks. In addition, risk management currently lacks in addressing these threats, which has resulted in them not being addressed on time. Higher education is hard without these threats. In recent years, a high rate of threats has been recorded, due to the reason that computers are an integral part of the university environment, in addition to increasing dependence on technology. Therefore, there is a need to improve these defenses using CTI, as CTI represents information about the nature of threats and a deep understanding of the attacker's objectives and thus the ability to respond to threats and take appropriate defensive measures. CTI aims to clarify the information an organization needs to know to increase awareness about threats to identify and address risks on time, as well as increase the capabilities of defenders to detect and respond. Threat information must be accurate and actionable to take full advantage of CTI. This survey focused on the impact of CTI in enhancing risk management for real-time response and discussed the main challenges and advantages of CTI as well as risk management processes and practices in higher education. CTI enables defenders to increase the ability to make decisions quickly in addition to addressing current and future attacks. The field of cyber security is an evolving field that is constantly changing, where it is possible to increase the strength and development of threats on a continuous and almost daily basis. This topic requires in-depth research on ways to take advantage of CTI, as well as a practical application that demonstrates CTI's ability to combat and reduce threats and raise the level of security in the university's network. Despite previous research efforts, studies discussing the use of CTI in risk management in higher education are almost non-existent despite the importance of the topic. One of the future directions of this survey is to propose a unified platform for Saudi universities to exchange CTI information. Training CTI specialists to raise their awareness and increase their capabilities in dealing with risks. However, gathering actionable information about threats is a significant challenge.

References

[1] The National Cybersecurity Authority Website. Retrieved from https://nca.gov.sa/pages/about.html.

[2] Rania, (2017 oct 20). Saudi Arabia is more than Middle Eastern countries vulnerable to cyber-attacks. Retrieved from https://www.aleqt.com/2017/10/19/article_1269641.html.

[3] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & security, 72, 212-233.K. Elissa, “Title of paper if known,” unpublished.

[4] Kim, Daegeon, and Huy Kang Kim. "Automated Dataset Generation System for Collaborative Research of Cyber Threat Analysis." Security and Communication Networks 2019 (2019).

[5] Mavroeidis, Vasileios, and Siri Bromander. "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence." 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, 2017.

[6] Bromiley, M. (2016). Threat intelligence: What it is, and how to use it effectively. SANS Institute InfoSec Reading Room, 15, 172.

[7] Chismon, D., & Ruks, M. (2015). Threat intelligence: Collecting, analysing, evaluating. MWR InfoSecurity Ltd.

[8] Shackleford, D. (2017). Cyber threat intelligence uses, successes and failures: The sans 2017 cti survey. SANS Institute.

[9] Boeke, S., & van de BDP, J. (2017). Cyber threat intelligence—from confusion to clarity; an investigation into cyber threat intelligence.

[10] Qiang, L., Zeming, Y., Baoxu, L., Zhengwei, J., & Jian, Y. (2016). Framework of cyber attack attribution based on threat intelligence. In Interoperability, Safety and Security in IoT (pp. 92-103). Springer, Cham.

[11] Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371-379.

[12] Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities. In Cyber Threat Intelligence (pp. 1-6). Springer, Cham.

[13] Sukhabogi, S. (2021). A Theoretical review on the importance of Threat Intelligence Sharing & The challenges intricated. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), 3950-3956.

[14] Seker, E. (2020). Cyber threat intelligence understanding fundamentals & Technological Research Council of Turkey, 12(3).

[15] Croitoru, I. (2019). RISK MANAGEMENT-BETWEEN NECESSITY AND OBLIGATION. Internal Auditing & Risk Management, 14(1).

[16] DOVAL, E. (2019). RISK MANAGEMENT PROCESS IN PROJECTS. Review of General Management, 29(2).

[17] Knok, Ž., Kondić, V., & Brekalo, S. (2020). Risk Management in the Higher Education Quality Insurance System. Tehnički glasnik, 14(1), 46-54.

[18] Riza, I. (2017). Risk management from the information security perspective. Junior Scientific Researcher, 3(2), 1-8.

[19] Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. Archives of Business Research, 6(12).

[20] Alelyani, S., & Kumar, H. (2018). Overview of cyberattack on saudi organizations.

[21] Kettani, H., & Wainwright, P. (2019, March). On the top threats to cyber systems. In 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT) (pp. 175-179). IEEE.

[22] Mtsweni, J., Muyowa Mutemwa, and Njabulo Mkhonto. "Development of a cyber-threat intelligence-sharing model from big data sources." Journal of Information Warfare 15.3 (2016): 56-68.

[23] Janiszewski, Marek, Anna Felkner, and Piotr Lewandowski. "A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence." Journal of Telecommunications and Information Technology (2019).

[24] Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 135-154.

[25] Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability'that needs to be fostered in information security practitioners and how this can be accomplished. Computers & Security, 92, 101761.

[26] Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. Journal of Management Information Systems, 34(4), 1023-1053.

[27] Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350-357.

[28] Joshi, C., & Singh, U. K. (2017). Information security risks management framework–A step towards mitigating security risks in university network. Journal of Information Security and Applications, 35, 128-137.